Gobierno espía - Tecnología espía

El Caso Pegasus

Recopilación de textos

El espionaje en internet estará siempre justificado por quienes la ejecutan. El Estado en sus respectivos gobiernos dice lo hace por motivos de seguridad ciudadana. Las corporaciones tecnológicas dicen lo hacen por mejorar el servicio, y también para contribuir a la seguridad ciudadana cuando entregan nuestros datos al Estado.

Lo hicieron, lo hacen y lo seguirán haciendo, aunque se haga una cruzada por el derecho a la privacidad de nuestros datos, porque tienen ellos el control el poder y las tecnologías para hacerlo sin que sepamos o también lo harán a la fuerza o con nuestra complacencia mayormente al usar redes propietarias tal como se viene haciendo en cuarentena con tanto debate virtual o campañas de solidaridad en que se hacen uso de facebook, zoom, youtube, gmail, google meet, el mismo uso de móviles, etc.

Usando redes libres no nos asegura al 100% de estos espionajes, pero lo aminora. Conociendo esto que poco se difunde en redes (sorprendentemente en redes libres se suele pasar por alto estas medidas de seguridad reduciendo solo a no usar las redes de las GAFAM) podemos ver entonces que debemos compartir o comunicar en redes aunque sean redes libres, y que no.

Y claro, el uso de redes propietarias de las Gafam y aliados, hace este espionaje más fácil.

Empecemos a normalizar el autocuidado en redes, no esperemos que nos pase como lo que ya sucede en diversas latitudes como Mexico, España, etc como entre varios casos el caso Pegasus que compartiré abajo en una recopilación de artículos de algunos lugares que están hablando de ese tema.

Pegasus Project | La nueva arma para silenciar a los periodistas

La casa de Khadija Ismayilova en Bakú se había convertido en una prisión. En Azerbaiyán, una nación rica en petróleo ubicada junto al mar Caspio que desde 2014 ha reprimido cada vez más la libertad de expresión y la disidencia, las investigaciones de Ismayilova sobre la familia gobernante la habían convertido en un objetivo principal de su propio gobierno.

La periodista de investigación azerbaiyana sabía que la vigilaban constantemente, y amigos y familiares a quienes se les había pedido que la espiaran se lo habían dicho.

Las autoridades le habían arrojado el libro: instalaron subrepticiamente cámaras en su casa para filmarla durante el sexo; arrestarla y acusarla de llevar a un colega al suicidio; y finalmente acusarla de fraude fiscal y sentenciarla a siete años de prisión.

Fue puesta en libertad bajo fianza después de 18 meses y se le prohibió salir del país durante cinco años.

Entonces, en mayo de 2021, al final de la prohibición de viajar, cuando Ismayilova empacó sus pertenencias y abordó un avión a Ankara, Turquía, pudo haber pensado que estaba dejando todo eso atrás.

Poco sabía ella que el espía más invasivo vendría con ella.

Durante casi tres años, el teléfono de Khadija Ismayilova fue infectado regularmente con Pegasus, una herramienta de software espía altamente sofisticada desarrollada por la compañía israelí NSO Group que brinda a los clientes acceso a la totalidad del contenido de un teléfono e incluso puede acceder de forma remota a la cámara y al micrófono, según un informe. análisis forense realizado por el Laboratorio de seguridad de Amnistía Internacional, en colaboración con Forbidden Stories.

"Toda la noche he estado pensando en qué hice con mi teléfono", dijo a los periodistas desde su hogar temporal en Ankara el día después de enterarse de que su teléfono había sido comprometido. "Me siento culpable por los mensajes que he enviado. Me siento culpable por las fuentes que me enviaron [información] pensando que algunas formas de mensajería encriptada son seguras y no sabían que mi teléfono estaba infectado ".

"Los miembros de mi familia también son victimizados", agregó. "Las fuentes son victimizadas, las personas con las que he estado trabajando, las personas que me dijeron sus secretos privados son victimizadas".

El Proyecto Pegasus

Ismayilova es una de los casi 200 periodistas de todo el mundo cuyos teléfonos han sido seleccionados como objetivos por los clientes de NSO, según el Proyecto Pegasus, una investigación publicada hoy por un consorcio global de más de 80 periodistas de 17 medios de comunicación en 10 países, coordinado por Forbidden Stories con el apoyo técnico del Laboratorio de Seguridad de Amnistía Internacional.

Forbidden Stories y Amnistía Internacional tuvieron acceso a una filtración de más de 50.000 registros de números de teléfono que los clientes de NSO seleccionaron para vigilancia. Según un análisis de estos registros realizado por Forbidden Stories y sus socios, los teléfonos de al menos 180 periodistas fueron seleccionados en 20 países por al menos 10 clientes de NSO. Estos clientes gubernamentales van desde autocráticos (Bahrein, Marruecos y Arabia Saudita) hasta democráticos (India y México) y abarcan todo el mundo, desde Hungría y Azerbaiyán en Europa hasta Togo y Ruanda en África. Como mostrará el Proyecto Pegasus, muchos de ellos no han tenido miedo de seleccionar a periodistas, defensores de derechos humanos, opositores políticos, empresarios e incluso jefes de Estado como blancos de esta tecnología invasiva.

Declarando "consideraciones contractuales y de seguridad nacional", NSO Group escribió en una carta a Forbidden Stories y sus socios de medios que "no puede confirmar o negar la identidad de nuestros clientes gubernamentales". Forbidden Stories y sus socios de medios se comunicaron con cada uno de los clientes gubernamentales citados en este proyecto, todos los cuales no respondieron a las preguntas antes de la fecha límite o negaron ser clientes de NSO Group.

Es imposible saber si un número de teléfono específico que aparece en la lista se vio comprometido con éxito sin analizar el dispositivo. Sin embargo, el Laboratorio de Seguridad de Amnistía Internacional, en asociación con Forbidden Stories, pudo realizar análisis forenses en los teléfonos de más de una docena de estos periodistas, y 67 teléfonos en total, revelando infecciones exitosas a través de una falla de seguridad en iPhones tan reciente como este mes.

Los números de teléfono filtrados, que Forbidden Stories y sus socios analizaron durante meses, revelan por primera vez la asombrosa escala de vigilancia de periodistas y defensores de los derechos humanos, a pesar de las reiteradas afirmaciones de NSO Group de que sus herramientas se utilizan exclusivamente para atacar a criminales y terroristas graves. y confirmar los temores de los defensores de la prensa sobre el alcance del software espía que se utiliza contra los periodistas.

"Las cifras muestran claramente que el abuso es generalizado, pone en peligro la vida de los periodistas, la de sus familiares y asociados, socava la libertad de prensa y cierra medios críticos", ha manifestado Agnes Callamard, secretaria general de Amnistía Internacional. "Se trata de controlar la narrativa pública, resistir el escrutinio, reprimir cualquier voz disidente".

Los periodistas que aparecen en estos registros han recibido amenazas legales, otros han sido arrestados y difamados, y algunos han tenido que huir de sus países debido a la persecución, solo para luego descubrir que todavía estaban bajo vigilancia. En raras ocasiones, los periodistas han sido asesinados después de haber sido seleccionados como objetivos. Las revelaciones de hoy dejan en claro que la tecnología se ha convertido en una herramienta clave en manos de los actores gubernamentales represivos y las agencias de inteligencia que trabajan para ellos.

"Vigilar a un periodista tiene un efecto paralizador muy fuerte", dijo a Forbidden Stories Carlos Martínez de la Serna, director del programa del Comité para la Protección de los Periodistas. "Este es un problema muy, muy importante que todos deben tomar en serio, no solo en el contexto de donde los periodistas están trabajando en un ambiente hostil para el periodismo, sino en los Estados Unidos, Europa Occidental y otros lugares".

El grupo NSO, en una respuesta escrita a Forbidden Stories y sus socios de medios, escribió que los informes del consorcio se basaban en "suposiciones erróneas" y "teorías no corroboradas" y reiteró que la empresa tenía una "misión de salvar vidas".

"NSO Group niega firmemente las afirmaciones falsas hechas en su informe, muchas de las cuales son teorías no corroboradas que plantean serias dudas sobre la confiabilidad de sus fuentes, así como sobre la base de su historia", escribió la compañía. "Sus fuentes le han proporcionado información que no tiene base fáctica, como lo demuestra la falta de documentación de respaldo para muchas de las afirmaciones".

“La supuesta cantidad de ‘datos filtrados de más de 50.000 números de teléfono’ no puede ser una lista de números a los que apuntan los gobiernos que usan Pegasus, basada en este número exagerado”, agregó NSO Group.

En una carta legal enviada a Forbidden Stories y sus socios de medios, NSO Group también escribió: “NSO no tiene información sobre las actividades de inteligencia específicas de sus clientes, pero incluso una comprensión rudimentaria y de sentido común de la inteligencia lleva a la clara conclusión de que estos Los tipos de sistemas se utilizan principalmente para fines distintos a la vigilancia “.

Tan peligroso como un presunto terrorista

Para Szabolcs Panyi, periodista de investigación de Direkt36 en Hungría, enterarse de que su teléfono celular había sido infectado con el software espía Pegasus fue “devastador”.

“Hay algunas personas en este país que consideran a un periodista regular tan peligroso como alguien sospechoso de terrorismo”, dijo a Forbidden Stories a través de una línea de comunicación cifrada.
Panyi tiene alrededor de 30 años. Lleva gafas de montura redonda y tiene una barba corta. El galardonado periodista ha informado sobre defensa, asuntos exteriores y otros temas sensibles y tiene un rolodex de miles de contactos en varios países, incluido Estados Unidos, donde pasó un año con una beca Fulbright, lo que lo convierte en un objetivo ideal para la inteligencia. servicios, que se sabe que desconfían de la influencia estadounidense en Hungría.

Panyi estaba trabajando en dos novedades importantes durante el tiempo que su teléfono se vio comprometido en 2019. Forbidden Stories, en asociación con el Laboratorio de Seguridad de Amnistía Internacional, pudo confirmar infecciones exitosas de su teléfono durante un período de 9 meses, de abril a diciembre. Estas infecciones, dijo Panyi, a menudo coincidían con sus solicitudes oficiales de comentarios y reuniones importantes con las fuentes.

Una de las intrusiones digitales ocurrió cuando se reunía con un fotoperiodista húngaro que trabajaba como reparador de un reportero de un medio de noticias con sede en Estados Unidos. Que trabajaba en una historia sobre el Banco Internacional de Inversiones, un banco respaldado por Rusia que en 2019 fue presionando para establecer sucursales en Budapest.

Por esa época, el fotoperiodista fijador también fue seleccionado como objetivo, según los registros a los que tuvo acceso Forbidden Stories.

“Es muy probable que quienes están operando este sistema estuvieran interesados en lo que estos periodistas húngaros y estadounidenses iban a escribir sobre este banco ruso”, dijo Panyi.

Al igual que Panyi, muchos periodistas que son objeto de amenazas digitales y vigilancia cibernética son interesantes para las agencias de inteligencia estatales debido a sus fuentes, según Igor Ostrovskiy, un investigador privado de la ciudad de Nueva York que anteriormente espió a periodistas como Ronan Farrow, Jodi Kantor. y el reportero del Wall Street Journal Bradley Hope como subcontratista de la empresa israelí Black Cube y ahora capacita a periodistas en seguridad de la información.

"Todos sabemos que los periodistas tienen un montón de información pasando por sus manos, por lo que podría ser la razón por la que la seguridad del Estado podría estar interesada", dijo. "La seguridad del estado podría estar interesada en quién está filtrando dentro del gobierno, o dentro de una empresa que es vital para el gobierno, y podrían estar buscando esa fuente".

Al otro lado del mundo, el teléfono de Paranjoy Guha Thakurta, un periodista de investigación indio y autor de varios libros sobre negocios y política indios, fue pirateado en 2018. Thakurta le dijo a Forbidden Stories que a menudo hablaba con fuentes bajo condición de anonimato. y dijo que en el momento de su ataque estaba trabajando en una investigación sobre las finanzas del difunto Drirubhai Ambani, anteriormente el hombre más rico de la India.

"Sabrían quiénes eran nuestras fuentes", dijo Thakurta. "El propósito de acceder a mi teléfono y ver quiénes son las personas con las que estoy hablando sería averiguar quiénes son las personas que nos han brindado información a mí y a mis colegas".

Thakurta es uno de los al menos 40 periodistas indios seleccionados como objetivos de un cliente de NSO que parece ser el gobierno indio, según el análisis del consorcio de los datos filtrados.

El gobierno indio nunca ha confirmado ni negado ser cliente de NSO Group. "Las acusaciones sobre la vigilancia gubernamental de personas específicas no tienen ninguna base concreta o verdad asociada", escribió un portavoz del Ministerio de Electrónica y Tecnología de la Información en respuesta a preguntas detalladas enviadas por Forbidden Stories y sus socios.

Si bien informes anteriores mostraron cuatro periodistas entre los 121 objetivos de Pegasus revelados en India en 2019, los registros a los que tuvo acceso Forbidden Stories muestran que esta vigilancia puede haber sido mucho más extensa. Más de 2.000 números indios y paquistaníes fueron seleccionados como objetivos entre 2017 y 2019, entre ellos periodistas indios de casi todos los principales medios de comunicación, incluidos The Hindu, Hindustan Times, Indian Express, India Today, Tribune y The Pioneer. Los periodistas locales también fueron seleccionados como objetivos, incluido Jaspal Singh Heran, editor en jefe de un medio con sede en Punjab que publica solo en Punjabi.

Los teléfonos de dos de los tres cofundadores del medio de noticias en línea independiente The Wire, Siddharth Varadarajan y MK Venu, fueron infectados por Pegasus, y el teléfono de Venu fue pirateado en julio. Varios otros periodistas que trabajan o han contribuido con el medio de noticias independiente, incluido el columnista Prem Shankar Jha, el reportero de investigación Rohini Singh, el editor diplomático Devirupa Mitra y el colaborador Swati Chaturvedi, fueron seleccionados como objetivos, según los registros a los que tuvo acceso Forbidden Stories y sus socios, que incluyen The Wire.

"Fue alarmante ver tantos nombres de personas vinculadas a The Wire, pero luego hay muchas personas que no están vinculadas a The Wire", dijo Varadarajan, cuyo teléfono se vio comprometido en 2018. "Así que esto parece ser una predisposición general a someter a los periodistas a una vigilancia de alto nivel por parte del gobierno".

Muchos de los periodistas que hablaron con Forbidden Stories y sus organizaciones de noticias asociadas expresaron consternación por haber aprendido que, a pesar de las precauciones que habían tomado para proteger sus dispositivos, como el uso de servicios de mensajería cifrada y la actualización de sus teléfonos con regularidad, su información privada aún no estaba segura.

"Nos hemos estado recomendando mutuamente esta o aquella herramienta, cómo mantener (nuestros teléfonos) cada vez más seguros de los ojos del gobierno", dijo Ismayilova. "Y ayer me di cuenta de que no hay forma. A menos que te encierres en [una] tienda de hierro, no hay forma de que no interfieran en tus comunicaciones".

A Panyi le preocupaba que el conocimiento público de su objetivo pudiera disuadir a las fuentes de ponerse en contacto con él en el futuro.

"La preocupación de todos los periodistas que han sido atacados es que una vez que se revela que usted fue vigilado e incluso nuestros mensajes confidenciales podrían haber sido comprometidos, ¿quién diablos va a hablar con nosotros en el futuro?" preguntó. "Todo el mundo pensará que somos tóxicos, que somos una carga".

"Leer por encima del hombro": cómo se utiliza Pegasus para espiar a los periodistas con cero clics

Los análisis forenses de Amnistía Internacional Security Lab de teléfonos móviles atacados con Pegasus como parte del Proyecto Pegasus son consistentes con análisis anteriores de periodistas atacados a través del software espía de NSO, incluidas las docenas de periodistas presuntamente pirateados en los Emiratos Árabes Unidos y Arabia Saudita e identificados por Citizen Lab en diciembre del año pasado.

"Hay un montón de piezas diferentes, esencialmente, y todas encajan muy bien", dijo Claudio Guarnieri, director del Laboratorio de Seguridad de Amnistía Internacional. "No tengo ninguna duda de que lo que estamos viendo es Pegasus porque las características

son muy distintas y todos los rastros que vemos se confirman".

En total, el Comité para la Protección de los Periodistas (CPJ) había documentado anteriormente 38 casos de software espía, desarrollado por empresas de software en cuatro países, utilizado contra periodistas en nueve países desde 2011.

Eva Galperin, directora de ciberseguridad de la Electronic Frontier Foundation (EFF), fue una de las primeras investigadoras de seguridad en identificar y documentar ciberataques contra periodistas y defensores de los derechos humanos en México, Vietnam y otros lugares a principios de la década de 2010.

En ese momento, a principios de la década de 2010, la mayoría de los ataques de malware eran menos sofisticados de lo que son hoy, explicó.

"En 2011, recibía un correo electrónico y el correo electrónico iría a su computadora y el malware estaría diseñado para instalarse en su computadora", dijo.

No fue hasta alrededor de 2014 que un enfoque de espionaje de periodistas de "dispositivos móviles primero" ganó popularidad, ya que los teléfonos inteligentes se volvieron más omnipresentes, dijo. Los clientes de empresas como NSO, Hacking Team y FinFisher utilizaron la "ingeniería social" para enviar mensajes específicamente diseñados a los objetivos, a menudo provocándolos con información sobre posibles primicias o información específica sobre miembros de sus familias. Los objetivos tendrían que hacer clic en un enlace para que el malware se instale en sus teléfonos.

Los periodistas son objetivos obvios para las agencias de inteligencia, dijo Ostrovskiy, porque siempre están buscando nuevas fuentes de información, abriéndose a intentos de phishing, y porque muchos a menudo no siguen las "mejores prácticas de la industria en seguridad digital".

Algunas de las primeras infecciones de periodistas por Pegasus se identificaron en México en 2015 y 2016.

En enero de 2016, Carmen Aristegui, periodista de investigación en México y fundadora de Aristegui Noticias, comenzó a recibir mensajes con vínculos sospechosos luego de que publicara una investigación sobre una propiedad del expresidente mexicano Enrique Peña Nieto.

Aristegui recibió más de 20 mensajes de texto que contenían enlaces maliciosos de Pegasus, según revelaría más tarde el grupo de derechos digitales Citizen Lab en el informe de Gobierno Espía ("Espionaje del gobierno") de 2017. Según el informe, los teléfonos de varios de sus colegas y familiares también fueron atacados con mensajes de texto que contenían enlaces maliciosos durante ese mismo periodo, incluidos los de sus colegas Sebastián Barragán y Rafael Cabrera y su hijo Emilio Aristegui, de solo 16 años -en ese

momento-.

Forbidden Stories y sus socios pudieron identificar por primera vez a otras tres personas cercanas a Aristegui que fueron seleccionadas como objetivos de vigilancia en 2016: su hermana Teresa Aristegui, su productora de CNN Karina Maciel y su exasistente Sandra Nogales.

"Fue un gran impacto ver a otras personas cercanas a mí en la lista", dijo Aristegui, quien era parte del Proyecto Pegasus. "Tengo seis hermanos, pero al menos uno de ellos, mi hermana, ingresó al sistema. Mi asistente Sandra Nogales, que sabía todo sobre mí, que tenía acceso a mi horario, todos mis contactos, mi día a día, mi hora a hora, también ingresó al sistema ".

Desde esos primeros días, la instalación del software espía Pegasus en los teléfonos inteligentes se ha vuelto más sutil, dijo Guarnieri. En lugar de que el objetivo tenga que hacer clic en un enlace para instalar el software espía, los llamados exploits de "clic cero" permiten al cliente tomar el control del teléfono sin ningún compromiso por parte del objetivo.

"La complejidad de realizar estos ataques ha aumentado exponencialmente", dijo.

Una vez instalado con éxito en el teléfono, el software espía Pegasus brinda a los clientes de NSO acceso completo al dispositivo y, por lo tanto, la capacidad de eludir incluso las aplicaciones de mensajería encriptadas como Signal, WhatsApp y Telegram. Pegasus se puede activar a voluntad hasta que se apague el dispositivo. Tan pronto como se vuelva a encender, el teléfono se puede volver a infectar.

"Si alguien está leyendo por encima de su hombro, no importa qué tipo de cifrado se haya utilizado", dijo Bruce Schneier, criptólogo y miembro del Centro Berkman Klein para Internet y Sociedad de Harvard.

Según Guarnieri, los operadores de Pegasus pueden grabar audio y video de forma remota, extraer datos de aplicaciones de mensajería, usar el GPS para rastrear la ubicación y recuperar contraseñas y claves de autenticación, entre otras cosas. Los gobiernos espías se han movido en los últimos años hacia una estrategia más de "golpe y fuga" para evitar la detección, dijo Galperin: infectar teléfonos, exfiltrar los datos y salir rápidamente del dispositivo.

Este tipo de tecnologías digitales van de la mano con la vigilancia física, según Ostrovskiy.

"Las intrusiones digitales son extremadamente valiosas", dijo. "Si pudiéramos, por ejemplo, haber conocido tu calendario, si pudiéramos haber sabido que vas a tener una reunión determinada o podríamos echar un vistazo a tu correo electrónico, tus notas a cualquier material que la mayoría de nosotros tengamos en nuestros teléfonos, tendríamos una gran

ventaja para tener más éxito en cualquier objetivo que intentemos lograr ".

Un nuevo mercado de software espía

La vigilancia de periodistas no es nueva, dicen los expertos en seguridad. Lo que ha cambiado es el mercado del software espía.

Mientras que en el pasado los gobiernos desarrollaron herramientas de software espía internamente, las empresas privadas de software espía como NSO Group, FinFisher y Hacking Team vieron una oportunidad para vender sus productos a gobiernos que anteriormente no tenían la experiencia técnica para desarrollar sus propios programas de inteligencia de señales, según a Galperin. Esto creó una especie de "salvaje oeste" de espionaje de periodistas y activistas, dijo.

En su informe "Hide and Seek" de 2018, la organización de derechos digitales Citizen Lab identificó a los operadores de Pegasus de NSO en varios países con registros de detenciones arbitrarias de periodistas y defensores de los derechos humanos, incluidos Arabia Saudita, Marruecos y Bahréin. En conjunto, los clientes de NSO en estos países han seleccionado decenas de miles de números de teléfono, basándose en el análisis del consorcio de los datos filtrados.

Algunos reporteros, como el periodista de investigación independiente marroquí Omar Radi, cuya intrusión cibernética Forbidden Stories informó en 2020, o el periodista indio y defensor de los derechos humanos Anand Teltumbde, fueron encarcelados después de que grupos de defensa y medios de comunicación documentaran sus infecciones telefónicas.

Las empresas de software espía se han enfrentado a relativamente pocas consecuencias legales o financieras por el uso de su software espía contra periodistas y defensores de los derechos humanos, aunque casos legales recientes han comenzado a presionar a estos proveedores. En junio de 2021, la empresa francesa de software espía Amesys fue acusada de "complicidad en actos de tortura" por vender su software espía a Libia entre 2007 y 2011. Según los demandantes en ese caso, la información obtenida a través de la vigilancia digital se utilizó para identificar y perseguir a los opositores de depuso al dictador Muammar Gaddafi, quien luego fue torturado en prisión.

"Si estás haciendo un buen periodismo, le estás diciendo la verdad al poder y estás cabreando a la gente con poder", dijo Galperin. "Las personas que estaban haciendo periodismo que contaban historias sobre corrupción a menudo eran blanco de ataques. Personas que estaban haciendo un activismo que era nuevamente, protestando contra la corrupción, protestando contra el autoritarismo, esas eran a menudo las personas que estaban en la primera línea de ser espiadas".

NSO Group sostiene que su tecnología es utilizada exclusivamente por agencias de inteligencia para rastrear criminales y terroristas. Según el informe de transparencia y responsabilidad de NSO Group, publicado en junio de 2021, la empresa tiene 60 clientes en 40 países de todo el mundo.

"(Pegasus) no es una tecnología de vigilancia masiva, y solo recopila datos de los dispositivos móviles de individuos específicos, sospechosos de estar involucrados en delitos graves y terror", escribió NSO Group en el informe.

Aunque la compañía también dice que tiene una lista de 55 países a los que no venderá debido a sus antecedentes de derechos humanos, esos países no figuran en el informe. Según el informe, NSO Group ha revocado el acceso a cinco clientes desde 2016 después de investigaciones sobre uso indebido y rescisión de contratos con otros cinco que no cumplían con los estándares de derechos humanos.

"NSO Group continuará investigando todas las denuncias creíbles de uso indebido y tomará las medidas adecuadas en función de los resultados de estas investigaciones", escribió NSO Group en su declaración a Forbidden Stories y sus socios de medios. "Esto incluye apagar el sistema de un cliente, algo que NSO ha demostrado su capacidad y voluntad de hacer, debido a un mal uso confirmado, lo hizo varias veces en el pasado y no dudará en volver a hacerlo si la situación lo amerita".

Sin embargo, los datos filtrados muestran que muchos otros gobiernos autoritarios conocidos por reprimir la libertad de expresión siguen siendo clientes.

Como parte del Proyecto Pegasus, Forbidden Stories ha podido documentar el uso de Pegasus por primera vez en Azerbaiyán. Más de 40 periodistas azerbaiyanos fueron seleccionados como objetivos, incluidos reporteros de Azadliq.info y Mehdar TV, dos de los únicos medios de comunicación independientes que quedan en el país.

En Azerbaiyán, la mayoría de los medios de comunicación independientes están bloqueados y las autoridades han acosado habitualmente a los familiares de los periodistas. Bajo el presidente Ilham Aliyev, cuya familia ha gobernado Azerbaiyán durante décadas, el espacio para las voces críticas, según Human Rights Watch, se ha "prácticamente extinguido".

El teléfono del periodista independiente Sevinc Vaqifqizi se vio comprometido entre 2019 y 2021, según un análisis realizado por el Laboratorio de seguridad de Amnistía Internacional, en asociación con Forbidden Stories. Como reportero independiente de Mehdar TV, Vaqifqizi ya había recibido varias amenazas, y en febrero de 2020 fue brutalmente golpeado mientras cubría una protesta.
La reportera, de unos 30 años y cabello negro hasta los hombros, dijo a los periodistas del consorcio Forbidden Stories que ya asumió que el gobierno tenía acceso a su información privada.

“Siempre les dije a mis amigos que pueden escucharnos”, dijo. “Me preocupan mis fuentes que confían en nosotros y nos escriben en WhatsApp. Si enfrentan algunos problemas, eso no es bueno para nosotros”.

Aunque actualmente se encuentra en Alemania con una beca de tres meses, no se sentía segura de las autoridades. Como han documentado Amnistía Internacional y otros, los activistas azerbaiyanos han sido atacados física y digitalmente incluso después de salir del país.

“Si tienes un teléfono, probablemente puedan seguir (apuntándote) en Alemania”, dijo.
Fuera de la vista, no fuera de su alcance

Las paredes de la oficina de Hicham Mansouri en la Maison des Journalistes (Casa de los Periodistas) en París están cubiertas con carteles de Reporteros sin Fronteras y otras organizaciones de defensa de la libertad de prensa. El periodista solía vivir en el edificio, que funciona como espacio de exposición y residencia para periodistas refugiados. Desde entonces se mudó, pero todavía comparte una pequeña oficina en la planta baja donde va a trabajar tres veces por semana.

Antes de hablar con Forbidden Stories, Mansouri apagó su teléfono prestado y lo enterró profundamente en su mochila. Según un análisis forense del Laboratorio de Seguridad de Amnistía Internacional, el iPhone anterior de Mansouri se había infectado con Pegasus más de 20 veces durante un periodo de tres meses desde febrero hasta abril de 2021.

Mansouri, periodista de investigación independiente y cofundador de la Asociación Marroquí de Periodistas de Investigación (AMJI, por sus siglas en francés) que actualmente está trabajando en un libro sobre el tráfico ilegal de drogas en las cárceles marroquíes, huyó de Marruecos en 2016 después de numerosas amenazas legales y físicas contra él.

En 2014, fue golpeado por dos agresores desconocidos después de salir de una reunión con defensores de los derechos humanos, incluida la historiadora Maati Monjib, que luego fue atacada con Pegasus. Un año después, agentes de inteligencia armados allanaron su casa a las 9 a.m. y lo encontraron a él y a una amiga en su habitación juntos. Lo desnudaron y lo arrestaron por “adulterio”, que es un crimen en Marruecos. Pasó 10 meses en una prisión de Casablanca, en una celda reservada para los delincuentes más graves que los reclusos habían apodado “La Poubelle” o “El cubo de la basura”. Al día siguiente de salir de la cárcel, Mansouri se fue de Marruecos a Francia, donde solicitó y se le concedió asilo.

Cinco años después, Mansouri descubrió que todavía era un objetivo del gobierno marroquí.

“Todo régimen autoritario ve peligro en todas partes”, dijo Mansouri a Forbidden Stories. “No nos consideramos peligrosos porque hacemos cosas que consideramos legítimas, que sabemos que están en nuestro derecho, pero para ellos son peligrosas”.

“Tienen miedo de las chispas, porque saben que son inflamables”, agregó.

Al menos 35 periodistas en cuatro países fueron seleccionados como objetivos por un cliente de NSO que parece ser el gobierno marroquí, según el análisis del consorcio de los datos filtrados. Muchos de los periodistas marroquíes seleccionados como objetivos han sido en algún momento detenidos, difamados o atacados de alguna manera por los servicios de inteligencia. Otros que fueron seleccionados como objetivos, incluidos los editores de periódicos Taoufik Bouachrine y Soulaimane Raissouni, se encuentran actualmente en prisión por cargos que, según las organizaciones de defensa de los derechos humanos, fueron instrumentalizados en un esfuerzo por acabar con el periodismo independiente en Marruecos.

En un comunicado compartido con Forbidden Stories y sus socios, un representante de la embajada marroquí escribió que no “entendía el contexto” de las preguntas enviadas por el consorcio y estaba “esperando pruebas materiales” de “cualquier relación entre Marruecos y el israelí declarado empresa.”

Bouachrine, editor de Akhbar al-Youm, fue arrestado en febrero de 2018 por cargos de trata de personas, agresión sexual, violación, prostitución y acoso. De 14 mujeres que presuntamente acusaron a Bouachrine, 10 comparecieron ante el tribunal y cinco declararon que Bouachrine era inocente, según el CPJ. El editor había escrito previamente artículos de opinión críticos con el régimen marroquí, acusando a varios funcionarios gubernamentales de alto nivel de corrupción. Fue sentenciado a 15 años de prisión y pasó más de un año en régimen de aislamiento.

Forbidden Stories y sus socios han podido confirmar que los números de al menos dos mujeres involucradas en el caso fueron seleccionados como objetivos de Pegasus.

El sucesor de Bouachrine, Soulaimane Raissouni, también fue arrestado por cargos de agresión sexual en mayo de 2020 y fue sentenciado a cinco años de prisión en julio de 2021. Raissouni fue acusado de agresión por un activista LGBTQ, Adil Ait Ouchraa, quien le dijo al CPJ que no había ‘ Anteriormente se sentía cómodo presentando una reclamación pública debido a su identidad sexual.

Periodistas y defensores de la libertad de prensa dijeron al CPJ que creían que la denuncia se había presentado como represalia contra los informes críticos de Raissouni. En 2021, aún en espera de juicio, Raissouni inició una huelga de hambre que, al momento de escribir estas líneas, había durado más de 100 días. Sus familiares dijeron que después de 76 días se encontraba en estado crítico.

“El objetivo (de la vigilancia) es presumiblemente rastrear la vida privada de las personas para encontrar un gancho en el que puedan colgar cualquier gran juicio”, dijo Ahmed Benchemsi, ex periodista y fundador de las organizaciones de medios independientes TelQuel y Nichane, quien ahora lidera comunicaciones para la región MENA en Human Rights

Watch.

Si bien en el pasado los periodistas marroquíes eran atacados habitualmente con ataques legales por cosas que escribían, como difamación o falta de respeto al rey, la nueva táctica era acusarlos de delitos más graves como espionaje y luego violación y agresión sexual, dijo. La vigilancia surgió como una herramienta clave para recopilar información personal que podría utilizarse para esos fines.

"A menudo hay una pizca de verdad en una gran masa de calumnias, pero esa pizca de verdad suele ser algo personal y confidencial que solo puede provenir de la vigilancia", dijo.

Los periodistas extranjeros que han cubierto la difícil situación de los periodistas marroquíes también han sido seleccionados como objetivos y, en algunos casos, sus teléfonos se infectaron con éxito.

El teléfono de Edwy Plenel, el director y uno de los cofundadores de Mediapart, un medio de periodismo de investigación francés, se vio comprometido en el verano de 2019, según un análisis del Security Lab de Amnistía Internacional que fue revisado por pares por la organización de derechos digitales Citizen Laboratorio.

En junio de ese año, Plenel había asistido a una conferencia de dos días en Essaouira, Marruecos, a petición de un periodista socio de Mediapart, Ali Amar, fundador de la revista de investigación marroquí LeDesk, cuyo número de teléfono también aparece en los registros accedidos por Forbidden Stories. En el acto, Plenel concedió una serie de entrevistas en las que habló sobre las violaciones de derechos humanos cometidas por el estado marroquí. A su regreso a París, comenzaron a aparecer procesos sospechosos en su dispositivo.

"Trabajamos con Ali Amar; publicamos algunas investigaciones juntos y conocí a Ali Amar, un poco como conozco a muchos de los periodistas que luchan por una prensa libre en Marruecos", dijo Plenel en una entrevista con Forbidden Stories. "Entonces, cuando me enteré de mi vigilancia, todo esto tuvo sentido".

Plenel dijo que el ataque de su teléfono y el de otro periodista de Mediapart, Lenaig Bredoux, con Pegasus era probablemente un "Caballo de Troya dirigido a nuestros colegas marroquíes".

Al igual que Mansouri, muchos periodistas marroquíes han huido del país o han dejado de hacer periodismo por completo. El periódico de Raissouni y Bouachrine, Akhbar al-Yaoum, agobiado por sus arrestos consecutivos y la presión financiera, dejó de publicar en marzo de 2021.
"Había espacio para la libertad de expresión en Marruecos hace unos 10 o 15 años", dijo Benchemsi. "No hay más. Se acabó. Sobrevivir hoy significa internalizar un alto nivel de autocensura, a menos que se apoye a las autoridades, por supuesto ".

¿Un arma mortal?

En el informe de transparencia de 2021 de NSO Group, una frase aparece tres veces: "salvar vidas". "Nuestro objetivo", escribe la empresa en un momento, "es ayudar a los estados a proteger a sus ciudadanos y salvar vidas". Sin embargo, el uso preocupante del software espía NSO contra periodistas y sus familiares, como se identifica en el Proyecto Pegasus y en informes anteriores de ONG de derechos digitales, arroja dudas sobre esta narrativa.

El 2 de octubre de 2018, alrededor de la 1 pm, el columnista del Washington Post, Jamal Khashoggi, entró al consulado saudí en Turquía y nunca volvió a salir. El descarado asesinato del periodista disidente inició una ola de respuestas globales, con líderes mundiales, grupos de derechos humanos y ciudadanos preocupados pidiendo una investigación en profundidad sobre su asesinato y la posible implicación del software espía de NSO Group en él.

Dos semanas después de su asesinato, la organización de derechos digitales Citizen Lab informó que un amigo cercano de Khashoggi, Omar Abdulaziz, había sido blanco de Pegasus de NSO en los meses previos al asesinato de Khashoggi.

NSO, por su parte, ha dicho en repetidas ocasiones que tiene acceso a un "interruptor automático" y que ha revocado el acceso a los clientes cuando no se respetan los derechos humanos. La empresa ha negado categóricamente cualquier implicación en el asesinato de Khashoggi.

Pero nuevas revelaciones de Forbidden Stories y sus socios han descubierto que el software espía Pegasus se instaló con éxito en el teléfono de la prometida de Khashoggi, Hatice Cengiz, solo cuatro días después del asesinato. El teléfono del hijo de Khashoggi, Abdullah, fue seleccionado como objetivo de un cliente de NSO que parece ser el gobierno de los Emiratos Árabes Unidos, según el análisis del consorcio de los datos filtrados, varias semanas después del asesinato. Los amigos cercanos, colegas y familiares del periodista asesinado fueron seleccionados como objetivos por clientes de NSO que parecen ser los gobiernos de Arabia Saudita y los Emiratos Árabes Unidos, según las revelaciones del Proyecto Pegasus publicadas hoy.

"Como ha dicho NSO anteriormente, nuestra tecnología no se asoció de ninguna manera con el atroz asesinato de Jamal Khashoggi", escribió NSO Group en su carta a Forbidden Stories. "Podemos confirmar que nuestra tecnología no se utilizó para escuchar, monitorear, rastrear o recopilar información sobre él o los miembros de su familia mencionados en su consulta".

La muerte de Khashoggi y el software espía que persiste en sus márgenes, dicen los expertos en seguridad, no fue necesariamente un caso único.

“(Khashoggi) ciertamente no es el primer periodista asesinado por un gobierno enojado. Y no es el primer periodista asesinado por un gobierno enojado por su periodismo con algún elemento de malware y vigilancia involucrado ”, dijo Galperin, de EFF. “Estas son cosas que con mucha frecuencia van juntas”.

El 2 de marzo de 2017, el periodista mexicano local Cecilio Pineda sacó su teléfono y grabó su última transmisión. En él, el reportero de la ciudad de Altamirano, quien dirigió un Facebook con más de 50.000 seguidores, habló sobre una supuesta colusión entre policías estatales y locales y el líder de un cartel de la droga.

Dos horas después, estaba muerto: dos hombres en una motocicleta le dispararon al menos seis veces mientras yacía en una hamaca afuera de un lavado de autos.

Cuando Pineda fue asesinada en 2017, a la edad de 38 años, el mundo parpadeó y siguió adelante. Su muerte fue vista como un reportero más asesinado en México, la zona sin conflicto más mortífera del mundo para ser periodista. Pero la muerte de Pineda pudo haber sido más que un trabajo de un cártel local, según los registros a los que tuvieron acceso Forbidden Stories y sus socios.

Solo unas semanas antes de su muerte, el teléfono celular del trabajo de Pineda fue seleccionado como objetivo de un cliente de NSO en México.

Forbidden Stories ha podido confirmar que no solo Pineda, sino también el fiscal estatal que investigó el caso, Xavier Olea Peláez, fueron seleccionados como objetivos de Pegasus en las semanas y meses previos a su asesinato. Forbidden Stories no pudo analizar el teléfono de Pineda porque desapareció inmediatamente después de su muerte. Peláez no guardó su teléfono de la hora, por lo que no fue posible confirmar una infección por Pegasus.

Sin embargo, el informe de Pineda da pistas de por qué el trabajo de Pineda pudo haber preocupado a las autoridades mexicanas que pudieron haber tenido acceso a esta tecnología. Al momento de su selección, Pineda estaba investigando los vínculos entre el jefe del crimen local, conocido como El Tequilero, y el gobernador de Guerrero, Héctor Astudillo. Amigos y familiares que hablaron con Forbidden Stories y sus socios dijeron que Pineda había recibido amenazas y había pedido ser colocado en un mecanismo federal para la protección de periodistas.

“Cecilio recibió muchas amenazas graves, pero las minimizó”, dijo Israel Flores, un amigo de Pineda, en una entrevista reciente. “Él siempre decía ‘no pasará nada’”.

A medida que Pineda continuaba informando sobre el nexo de políticos locales y narcotraficantes, las amenazas se acercaban cada vez más a él. Unos días antes de su muerte, hombres en un automóvil blanco tomaron fotos de su casa, dijo su madre.

El día que lo mataron, pasó por la casa de su madre antes de encontrarse con un amigo en un mitin político. Esa fue la última vez que lo vio.

"Me dijo 'los malos no me van a matar, me conocen, son mis amigos. Si me matan será el gobierno ", dijo su madre en una entrevista.

La esposa de Pineda, Marisol Toledo, le dijo a un miembro del consorcio Forbidden Stories que al día siguiente de la muerte de Pineda recibió una llamada de un empleado del gobierno que le dijo que estaba investigando el asesinato. Nunca dio seguimiento.

"No sabemos qué pasó en la investigación", dijo Toledo. "No queremos problemas. Las personas con poder pueden hacer lo que quieran, a quienes quieran ".

El teléfono de Pineda tampoco fue encontrado nunca, ya que había desaparecido de la escena del crimen cuando llegaron las autoridades. Pero cuando se le informó sobre el posible papel del software espía en el seguimiento de los movimientos de Pineda, Toledo no se sorprendió.

"Si tenían éxito, habrían sabido dónde estaba en todo momento", dijo.

Fuente:

https://aristeguinoticias.com/1907/mexico/pegasus-project-la-nueva-arma-para-silenciar-a-los-periodistas/

Gobierno Espía a activistas, defensores de derechos humanos y periodistas en México

Ciudad de México, 19 de junio de 2017.- El día de hoy fue publicada por Citizen Lab[1] y por las organizaciones ARTICLE 19 Oficina para México y Centroamérica, R3D: Red en Defensa de los Derechos Digitales y SocialTIC[2] una nueva investigación, recogida por el diario The 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:

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.

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.

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.

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.

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..

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.

Descarga (y lee) el informe #GobiernoEspía: Vigilancia sistemática a periodistas y defensores de derechos humanos en formato PDF en este enlace.

https://articulo19.org/wp-content/uploads/2017/06/Reporte-Gobierno-Espia-Final.pdf

Referencias:

[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/

[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/

Fuente:

https://articulo19.org/gobiernoespia/

About The Pegasus Project

An unprecedented leak of more than 50,000 phone numbers selected for surveillance by the customers of the israeli company NSO Group shows how this technology has been systematically abused for years. The Forbidden Stories consortium and Amnesty International had access to records of phone numbers selected by NSO clients in more than 50 countries since 2016.

NSO Group asserts that the product it sells to government clients - most commonly referred to as Pegasus - is intended to "collect data from the mobile devices of specific individuals, suspected to be involved in serious crime and terror." Pegasus has extensive capabilities: the spyware can be installed remotely on a smartphone without requiring any action from its owner. Once installed, it allows clients to take complete control of the device, including accessing messages from encrypted messaging apps like WhatsApp and Signal, and turning on the microphone and camera.

The Forbidden Stories consortium discovered that, contrary to what NSO Group has claimed for many years, including in a recent transparency report, this spyware has been widely misused. The leaked data showed that at least 180 journalists have been selected as targets in countries like India, Mexico, Hungary, Morocco and France, among others. Potential targets also include human rights defenders, academics, businesspeople, lawyers, doctors, union leaders, diplomats, politicians and several heads of states.

In a letter shared with Forbidden Stories and its partners, NSO Group contended that the consortium's reporting was based on "wrong assumptions" and "uncorroborated theories." NSO Group insisted that the analysis of the data by journalists who were part of the Pegasus Project relied on a "misleading interpretation of leaked data from accessible and overt basic information, such as HLR Lookup services, which have no bearing on the list of the customers targets of Pegasus or any other NSO products."

HLR refers to Home Location Register - a database that is essential to operating cellular phone networks. A person with direct knowledge of NSO's systems, speaking on the condition of anonymity, told journalists from the Pegasus Project that an HLR lookup is a key step of determining certain characteristics of a phone, such as whether it is turned on or in a country that allows Pegasus targeting.

Asked about those findings by Forbidden Stories, NSO Group denied and said "it will continue to investigate all credible claims of misuse and take appropriate action based on the results of these investigations."

The consortium met with victims from all over the world whose phone numbers appeared in the data. The forensic analyses of their phones - conducted by Amnesty International's Security Lab and peer-reviewed by the Canadian organization Citizen Lab - was able to confirm an infection or attempted infection with NSO Group's spyware in 85% of cases, or 37 in total. Such a rate is remarkably high given the state-of-the-art spyware is supposed to be undetectable on the device in compromises.

Journalists from the Pegasus Project - more than 80 reporters from 17 media organizations in 10 countries coordinated by Forbidden Stories with the technical support of Amnesty International's Security Lab - sifted through these records of phone numbers and were able to take a peak behind the curtain of this surveillance weapon, which had never been possible to this extent before.

Among the victims were several journalists from the Pegasus Project, such as Siddarth Varadarajan, an Indian investigative journalist and founder of the news site The Wire, who was hacked in 2018 and Szabolcs Panyi, an investigative reporter for Direkt36 in Hungary whose phone was compromised during a seven-month period in 2019.

All shared a general sense of powerlessness when informed about the cyber attacks they had suffered. "We've been recommending each other this tool or that tool, how to keep [our phones] more and more secure from the eyes of the government," Azerbaijani journalist Khadija Ismayilova said. "And yesterday I realized that there is no way. Unless you lock yourself in [an] iron tent, there is no way that they will not interfere into your communications."

Amnesty International's Security Lab also identified new ways through which Pegasus can be installed on a phone, such as through a security flaw in iPhones that has been frequently

used since 2019 and was still detected as recently as in July 2021. Well-informed sources shared concerns about countless vulnerabilities linked to Apple's messaging service iMessage, a problem they say has gotten worse over the years.

The leaked data suggests that the spyware is used much more carelessly than advertised. In the transparency report published in June 2021, the Israeli company stressed that Pegasus was "not a mass surveillance technology" and was "used only where there [was] a legitimate law enforcement or intelligence-driven reason." Yet, more than 10,000 phone numbers were selected for surveillance by NSO Group's Moroccan client alone over a two-year period.

The project shines a harsh light on the business of NSO Group, which, despite claiming it vets its clients based on their human rights track records, decided to sell its product to authoritarian regimes such as Azerbaijan, the United Arab Emirates and Saudi Arabia. Insiders disclosed the important role played by the Israeli Ministry of Defense when it came to picking NSO Group's clients. Multiple sources corroborated the fact that Israeli authorities pushed for Saudi Arabia to be added to the list of customers despite NSO Group's hesitations. The company's lawyer denied "NSO Group takes governmental direction regarding customers."

The revelations stemming from this international collaborative investigation throw into question the safeguards put in place to prevent misuse of cyber weapons like Pegasus and, more specifically, NSO Group's commitment to creating "a better, safer world."

Fuente:

https://forbiddenstories.org/about-the-pegasus-project/

Más:

https://forbiddenstories.org/

https://forbiddenstories.org/pegasus-project-articles/

Pegasus Project | Familiares de los 43 normalistas de Ayotzinapa, en la lista de objetivos de espionaje con Pegasus

La nueva investigación arroja que familiares de los 43 estudiantes desaparecidos, sus defensores e incluso autoridades investigadoras del caso, fueron seleccionados como objetivos de espionaje en el sexenio de Enrique Peña Nieto.

Las familias de los 43 estudiantes de la escuela normal rural Isidro Burgos de Ayotzinapa, desaparecidos la noche del 26 y la madrugada del 27 de septiembre de 2014, fueron seleccionadas como objetivo de espionaje por parte de los clientes mexicanos de la empresa de cibervigilancia israelí NSO Group, creadora del programa Pegasus.

Así lo revela este domingo una nueva investigación de la organización francesa Forbidden Stories, con la colaboración de 80 periodistas pertenecientes a 17 medios -entre ellos Aristegui Noticias- de 10 países y el apoyo técnico del Security Lab de Amnistía Internacional.

Si bien Citizen Lab había documentado cómo defensores de derechos humanos e investigadores implicados en el caso, fueron objetivo de los clientes mexicanos de la empresa NSO Group, creadora de Pegasus, ahora se sabe de manera fehaciente que las familias de los normalistas también estuvieron en la mira.

Fue tras el 'carpetazo' que el gobierno de Enrique Peña Nieto le dio al caso en 2015, con la instauración de la llamada 'verdad histórica' que limitaba la responsabilidad de la desaparición de los estudiantes al alcalde de Iguala, José Luis Abarca, a su esposa, María de los Ángeles Pineda y al cártel Guerreros Unidos. Ello, sin tomar en consideración las evidencias que apuntaban al involucramiento de las fuerzas estatales, federales y el Ejército en los hechos, ya sea por acciones directas u omisiones deliberadas.

La versión del entonces procurador Jesús Murillo Karam, era que el cártel había incinerado a los estudiantes en el basurero de Cocula, lo que se demostró falso, de acuerdo con las investigaciones que demostraron la manipulación de las indagatorias y la obtención de confesiones bajo tortura.

Con la información aportada por Pegasus Project, como se denomina esta investigación periodística de alcance internacional, se puede afirmar que tres familiares de los normalistas estuvieron dentro de la lista de objetivos mexicanos de uno de los clientes de NSO Group, compañía que solo vende su software a gobiernos.

Se trata de Melitón Ortega, tío del estudiante Mauricio Valerio; Cristina Bautista, madre de Benjamín Ascencio, y Felipe de la Cruz, padre de uno de los sobrevivientes de la masacre, y vocero de los padres hasta finales de enero de 2021, cuando se registró por una diputación plurinominal por el Movimiento de Regeneración Nacional (Morena).

En el caso de Melitón Ortega, que desde principios de febrero hasta finales de mayo de 2017 fue sometido a varios intentos de intromisión por parte del 'malware' Pegasus, sospechaba que era espiado por las autoridades mexicanas.

De acuerdo con el reporte del periodista Mathieu Tourliere en la revista Proceso, "escuchaba ruidos extraños y voces mientras estaba en llamadas telefónicas, y asumía que el gobierno lo espiaba".

"Son absolutamente capaces de esto; yo soy un organizador, mi papel es comunicarme con diversas organizaciones e instituciones estatales y federales; entonces me hace sentido que me hayan atacado", mencionó en una entrevista que forma parte de los testimonios recopilados por Pegasus Project.

A Cristina Bautista, una de las madres más activas en el movimiento de búsqueda de los estudiantes desaparecidos, se le enviaron mensajes infecciosos en marzo de 2017. Sucedió en las semanas previas a la visita a México de los integrantes de la Comisión Interamericana de los Derechos Humanos (CIDH), en la que denunciaron que a esa fecha aún no había sido procesada ninguna persona por desaparición forzada en el contexto de la investigación y no se había presentado ninguna nueva acusación al respecto.

Bautista, quien estuvo presente en la sesión de la CIDH, dijo entonces que existía una intención del gobierno federal por encubrir la participación del Ejército y que el 19 de enero

de 2015 la entonces Procuraduría General de la República (PGR) intentó cerrar el caso con la versión del basurero de Cocula. "Y con pruebas científicas les dijimos que nuestros hijos no fueron calcinados en el basurero. Se derrumbó su verdad histórica", comentó, según el periódico El Sur.

De acuerdo con las revelaciones del Pegasus Project, en las que participa el Proyecto de Reportería sobre Crimen Organizado y Corrupción (OCCRP), a Felipe de la Cruz se le ubicó como objetivo entre marzo y mayo de 2017, con varios intentos infecciosos documentados.

En 2017, Citizen Lab de la Universidad de Toronto, reveló que miembros del Centro de Derechos Humanos "Miguel Agustín Pro Juárez" -también conocido como Centro Prodh- fueron espiados con el software Pegasus a partir de su participación en las indagatorias de la desaparición de los 43 estudiantes de Ayotzinapa.

Mario Patrón, Stephanie Brewer y Santiago Aguirre recibieron mensajes en sus dispositivos con el fin de infectarlos. También los recibieron miembros del Grupo Interdisciplinario de Expertos Independientes (GIEI), así como periodistas, políticos y miembros de organizaciones civiles.

Ahora, Pegasus Project confirma que Vidulfo Rosales, abogado de los normalistas y miembro del Centro de Derechos Humanos de la Montaña Tlachinollan, también fue objeto de intentos de intromisiones desde enero de 2017.

De la misma manera que el antropólogo Abel Barrera, fundador del centro, recibió extraños mensajes en su teléfono desde que se involucró en el caso. "Hemos sido monitoreados, amenazados y nuestros teléfonos han sido interceptados desde 1996, cuando defendimos a un profesor torturado por las fuerzas armadas, que decían que era un guerrillero", mencionó en una entrevista concedida a Pegasus Project, recuperada por Proceso.

La vigilancia sobre Rosales tiene un antecedente en 2016, momento en que algunas de sus conversaciones telefónicas fueron filtradas a la prensa con el objeto de sembrar la división en el movimiento. Llama la atención que los intentos de intervención al abogado mediante Pegasus en 2017, se realizaron en los mismos horarios y fechas que los intentos contra Cristina Bautista, lo que configura un escenario de seguimiento del movimiento de los padres y sus defensores.

Además, el Pegasus Project pudo verificar de forma independiente que un investigador del GIEI también estuvo en la lista de objetivos del programa de cibervigilancia. Este grupo evidenció desde 2015 las contradicciones e irregularidades en la investigación hecha por el gobierno de Peña Nieto. CitizenLab había revelado intentos de intromisión en marzo de ese año; la investigación publicada este domingo documentó otro intento en junio, que no parece haber funcionado, al no ser un teléfono inteligente o 'smartphone', detalla Forbidden Stories.

Incluso apareció el exguerrillero y activista David Cabañas Barrientos, hermano de Lucio Cabañas -quizá el alumno más destacado de la escuela normal de Ayotzinapa-, quien fue asesinado por el Ejército en 1974.

De la misma forma, el exprocurador de Guerrero, Iñaki Blanco Cabrera, está en la base de datos con cinco selecciones como objetivo entre el 11 de abril y el 18 de mayo de 2017. También el que fuera primer fiscal del estado, Miguel Ángel Godínez Muñoz, así como el que fuera fiscal federal encargado del caso, Alfredo Higuera Bernal.

La nueva investigación muestra que, para tratar de tomarle el pulso a las investigaciones sobre la desaparición de los 43 estudiantes normalistas, no se escatimaron esfuerzos ni se hicieron distinciones entre objetivos.

De acuerdo con Proceso, el gobierno mexicano intentó espiar en junio de 2016 a Emilio Álvarez Icaza, quien había dejado la secretaría ejecutiva de la CIDH y fundado en el país el movimiento político Ahora. También detalla que en abril de 2017 buscó intervenir los teléfonos celulares de Israel Núñez Delgadillo y Eduardo Navarro Padilla, líderes del Sindicato Mexicano de Electricistas (SME) y del Frente Popular Francisco Villa México Siglo XXI, organizaciones que han apoyado la lucha de los padres de Ayotzinapa.

¿Quién fue el cliente de NSO Group interesado en seguir a detalle a familiares de los 43 estudiantes desaparecidos, a sus defensores y hasta las autoridades que investigaban el caso? En 2016 se publicó un contrato entre la entonces PGR y la empresa Tech Bull por 32 millones de dólares para usarlo contra 500 objetivos.

Un año después, Aristegui Noticias reveló que la PGR, el Centro de Investigación y Seguridad Nacional (Cisen) y el Ejército mexicano pagaron 489 millones de pesos a una sola empresa para actualizar el sistema Pegasus y escalar sus capacidades de espionaje.

Los comprobantes fiscales en poder de este medio confirmaron que además de la Procuraduría, el Cisen y la Sedena también tuvieron acceso a la plataforma de espionaje, utilizada en todo el mundo para atacar a periodistas, activistas anticorrupción y defensores de derechos humanos.

Fuente:

https:// aristeguinoticias . com/1807/mexico/pegasus-project-familiares-de-los-43-normalistas-de-ayotzinapa-en-la-lista-de-objetivos-del-programa-de-espionaje-pegasus/

Presentan plataforma sobre espionaje con Pegasus en el mundo; investigación nació en México

La plataforma "Violencia Digital" es una iniciativa de Forensic Architecture, con el apoyo de Amnistía Internacional y The Citizen Lab, para dar a conocer toda la información que existe hasta el momento sobre el malware Pegasus.

Así fue la presentación de la nueva investigación de Forensic Architecture, con el apoyo de Amnistía Internacional, Citizen Lab y Laura Poitras, que ofrece por primera vez un mapa de la totalidad de las infecciones conocidas en todo el mundo por el malware 'Pegasus', creado por la empresa de cibervigilancia NSO Group.

La organización internacional Forensic Architecture (FA) dio a conocer este sábado la plataforma "Violencia Digital", que reúne toda la información hasta ahora conocida sobre las intromisiones ilegítimas que en todo el mundo se hicieron con el malware 'Pegasus', creado por la empresa de cibervigilancia israelí NSO Group.

En un acto que fue difundido en vivo por internet y que tuvo como sede física la ciudad de Berlín, fue presentado este trabajo global sobre el software que ha infectado los teléfonos de periodistas y defensores de derechos humanos de todo el mundo.

La plataforma "Violencia Digital", creada por FA con el apoyo de Amnistía Internacional y The Citizen Lab, tiene como antecedente un informe de 2017 que esta última organización realizó en México.

Aquella investigación reveló que miembros del Centro de Derechos Humanos "Miguel Agustín Pro Juárez" -también conocido como Centro Prodh- fueron espiados con el software

Pegasus a partir de su participación en las indagatorias de la desaparición de los 43 estudiantes de la Escuela Normal Rural "Isidro Burgos" de Ayotzinapa, la noche del 26 y la madrugada del 27 de septiembre de 2014 en Iguala, Guerrero.

Forensic Architecture, que junto con el Centro Prodh y el Equipo Argentino de Antropología Forense realizaron una herramienta cartográfica en línea para analizar las versiones contradictorias de las autoridades sobre estos hechos, ocurridos durante el gobierno de Enrique Peña Nieto, descubrió en 2019 que sus miembros también eran espiados. Entonces, FA participaba en una demanda contra NSO Group en nombre de varios defensores de derechos humanos.

Por esta razón, comenzaron a trabajar en una plataforma que exhibiera en un solo lugar todas las actividades documentadas de NSO en todo el mundo. El malware Pegasus, detectado por primera vez por Citizen Lab, se ha utilizado por lo menos desde 2015, en alrededor de 45 países de todo el mundo, para espiar los teléfonos de activistas, periodistas y defensores de los derechos humanos.

La empresa aún recibe licencias de exportación por parte del Ministerio de Defensa de Israel para vender este software de espionaje, pese a haber sido impugnado en tribunales israelíes e internacionales.

El proyecto "Violencia Digital" consta de una plataforma digital navegable en la que se pueden consultar todas las infecciones reportadas hasta la fecha por Pegasus. Además, cruza esta información con la violencia en el mundo físico (allanamientos, acoso, intimidación y asesinato) contra muchos de los objetivos de las intromisiones.

La cineasta Laura Poitras realizó un cortometraje en el que las víctimas de Pegasus en todo el mundo cuentan su historia y muestran los efectos psicológicos tras haber sido intervenidas sus comunicaciones, además de las intimidaciones y el acoso contra ellos, sus familias y colegas.

Poitras es conocida por la realización del documental Citizenfour (2014) sobre el ex analista de la Agencia Central de Inteligencia de Estados Unidos (CIA), Edward Snowden, quien denunció las prácticas ilegales de vigilancia de la Agencia de Seguridad Nacional (NSA) estadounidense.

Durante la presentación de la plataforma "Violencia Digital", la directora de cine señaló que buscó mostrar el daño causado por la experiencia de "sentirse cazado, de que tu familia sea violentada, tus amistades, tu comunidad". Además destacó el trabajo realizado por el músico y activista inglés Brian Eno, quien compuso la banda sonora del corto.

La plataforma también cuenta con un diagrama interactivo y un video que presenta nuevas investigaciones sobre el entramado corporativo de NSO Group. Mediante informes de Amnistía Internacional, investigaciones de código abierto y documentos filtrados, se revela

cómo la inversión privada permite la proliferación de la vigilancia digital, que probablemente incluye la venta de software espía de fabricación israelí a varios países como Arabia Saudita, los Emiratos Árabes Unidos y los Estados Unidos.

Las investigaciones del video están narradas por Edward Snowden, presidente de la Fundación para la Libertad de Prensa, quien participó este sábado en el lanzamiento de la plataforma.

Durante su intervención desde Moscú -donde se encuentra exiliado-, Snowden señaló que el público en general no entiende bien las implicaciones de que un teléfono celular o un dispositivo electrónico sea 'hackeado', ni entiende cómo todos estamos conectados con todos mediante Internet.

Aseguró que si bien internet es una herramienta que podría cerrar brechas entre personas que hablan idiomas distintos, con malwares como Pegasus se rompen estas posibilidades. Las herramientas de espionaje que vende NSO Group, dijo, significan la depredación de nuestro tejido social global, por lo que la plataforma de FA revela la historia más importante, que no se estaba contando.

Los datos que alimentan la plataforma "Violencia Digital" fueron obtenidos tras 15 meses de investigación y revisión de documentación disponible sobre Pegasus.

Eyal Weizman, director de Forensic Architecture, mencionó que en el caso de NSO/Pegasus, la plataforma muestra cómo la violencia digital se traduce en violencia física. Aseveró que así como Israel pretende dominar al pueblo palestino con su poderío armamentístico, Pegasus es la traducción de este espíritu de dominación en el espacio digital.

Relató que el interés de FA por NSO Group comenzó en México, a raíz de su participación en las investigaciones del caso Ayotzinapa, cuando el Centro Prodh les avisó que el gobierno de Peña Nieto los espiaba. "¿Qué pasa cuando los investigadores están siendo investigados?", se preguntó entonces.

"Y nos dimos cuenta que lo que hacía falta era reunir todas las experiencias y mostrar al público una imagen de cómo la violencia digital se puede representar. Hilvanar cómo se relaciona la infección de una persona en un país con la experiencia de violencia de otra persona en otro país. Esta investigación se trata de eso: de las relaciones entre las diversas personas que han sufrido esta violencia digital", comentó.

En el caso de la periodista Carmen Aristegui, el espionaje con Pegasus comenzó tras la difusión del reportaje "La Casa Blanca de Enrique Peña Nieto", que en 2014 mostró como el entonces presidente mexicano adquirió una casa en Lomas de Chapultepec valuada en 7 millones de dólares.

La mansión fue construida a su gusto y de su entonces esposa Angélica Rivera, por Grupo Higa, una de las empresas que ganó la licitación del tren México-Querétaro (hoy revocada) y levantó obras importantes en el Estado de México cuando él fue gobernador en dicha entidad.

No solo se espió a Carmen Aristegui, sino a su hijo Emilio, que entonces era menor de edad, así como a los periodistas que participaron en el reportaje: Sebastián Barragán, Daniel Lizárraga, Rafael Cabrera y quien era entonces coordinador de información del noticiario, Salvador Camarena.

En un mensaje durante el acto de lanzamiento de la plataforma, Aristegui mencionó que aún no se conoce el tamaño real que alcanzó el espionaje con Pegasus en México. "La investigación de 2017 mostró cómo el gobierno mexicano dinamitó la intimidad y la privacidad de todos nosotros [...] El gobierno mexicano se atrevió a espiar a ciudadanos mexicanos, extranjeros y hasta mi hijo Emilio que era menor de edad", comentó.

"Lo que hoy se presenta nos ayuda a saber más y a exigir más a las democracias del mundo, cuando hacen uso de la tecnología para atacar a los ciudadanos", enfatizó.

El proyecto "Violencia Digital" destaca que las infecciones digitales de grupos de la sociedad civil ocurren junto con otras formas de violencia experimentadas en el mundo físico. La cibervigilancia está constantemente enredada con un espectro de violaciones físicas, que incluyen allanamientos, intimidación, asaltos, arrestos, demandas, campañas de difamación, y asesinatos, como ocurrió en 2018 con el periodista saudí Jamal Khashoggi, cuyos amigos y colegas fueron atacados por Pegasus.

En la presentación ofrecieron su testimonios otras personas espiadas con Pegasus, como Yahya Assiri, activista de Arabia Saudita y ex miembro de la Real Fuerza Aérea de ese país, quien comentó que "la tecnología nos amenaza constantemente" y que no solo se trata de hackeo y robo de información, sino de poner vidas en riesgo permanente.

Por su parte, Danna Ingleton, de Amnistía Internacional, destacó la importancia de revelar la estructura corporativa de la empresa NSO Group, para explicar cómo se facilita que existan herramientas de espionaje como Pegasus.

Fuente:

https://aristeguinoticias.com/0307/mundo/presentan-plataforma-sobre-espionaje-con-pegasus-en-el-mundo-investigacion-nacio-en-mexico/

https://digitalviolence.org/#/

Espionaje de periodistas mexicanos: una investigación sobre el rentable negocio del ciberespionaje

A pesar de los sucesivos escándalos, la industria mundial de la cibervigilancia, apoyada por algunos intermediarios con muy buenos contactos, sigue proporcionando a México tecnologías cada vez más invasivas. Varios periodistas han sido blanco de estos instrumentos, sin que ningún responsable mexicano haya sido cuestionado. Veracruz, estado que cuenta con el mayor número de periodistas asesinados, incluso Regina Martínez, hasta instauró una unidad de espionaje ultraequipada, que tenía en la mira a esta profesión.

El mensaje pasó inadvertido, pero oculta una operación de vigilancia de muy alto nivel, con tecnología de punta. O, al menos, ese era el plan. En la primavera de 2016, el periodista mexicano Jorge Carrasco acaba de pasar varios meses investigando los Panama Papers para la revista Proceso. Estando en plena faena, investigando a los clientes mexicanos del tristemente célebre bufete panameño Mossack Fonseca, recibe un mensaje de texto de un número desconocido: "Buena tarde Jorge, paso a compartirte la nota que publica hoy Animal Político y parece importante retomar". Y el mensaje viene con un enlace. "¿Quién eres?", pregunta el periodista. El emisor no responderá jamás.

¿Qué hay tras este misterio?: se trataría de una tentativa de intromisión del programa informático espía Pegasus, vendido por la sociedad israelí NSO Group a varios clientes

miembros del gobierno mexicano. Es lo que concluyó el análisis técnico realizado por el equipo de especialistas de seguridad digital de Amnistía Internacional, en colaboración con Forbidden Stories. Este enlace, si se hace clic en él, permite instalar un software invisible que capta todos los datos del teléfono, particularmente los mensajes de texto, y permite activar a distancia su micrófono y su cámara. Un atentado temible contra un periodista.

"En ese entonces, me había llamado la atención ese mensaje, pero recibía muchos de este estilo", recuerda hoy el periodista, que actualmente es el jefe de redacción de la revista Proceso.

"Probablemente, el mensaje formaba parte de una campaña en curso en México durante este periodo", considera Claudio Guarnieri, de Amnesty Security Lab. En ese momento, el programa informático es utilizado ampliamente por los clientes mexicanos. Según Amnistía, el número de teléfono que apuntaló a Jorge Carrasco envió también, durante el mismo periodo, mensajes de texto con enlaces maliciosos a Carmen Aristegui, una de las más famosas periodistas de investigación en México. Tras este enlace, un nombre de dominio. Éste será utilizado, de igual forma, en 2017, para vulnerar, con el mismo programa informático, a varios defensores de un impuesto sobre las bebidas azucaradas.

"La selección de las personas a las que querían llegar no sólo era muy amplia, sino que además era a menudo efectuada de forma bastante imprudente, con mensajes alarmantes y molestos cuyo objetivo era provocar una reacción por parte de los blancos del software malicioso", explica John Scott-Railton de Citizen Lab, una organización que investiga, desde hace varios años, los ataques de este programa informático.

Jorge Carrasco se agrega a la lista de nueve periodistas en cuyos teléfonos encontraron rastros de un ataque del programa espía Pegasus en México. Desde hace 10 años, el país es un gran importador de tecnologías de vigilancia, pese a los sucesivos escándalos respecto al uso de esas herramientas contra periodistas y activistas. A pesar de las promesas del gobierno, no se hizo nada para regular su uso, ningún operador de los que previamente utilizó las herramientas fue llevado ante la justicia, y el país sigue importando softwares intrusivos que adquieren en empresas extranjeras.

Atraídos por la tecnología israelí

Según un alto responsable de la DEA, la agencia antidroga estadounidense, unas 20 empresas privadas de software de espionaje vendieron sus programas a varios servicios de policía federales y de estados mexicanos. "Pareciera que, en un momento dado, casi todas las tecnologías disponibles se presentaron en México, se hicieron demostraciones con ellas y/o fueron utilizadas", explica John Scott-Railton.

Las tecnologías israelíes tienen una reputación particularmente buena entre los responsables mexicanos. "En México es común en la comunidad de seguridad e inteligencia considerar que Israel posee las tecnologías más avanzadas y las mejores técnicas de

adiestramiento civil y militar", explica Paloma Mendoza Cortés, analista y consultora en asuntos de seguridad nacional.

México, por lo demás, ha sido desde hace tiempo uno de los más importantes clientes de NSO. Tras una primera fase de prueba con la Secretaría de la Defensa Nacional, la empresa israelí se implantó definitivamente en el mercado en 2014, firmando un contrato de 32 millones de dólares con el despacho del procurador general. En los correos electrónicos de su competidor italiano, Hacking Team, que fueron masivamente pirateados y difundidos en 2015, se lee, entre líneas, cómo NSO se volvió poderoso en esa época. Para los vendedores italianos, se trata entonces de "derribar el mito NSO" ante los clientes mexicanos fascinados por esta tecnología que promete un acceso total a los teléfonos captados.

Según un experto en seguridad, Gadi Evron, las empresas israelíes ofrecen un abanico de herramientas: abarcan desde la vulneración de los programas informáticos hasta un servicio, llave en mano, donde el cliente simplemente transmite un número de teléfono o una dirección de correo electrónico y recibe de vuelta todo lo que requiere saber respecto a su objetivo.

NSO impuso su liderazgo en este mercado. "Somos como un fantasma", se vanagloriaba el cofundador de dicha empresa, Omri Lavie, en 2013. "Somos totalmente invisibles para el blanco, y no dejamos ningún rastro". El producto estrella de la empresa, Pegasus, infecta los teléfonos de sus objetivos mediante mensajes de texto maliciosos como el que recibió Jorge Carrasco. Sin embargo, alrededor de 2018, la empresa busca métodos más discretos para infectar teléfonos. "Los mensajes de texto son muy visibles y dejan muchas huellas, a las que los investigadores recurrieron, una y otra vez, para confirmar que habían sido víctimas de un ataque NSO", explica Claudio Guarnieri. En 2019, se supo que la empresa israelí utiliza, desde entonces, una falla de seguridad de la aplicación WhatsApp. Actualmente no se necesita ninguna reacción del usuario, porque simplemente redirecciona el tráfico de su web en una fracción de segundo. Una vez que el ataque se ha llevado a cabo exitosamente, el cliente puede aspirar todos los datos del teléfono de su blanco, puede ver todo.

"Pienso que los problemas de abusos probablemente han aumentado en el mundo entero, pero es más difícil dar con ellos", lamenta John Scott-Railton. "Como NSO y otros tienden a optar por la venta de tecnologías 'cero-clic' que no dependen de un mensaje de texto, estamos en una situación que dificulta más investigar al respecto".

Esta poderosa herramienta, supuestamente creada para combatir el terrorismo y el crimen organizado, puede volverse muy peligrosa si se usa contra periodistas, opositores o activistas. "Gracias al desarrollo de esta tecnología, se puede identificar, en varios lugares, quién es el próximo Nelson Mandela antes de que él mismo sepa que es el próximo Nelson Mandela", explica Eitay Mack, un abogado israelí de derechos humanos. Pero el público en general difícilmente percibe estas herramientas de vigilancia como algo tan amenazante como las armas. "Un arma representa algo malo, algo peligroso", explica el abogado. "Pero un

sistema de vigilancia es más difícil de comprender, es algo que no se puede ver".

En una respuesta escrita a Forbidden Stories, NSO declaró que "investiga totalmente todas las denuncias creíbles de uso abusivo, incluidas las afirmaciones de que [su] tecnología se ha utilizado para fines distintos de la prevención e investigación legítimas del terrorismo u otros delitos".

Respecto a las autoridades israelíes, a pesar de las sucesivas denuncias del uso de Pegasus contra miembros de la sociedad civil, no justifican sancionar a NSO, cuya licencia de exportación sigue siendo renovada. "Para el gobierno israelí, vigilar a los periodistas y activistas es algo que simplemente se hace", constata Eitay Mack.

"Cuando se evalúa una licencia, se toman en consideración diversos aspectos, en particular la evaluación del país donde será comercializado el producto", respondió a Forbidden Stories un vocero del Ministerio de Defensa de Israel. "Los derechos humanos, la política y los asuntos de seguridad son tomados en cuenta, absolutamente todos".

Según un ex empleado de Hacking Team, el objetivo original de la industria de la cibervigilancia era combatir la criminalidad, pero con el paso del tiempo, sus clientes y sus misiones cambiaron. Fue el caso en dicha empresa italiana. "Las grandes agencias de espionaje comenzaron a equiparse para manejar estas operaciones por sí mismas", explica. "Entonces, nos dirigimos a otros segmentos de la clientela, a los países que no tienen herramientas. Poco a poco, cada vez hubo más operaciones realmente al borde del límite... Y casi al final, la mayoría de las operaciones claramente había sobrepasado todos los límites". El exdirector de Hacking Team, David Vincenzetti, fue contactado por Forbidden Stories, pero no quiso contestar nuestras preguntas.

Por otra parte, hay países como México que priorizan la necesidad de tener herramientas para luchar contra organizaciones criminales poderosas. "Los problemas de seguridad en México, y la forma en que son comunicados, son utilizados como excusa para gastar inmensas cantidades de dinero en la adquisición de tecnologías supuestamente usadas para luchar contra el crimen organizado", explica Luis Fernando García, director de la organización de defensa de los derechos digitales, R3D. "Incluso, si, como sabemos, la línea de demarcación entre el crimen organizado y el gobierno no existe en México, o, a menudo, no es muy clara".

Los gobernadores y la colusión con los cárteles

Esta colusión ocurre principalmente en los estados federales, donde algunos funcionarios se vinculan con los carteles que operan en la región. La división de México en numerosos estados es precisamente lo que vuelve a este país tan atractivo para las empresas de cibervigilancia, ya que pueden vender su tecnología, reservada a actores públicos, a muchos clientes.

La estrategia funciona bien. Tomás Zerón, director jefe de la Agencia de Investigación Criminal (AIC) del despacho del procurador, cree en la solución Remote Control System (RCS) de Hacking Team, que permite infectar computadores gracias a archivos maliciosos. Zerón se transforma en embajador del producto ante los estados. "Su idea es ir equipando, paso a paso, en caso de éxito, a cada procurador local del país con RCS", explica un empleado en un mail de 2014.

Luego de los despachos de los procuradores, vienen los ejecutivos locales, e incluso una empresa pública, Pemex, que consigue el programa RCS. "La constitución no les otorga el poder de interceptar las comunicaciones, pero adquirieron herramientas que les permiten justamente hacer eso", explica Luis Fernando García. Para Paloma Mendoza Cortés, la falta de legislación adecuada y de definiciones claras en materia de seguridad, es la que crearía una confusión en el plano jurídico.

Por cierto, las propias empresas de cibervigilancia no siempre saben claramente quienes son los usuarios finales. Por ejemplo, en 2011, durante varios meses, el intermediario mexicano DTXT Corp. se queda con el software RCS sin entregarlo al supuesto cliente: la policía federal. Los empleados de Hacking Team les solicitan una y otra vez que devuelvan firmado el contrato de licencia de usuario, pero no lo consiguen. Un año más tarde, un empleado comentará en una nota general: "Pareciera que es algo que ocurre a menudo en México". El director de DTXT Corp. no respondió las preguntas de Forbidden Stories.

En el estado de Puebla, algunos empleados de la empresa italiana cuentan cómo se llevó a cabo una instalación particularmente sospechosa. "Debían aportar la solución para el cliente, y los llevaron a una casa abandonada, sin ventanas, a dos horas de la ciudad", da testimonio un ex empleado, que manejaba la situación desde lejos. Entonces, uno de los ingenieros de Hacking Team, aterrado, reconoció a un funcionario, Joaquín Arenal Moreno, de quien sospechaba estaba vinculado con el cartel de Los Zetas. "No son cosas que pasaban todos los días, pero ciertamente ocurrían a menudo", cuenta otro empleado de la empresa. "A veces llegaban personas que se presentaban como miembros de los servicios secretos, y nos preguntábamos, '¿pero, quiénes son estas personas?'". En 2017, entrevistado por el New York Times, el gobierno de Puebla negó haber comprado tecnología alguna de Hacking Team.

Un exempleado de la empresa italiana recuerda que el nivel de profesionalismo variaba mucho de un cliente a otro. "Había agencias de alto nivel, estructuradas, que disponían de una sala segura y un auditor en el lugar, que realmente hacía su trabajo", explica. "Pero también había agencias que carecían de todo procedimiento y cualquier persona podía hacer cualquier cosa".

Este escenario no sería una excepción según un alto responsable de la DEA estadounidense que afirma que la policía que posee esta tecnología también la vendería a los cárteles. Efectivamente, los traficantes de drogas parecen particularmente aficionados a este tipo de programas, como lo mostró el juicio del jefe del cártel de Sinaloa, Joaquín

Guzmán Loera. Durante una audición, el que oficiaba como ingeniero para el capo de la droga, reconoció haber comprado "equipos que permitían acceder a las llamadas telefónicas, a internet, a los mensajes texto". Y a los cárteles que no tienen sus propios ingenieros, les queda la alternativa de los funcionarios corruptos que, según la DEA, aceptan atacar a ciertas personas a cambio de sobornos.

"Si la agencia que tenía nuestra tecnología la compartía con un cártel, no podíamos saberlo", se justifica un ex empleado de Hacking Team. "Y si nos enterábamos de situaciones abusivas, lo único que podíamos hacer era no renovarles la licencia, y dejarla expirar. Pero no podíamos detenerla a distancia".

Periodistas vigilados de muy cerca

En el Estado de Veracruz se montó en la década de 1990 una verdadera unidad de espionaje, dirigida por la Secretaría de Seguridad Pública. Se movilizó una larga red de informantes para reunir información sobre supuestos oponentes políticos. La unidad utilizó técnicas de inteligencia tradicionales, incluyendo el mantenimiento de fichas personales de los periodistas, según un funcionario de alto rango que trabajó para los gobernadores de esos años.

Entre 2017 y 2019, la unidad adquirió también tecnología de punta, proveniente de Europa, en particular. Sin embargo, los correos electrónicos de Hacking Team revelan que, ya en 2012, Veracruz tuvo acceso a una versión de prueba de RCS. En 2018, el gobernador anunció el cese de las actividades de espionaje, aunque no se sabe si sería una suspensión o un desmantelamiento permanente.

"Veracruz dispone de una tecnología muy sofisticada en materia de espionaje; no es Pegasus, pero es tan buena como esta", revela una fuente bien situada. "Los analistas de información tienen mucha experiencia, así como la capacidad y la tecnología necesarias para piratear computadores y teléfonos". De esta forma, ellos serían considerados como una de las unidades de espionaje estatales más sofisticadas y competentes del país. La Secretaría de Seguridad Pública del Estado de Veracruz no respondió ninguno de los varios correos electrónicos enviados por Forbidden Stories.

La situación es particularmente peligrosa para los periodistas. En 2012, Regina Martínez, quien estaba investigando a dos gobernadores del estado, Fidel Herrera y Javier Duarte, fue asesinada. Según Reporteros Sin Fronteras, la elección de este último, en 2010, marcó el inicio de una época de terror para los periodistas. Dieciséis fueron asesinados en los años siguientes. Javier Duarte fue finalmente arrestado en Guatemala en 2017, después de seis meses de fuga, por "malversación de fondos, enriquecimiento ilícito y lavado de dinero".

Un amigo de Regina Martínez de esa época, Andrés Timoteo, afirma que ella siempre se sentía vigilada. "Regina escuchaba ruidos en su teléfono, un eco. Pero a todos nos espiaban, eso era parte de nuestra vida diaria". El mismo Andrés Timoteo escapó de

México justo después del asesinato de su amiga, por temor.

En otro estado, un exempleado de la empresa italiana recuerda haber estado presente en el despacho de un gobernador cuando este vigilaba a una periodista. "Estaba orgulloso", comenta.

En 2017, varias organizaciones mexicanas e internacionales se asociaron para publicar el informe "Gobierno Espía". Desde hace un año, investigadores y activistas trabajaban en la identificación de tentativas de infección abusivas cometidas contra periodistas, abogados y militantes anticorrupción. Encontraron más de 80 tentativas de infección efectuadas mediante el programa espía de NSO en México, entre 2015 y 2016.

El país cuenta con el mayor número de casos documentados en el mundo de uso abusivo de este software, con al menos 25 personas vulneradas ilegítimamente, según el grupo de investigación Citizen Lab. Nadie parecía alarmarse en la empresa. "Esto nos hizo preguntarnos si esta firma no otorgaba un trato especial a México, por algún tipo de favoritismo", se cuestiona John Scott-Railton.

Un portavoz de NSO dijo a Forbidden Stories que la empresa había investigado todos los presuntos abusos de su tecnología, añadiendo que "en múltiples casos, NSO [había] rescindido contratos y roto relaciones con clientes después de que se identificaran los abusos", sin nombrar a ningún cliente específico.

Un grupo de expertos de las Naciones Unidas le pide entonces al gobierno mexicano que se comprometa a detener de forma inmediata la vigilancia. "Este compromiso debe incluir el controlar eficazmente los servicios de seguridad y de información para prevenir el uso ilegal de las herramientas de vigilancia del estado", insisten.

La impunidad, todavía y siempre

México promete investigar. Diversas asociaciones se suman a periodistas que han sido blanco de espionaje por parte de Pegasus para presentar una demanda. Desde entonces, nada. El despacho del procurador exige recuperar los teléfonos que fueron objeto de las tentativas de infección para hacer avanzar la investigación. "El análisis del teléfono es particularmente poco concluyente en este tipo de casos, en parte porque Pegasus dispone de atributos que bloquean el análisis técnico", replica John Scott-Railton. "Nosotros subrayamos que la red telefónica, o el registro de la implantación del mismo Pegasus eran más confiables para las pruebas". Por lo demás, las ONG implicadas cuestionan la imparcialidad del despacho del procurador, que debe investigar una tecnología luego de haber sido uno de sus clientes.

"No está claro que el gobierno pueda llevar a cabo una investigación independiente realmente sería", considera David Kaye, relator especial de la ONU sobre libertad de expresión hasta julio de 2020. Contactamos el despacho del procurador, pero respondió

que no se pronunciaba sobre investigaciones en curso.

Por su parte, en 2018, el presidente mexicano Andrés Manuel López Obrador declaró que el gobierno ya no usaba el programa Pegasus. "Desde entonces, no se refirió más al respecto en sus alocuciones cotidianas", lamenta Luis Fernando García. "Y por el momento no se puede comprobar su compromiso real". El presidente mexicano no respondió la larga lista de preguntas enviadas sobre este tema por Forbidden Stories.

Según David Kaye, "estamos en una situación donde debemos suponer que estas herramientas todavía están disponibles para ser utilizadas, y que al gobierno le corresponde demostrar que lo hace dentro del marco del estado de derecho".

Finalmente, predomina un sentimiento de impunidad. Ninguno de los operadores, ni de RCS ni de Pegasus, tuvo que enfrentar a la justicia. "Lo más probable es que usted no sea atrapado", resume Luis Fernando García. "Si lo llegaran a atrapar, es muy poco probable que se abra una investigación judicial. Si se llegara a abrir una investigación judicial, es muy poco probable que usted sea enjuiciado. E, incluso, si llegara a ser enjuiciado, es improbable que las acciones judiciales se mantengan y que sea condenado".

En 2014, Tomás Zerón, el ex director de AIC, era conocido como "el comprador final" de los sistemas de cibervigilancia, especialmente de Pegasus. Hoy lo buscan las autoridades mexicanas por, entre otras causas, malversación de fondos relacionados con tres contratos de adquisición de material de espionaje, entre 2013 y 2014. También lo buscan por falsificar elementos de una investigación sobre la desaparición de 43 estudiantes en el estado de Guerrero en 2014. Previamente, Citizen Lab demostró que un grupo internacional de expertos que estaba investigando este asunto también fue blanco del software Pegasus.

Según el presidente mexicano, actualmente Tomás Zerón se escondería en Israel. "Pienso que claramente Zerón desempeñó un papel clave en facilitar los contratos y garantizar su seguridad, en especial en el caso de las empresas de vigilancia israelíes", explica Luis Fernando García. "Y es una coincidencia interesante que haya escogido como refugio Israel, para escapar de la justicia mexicana".

En tanto, el Ministerio de Relaciones Exteriores de Israel contestó muy brevemente: "Israel recibió una solicitud al respecto y estamos examinando este asunto".

Juego de influencia y de corrupción

Efectivamente, el fugitivo se encontró al centro de un sistema oscuro y muy lucrativo de contratos de cibervigilancia en México. En esta área, la mayoría de los contratos se firman sin licitación alguna y sin la más mínima transparencia, lo que la vuelve un terreno particularmente propicio para la corrupción. "Se ha vuelto un concurso de tráfico de influencias", resume Luis Fernando García. "Las empresas, los intermediarios se pelean entre sí para hacerse amigos del funcionario que toma la decisión de a quién atribuir el

contrato".

Entre éstos, se encuentra Uri Emmanuel Ansbacher, originario de Israel y propietario de numerosas empresas en México. Amigo del director de NSO, Shalev Hulio, sería el intermediario de numerosas empresas de cibervigilancia israelíes. Interrogado por Forbidden Stories, Uri Emmanuel Ansbacher negó todo.

Los intermediarios pueden ser empresas de seguridad privadas mexicanas o empresas fantasmas creadas únicamente para este fin. "Las empresas extranjeras utilizan empresas de seguridad privada mexicanas como intermediarias o crean empresas falsas porque con frecuencia se recurre a la corrupción de los funcionarios mexicanos, a quienes se les ofrece un porcentaje de la compra para asegurar el contrato", afirma Paloma Mendoza Cortés. "El resultado ha sido el sobreprecio de productos y servicios de seguridad que compra el gobierno mexicano".

Por ejemplo, un empleado de Hacking Team se refiere al caso de un intermediario: "Se hizo amigo del hijo del jefe de adquisiciones y propuso NSO por 15 millones de dólares. Estoy seguro de que hay buenos beneficios relacionados con esta compra". NSO no quiso responder preguntas sobre ese contrato. Los documentos que se filtraron de la empresa italiana revelaron comisiones importantes para los intermediarios, del orden del 30% en contratos por decenas de miles de dólares.

Ciertos intermediarios mencionados en ese entonces, Neolinx de México y Sym Servicios, siguen activos todavía. Los datos de importación registrados por el gobierno mexicano, que Forbidden Stories pudo consultar con la ayuda de un analista del grupo de expertos C4ADS, muestran que en 2019 las empresas aún importaban material de grupos o firmas israelíes.

El director de Neolinx no respondió las preguntas de Forbidden Stories. El director de Sym Servicios, Niv Yarimi, afirma que desde 2015 ya no hace de intermediario para empresas de cibervigilancia. Ahora concentraría sus actividades en el uso de objetos conectados para mejorar la seguridad de las ciudades. Según Paloma Mendoza Cortés, hoy está impulsada la lógica de la "ciudad inteligente y segura" en las empresas de seguridad privadas para promover sus productos y servicios en México.

Por lo demás, otro intermediario mexicano, EyeTech Solutions, recibió dos encargos, en 2016 y 2018, provenientes de la empresa Circles Bulgaria, filial de la firma Circles que pertenece a NSO. El director de operaciones de EyeTech Solutions, Gilad Pait, fue contactado por Forbidden Stories, pero él negó que hubiera trabajado con NSO. Luego colgó y bloqueó nuestro número telefónico.

Esto obliga a cuestionar la versión oficial de la retirada de NSO del mercado mexicano. Porque, más encima, en mayo de 2019 varios números mexicanos aparecieron entre los blancos de Pegasus relacionados con la falla de la aplicación WhatsApp. "El gobierno federal

dice que no son ellos. Entonces, ¿quién es? ¿Y por qué no lo sabemos?", protesta Luis Fernando Garcia.

¿Qué pasa con los derechos humanos en este escenario?

Hay pocas esperanzas de que la respuesta llegue de Israel. Luego de que en 2018 se iniciaran acciones judiciales contra NSO, por su negligencia ante los abusos cometidos por el gobierno mexicano, la justicia israelí cedió a la petición de la empresa de llevar a cabo el proceso en forma confidencial, pretextando razones de seguridad nacional, de injerencia en las relaciones internacionales de Israel, y de secreto comercial.

De igual forma, respecto a los clientes y las licencias de exportación, todo es confidencial. Para las autoridades, "la política consiste en no denunciar, no decir que es falso, no decir nada", detalla Eitay Mack.

Según él, incluso las comisiones encargadas de evaluar la política respecto a los derechos humanos en esas empresas no saben nada de sus clientes. "Si no cuentan con la información, ¿cómo pueden promover una reglamentación? Es una broma".

El exembajador francés Gérard Araud, quien actuó como consejero exterior de NSO Group en materia de derechos humanos de 2019 a 2020, confirma que no sabe lo que se llevó a cabo y lo que no. "El secreto es parte sustancial de la empresa, lo que relativiza mi aporte", explica. "Mi trabajo consistía principalmente en establecer un diálogo con los inversionistas, más que con la misma empresa". Según el diplomático, "el tema de las tecnologías de vigilancia y los derechos humanos requeriría una legislación, o incluso una convención de las Naciones Unidas; o abrir un diálogo con las organizaciones de derechos humanos". Por su parte, NSO alabó el "importante papel" desempeñado por Gérard Araud como consejero de la empresa.

Por su parte, un exempleado de Hacking Team conserva un recuerdo amargo del comité de ética de la empresa italiana. "Ese Consejo nunca hizo nada, sólo redactaba informes que decían que tal país estaba bien, que este otro estaba menos bien, pero que igual se les podían vender los productos. Era sólo un show". Su jefe de entonces tenía una forma de pensar muy simple: si un gobierno dice que una persona es un terrorista, es un terrorista. No es el papel de la empresa involucrarse en el asunto".

"Les puedo decir que no les importa en absoluto", confiesa hoy. "Tanto Hacking Team como NSO pretenden que hacen cosas, pero les importa un comino".

Fuente:

https://aristeguinoticias.com/0712/mexico/espionaje-de-periodistas-mexicanos-una-investigacion-sobre-el-rentable-negocio-del-ciberespionaje/

Pegasus | México tiene un gobierno que no espía, no persigue y no tortura: Delgado

El presidente nacional de Morena, Mario Delgado Carrillo, afirmó que Proyecto Pegasus desnuda el talante autoritario de los gobiernos neoliberales del pasado, quienes a través del uso del presupuesto público espiaron a sus críticos y opositores políticos.

"Proyecto Pegasus desnuda el talante autoritario de los gobiernos neoliberales del pasado, quienes a través del uso del presupuesto público espiaron a sus críticos y opositores políticos", afirmó el presidente nacional de Morena, Mario Delgado Carrillo.

A través de un comunicado, el dirigente de los morenista aseguró que con la Cuarta Transformación se terminaron los gobiernos autoritarios, antidemocráticos y violadores de los derechos humanos, pues dijo, se cortó de tajo con el uso faccioso de los recursos del pueblo de México y se desterraron estas viejas prácticas.

"Hoy, por primera vez tenemos un gobierno de convicciones y principios que antepone siempre a quien más lo necesita. Esta Cuarta Transformación busca que vivamos en una auténtica democracia, donde el pueblo mande, donde periodistas, empresarios, intelectuales y la oposición, así como todas y todos los mexicanos puedan expresarse con total libertad sin temor a represalias políticas", resaltó Delgado Carrillo.

Añadió que a pesar de que en los gobiernos del Partido Revolucionario Institucional y del Partido Acción Nacional por años se persiguieron, desaparecieron y torturaron a quienes pensaban diferente, ahora "gracias a una revolución pacífica en las urnas, México tiene un gobierno que no espía, no persigue y no tortura, y que por el contrario está regenerando la vida pública del país.
"En Morena y en la Cuarta Transformación tenemos el firme compromiso de hacer valer las libertades, de buscar la justicia social y terminar con la impunidad. Trabajamos por construir un país en donde se respeten con plenitud los derechos humanos, donde se termine con la violencia y se construya la paz", expresó.

Fuente: https://aristeguinoticias.com/2007/mexico/pegasus-mexico-tiene-un-gobierno-que-no-espia-no-persigue-y-no-tortura-delgado/

"Quienes nos han espiado, miren la paradoja, no reciben el mismo trato": Gutiérrez Müller

Beatriz Gutiérez Müller reaccionó al hecho de que ella y todo el círculo cercano de Andrés Manuel López Obrador fuera blanco de Pegasus, lo cual "no me sorprende. Me repugna pero estamos acostumbrados", y apuntaló: "Quienes nos han espiado, miren la paradoja, no reciben el mismo trato".

Aquí su postura íntegra difundida esta mañana:

Espionaje telefónico, seguimiento físico de nuestros movimientos, revisión periódica de cuentas bancarias y de declaraciones ante el SAT; chips en los vehículos, cámaras en la calle donde hemos habitado; visitas continuas al Registro Civil (para confirmar parentescos) y al Registro Público de la Propiedad (para inspeccionar propiedades, hasta en el extranjero); intromisión en cuentas de redes sociales (todas) ¡no terminaría de enumerar! ¡Así han sido muchos años acompañando a Ya Saben Quién!

El gobierno violó sistemáticamente nuestros derechos individuales como el de la privacidad. Por fortuna, lo ha declarado el actual presidente Andrés Manuel López Obrador, ya no se realizan violaciones a la ley. Quienes nos han espiado, miren la paradoja, no reciben el mismo trato.
Es sin duda importante la exhibición pública de estas prácticas que confirman nuestras antiguas sospechas. No me sorprende. Me repugna pero estamos acostumbrados. Gracias a todos los investigadores que emprendieron la revisión de esos expedientes de aquella empresa extranjera que fue contratada para entrometerse en casa.
Autoridades mexicanas como la Fiscalía General de la República deben hacer las indagaciones correspondientes. En lo personal, deseo con toda el alma vivir en un Estado de Derecho y no acostumbrarnos a estas intimidaciones no solo del periodo indicado por los reportajes que circulan, sino de antes.

Fuente: https://aristeguinoticias.com/2007/mexico/quienes-nos-han-espiado-miren-la-paradoja-no-reciben-el-mismo-trato-gutierrez-muller/

Pegasus | Bachelet exige a gobiernos 'cese inmediato' del espionaje; 'absolutamente inaceptable', espionaje a la prensa: Von der Leyen

La Alta Comisionada de Naciones Unidas para los Derechos Humanos calificó de 'extremadamente alarmantes' el uso generalizado en distintos países de Pegasus, creado por la empresa israelí NSO; la presidenta de la Comisión Europea, Ursula von der Leyen, calificó com 'absolutamente inaceptable' el espionaje a periodistas.

La Alta Comisionada de Naciones Unidas para los Derechos Humanos, Michelle Bachelet, exigió a los gobiernos el "cese inmediato" del espionaje con tecnologías como el software espía israelí Pegasus "que violen los derechos humanos".

"El uso del software Pegasus para espiar a periodistas y defensores de derechos humanos entre otras figuras públicas es sumamente preocupante", afirmó Bachelet en un comunicado.

Asimismo, calificó de "extremadamente alarmantes" las informaciones que dan cuenta de un uso generalizado en distintos países del software Pegasus, creado por la empresa israelí NSO, y apuntó que estas revelaciones confirman "algunos de los peores temores" sobre el uso indebido e ilegal de la tecnología de vigilancia para socavar los derechos humanos.

“Estos informes confirman la urgente necesidad de regular mejor la venta, transferencia y uso de tecnología de vigilancia y de garantizar una supervisión y autorización estrictas. Sin marcos regulatorios que cumplan con los derechos humanos, existen demasiados riesgos de que se abuse de estas herramientas para intimidar a los críticos y silenciar la disidencia”, resaltó la Alta Comisionada de la ONU.

Bachelet explicó también que el uso de este software de vigilancia se ha asociado con “arrestos, intimidación e incluso asesinatos de periodistas y defensores de derechos humanos“.

Lamentó que los informes de vigilancia también hacen que las personas se autocensuren “por miedo”.

“Los periodistas y defensores de las garantías fundamentales juegan un papel indispensable en nuestras sociedades y cuando son silenciados todos sufrimos”, expresó.

De este modo, se dirigió a los gobiernos para recordarles que las medidas de vigilancia “sólo se justifican en circunstancias definidas rigurosamente y con un objetivo legítimo que las haga necesarias”.

Bachelet añadió que las naciones tienen el deber de proteger a las personas de las transgresiones del derecho a la privacidad por parte de las empresas.

“Un paso clave para prevenir eficazmente el abuso de la tecnología de vigilancia es que los estados exijan por ley que las empresas involucradas cumplan con sus responsabilidades en materia de derechos humanos, sean mucho más transparentes en relación con el diseño y uso de sus productos y establezcan mecanismos de rendición de cuentas más efectivos”.

La Alta Comisionada de la ONU indicó que tanto su oficina como otras instancias de Naciones Unidas han advertido “repetidamente” del riesgo de que las autoridades de los países usen esas herramientas de espionaje para “piratear teléfonos y computadoras personales de periodistas, activistas y opositores que llevan a cabo una labor legítima“.

Bachelet resaltó, además, que los software como Pegasus, Candiru u otros, que permiten la intrusión detallada en los dispositivos personales, sólo deben utilizarse en investigaciones de delitos graves y de amenazas a la seguridad, una “línea roja” que “se ha cruzado con total impunidad” si las recientes acusaciones sobre el uso del software israelí “son parcialmente ciertas”.

Reiteró que los gobiernos deben cesar “inmediatamente” el uso de estas tecnologías y que deben tomar medidas “concretas” para protegerse contra las “invasiones de la privacidad”, e hizo hincapié en que las empresas que desarrollan y distribuyen esas tecnologías son “responsables de evitar daños a los derechos humanos por medio de salvaguardas que mitiguen y remedien los daños que sus productos están causando”.

Absolutamente inaceptable, el espionaje a la prensa: Von der Leyen

Por su parte, la presidenta de la Comisión Europea, Ursula von der Leyen, calificó como "absolutamente inaceptable" el espionaje a periodistas con el software israelí Pegasus.

"Lo que hemos leído hasta ahora, que debemos verificar, es que si esto en realidad ocurrió, es absolutamente inaceptable, y está en contradicción con cualquier regla de la Unión Europea", declaró en conferencia de prensa.

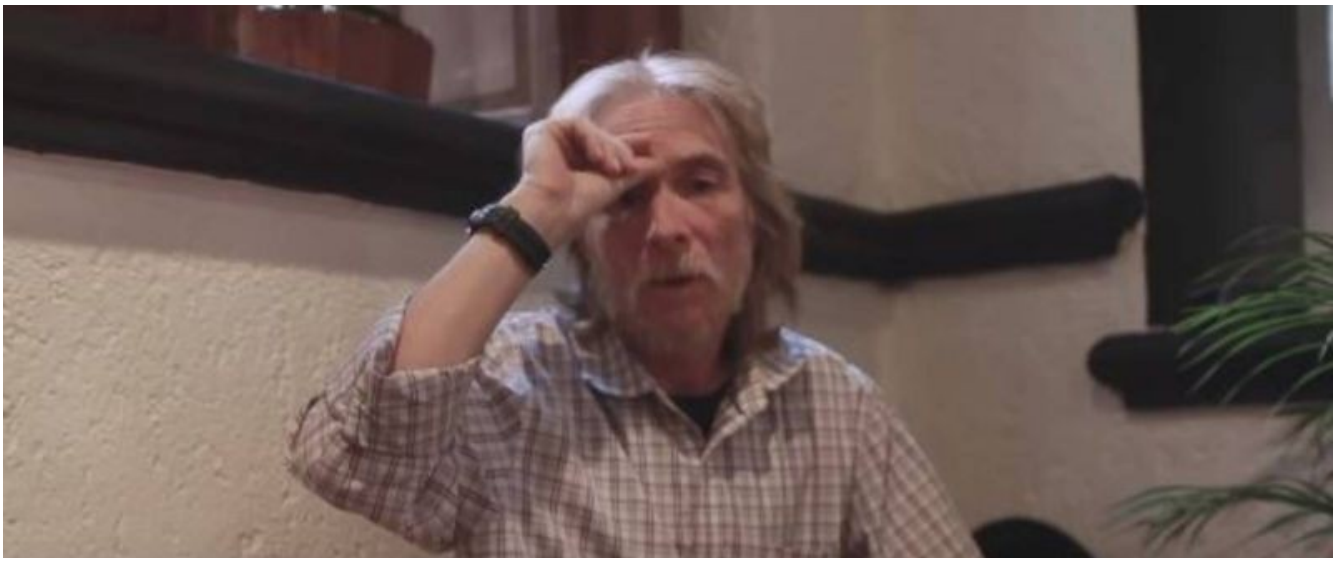
De visita en Praga, denunció en particular el presunto espionaje contra periodistas.

"La libertad de prensa es uno de los valores fundamentales de la Unión Europea", dijo tras reunirse con el primer ministro checo Andrej Babis.

Fuente :

https://aristeguinoticias.com/1907/mundo/pegasus-bachelet-exige-a-gobiernos-el-cese-inmediato-del-espionaje-contra-sus-ciudadanos/

Detienen al hacktivista Commander X; exigen al gobierno mexicano gestionar su liberación



He colocado esta noticia para ver la hipocresía del gobierno actual de México reflejado en los 3 artículos anteriores

CIUDAD DE MÉXICO (apro).- Christopher Doyon, el hacktivista estadunidense refugiado en México desde 2017, fue detenido en su domicilio por agentes del Instituto Nacional de Migración (INM) y, posteriormente, deportado a su país, donde fue arrestado por agentes de la Oficina Federal de Investigaciones (FBI, por sus siglas en inglés), informó el Departamento de Justicia de Estados Unidos.
El gobierno de su país lo acusa de no comparecer ante un juez del Distrito Norte de California el 2 de febrero de 2012, después de ser puesto en libertad preventiva tras un caso penal un año antes, donde se le acusó de "conspiración para causar daño intencional a una computadora protegida", según se asienta en los expedientes del caso CR11-00683.

Doyon es acusado de participar en un ataque de denegación de servicio (DDoS) contra los servidores del condado de Santa Cruz, California, el 16 de diciembre de 2010, en protesta por las nuevas políticas públicas contra la gente sin casa. La acusación plantea que el Frente de Liberación Popular (PLF), uno de los grupos asociados a Anonymous, coordinó y ejecutó el ataque.
Por otro lado, información dada a conocer en Indybay, un medio independiente en San Francisco, asegura que Doyon fue detenido ilegalmente por policías vestidos de civil y, posteriormente, trasladado a Estados Unidos, donde fue encarcelado con el número de registro 03476-028, según el localizador de la Agencia Federal de Prisiones (BOP, por sus siglas en inglés).

Entre las 15:30 y 16:00 horas, "dos agentes mexicanos uniformados llegaron al domicilio de X. La casera les solicitó una orden judicial. Se fueron, regresaron un par de horas después

vestidos de civil, saltaron la cerca, irrumpieron y sacaron a X arrastrando. En ese momento estaba hablando con su abogado. Sabemos que está en suelo estadunidense detenido bajo una violación migratoria, pero probablemente será detenido dado su historial con el FBI", explica el mensaje de los activistas allegados a Doyon.
Jay Leiderman, abogado del activista, confirmó en Twitter (@JayLeidermanLaw), que Doyon se encuentra detenido en una cárcel de baja seguridad en Dublin, California.

Después de su detención, su hermana Amy Beth Doyon (@AmyBethDoyon) posteó:

"Nuestro derecho a buscar y recibir #politicalasylum está en riesgo. Amarlo u odiarlo, no hace ninguna diferencia para mi. Vinieron por #JulianAssange. Vinieron por mi hermano #FreeCommanderX . Su libertad es nuestra libertad. Vienen por todos nosotros".

De manera inédita el gobierno mexicano desplegó un operativo en conjunto con el gobierno estadunidense para dar con el activista. Su detención fue coordinada por el agregado legal del FBI en la CDMX, la Agencia de Investigación Criminal (AIC), la Fiscalía General del Estado de Morelos (FGEM), el Instituto Nacional de Migración (INM), la Interpol y la Oficina de Servicios al Ciudadano Estadunidense en la CDMX.
Asimismo, el Registro Nacional de Detenciones (RND) de la Secretaría de Seguridad y Protección Ciudadana (SSPC), confirma el viernes 11 de junio como la fecha de su detención.

En la cuenta de Twitter @FreeCommanderX_ amigos del hacktivista iniciaron una campaña para liberarlo "del secuestro injusto de Estados Unidos" con el hashtag #FreeCommanderX.

Doyon se enfrenta al menos a una pena de dos años de prisión por no comparecer después de obtener su libertad condicional.
En noviembre de 2018, Proceso logró encontrarse con Doyon. En dicha entrevista habló de su petición de asilo al gobierno mexicano y sobre una guerra que se desenvuelve en el ciberespacio.
"Espero que el gobierno mexicano obedezca su propia Constitución, que obedezcan las leyes estipuladas en el acta de refugiados, en el tratado de asilo a refugiados de la OEA, invoco mis derechos bajo el acuerdo de derechos humanos de la ONU, invoco todos mis derechos y, si son respetados estos instrumentos, México no tiene otra opción más que darme asilo político y espero que sigan su propia ley", expreso el hacktivista desde una ubicación que aún permanece reservada.

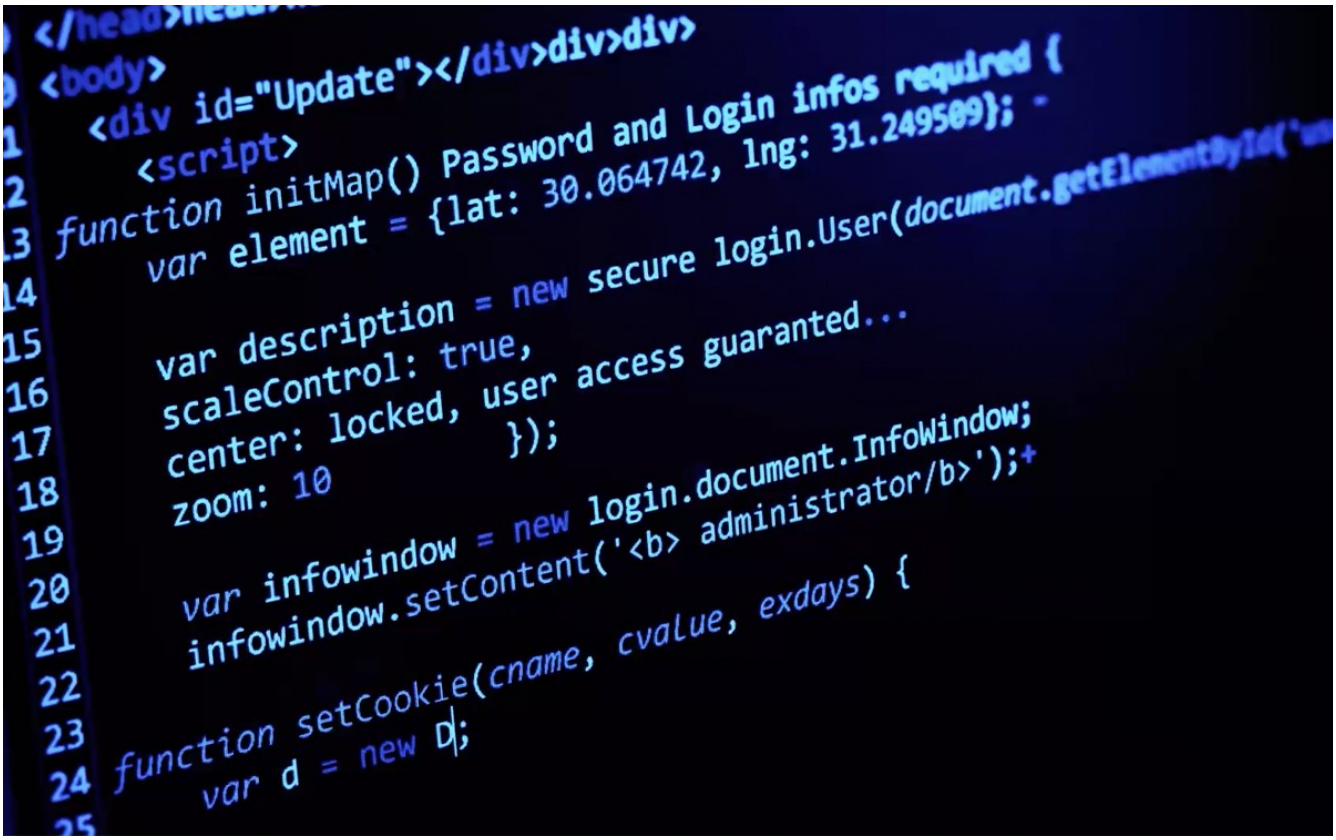
Lee su testimonio en Proceso 2192.

Escuchalo en el siguiente video:

https://yewtu.be/Fqf_MluCvr0

Fuente: https://www.proceso.com.mx/nacional/2021/6/16/detienen-al-hacktivista-commander-x-exigen-al-gobierno-mexicano-gestionar-su-liberacion-266008.html

Pegasus Project | Reporteros Sin Fronteras alista acciones legales por el software espía



También pide a los sistemas judiciales de los países democráticos sancionar a los responsables por el uso del programa espía Pegasus.

La organización Reporteros Sin Fronteras (RSF) informó este lunes que está decidiendo qué acciones legales y en qué países las emprenderá para castigar a quien resulte responsable por el uso del software espía Pegasus.

Asimismo instó a los periodistas y medios afectados a que contacten con Reporteros Sin Fronteras para unirse en una respuesta legal adecuada a las revelaciones sobre el software espía.

En Aristegui en Vivo se dio a conocer, como parte de la investigación internacional Pegasus Project -en la que colaboraron Forbidden Stories y Amnistía Internacional-, que al menos 180 periodistas, de 20 países, desde 2016 hasta junio de 2021, fueron blanco del software espía.

En una serie de tuits Reporteros Sin Fronteras recuerda que en 2017 "dio la primera voz de alarma" sobre este programa espía después de que se utilizase para espiar a periodistas mexicanos.

Asimismo señala que la empresa israelí Grupo NSO no contribuye a la "seguridad global y a la estabilidad", como la compañía proclama. "Al contrario. Pegasus es una herramienta ruin y repugnante, creada por mercenarios digitales y adorada por los depredadores de la #LibertadDePrensa por su uso para perseguir periodistas".

Grupo NSO insistió en que Pegasus Project está lleno de acusaciones falsas y engañosas, y dice que considera demandar por difamación.

"Haremos todo lo posible para garantizar que se castiga a #NSO por los delitos que ha cometido y las tragedias que ha posibilitado. Los sistemas judiciales de los países democráticos deben abordar este asunto de extrema gravedad, aclarar los hechos y sancionar a los responsables", indicó Reporteros Sin Fronteras en Twitter.

RSF instó a los gobiernos democráticos a que declaren de inmediato una moratoria sobre la venta de software espía hasta que se hayan establecido garantías para evitar su uso en la opresión.

Fuente:

https://aristeguinoticias.com/1907/mexico/pegasus-project-reporteros-sin-fronteras-alista-acciones-legales-por-el-software-espia/

Peña Nieto, el desenfrenado espionaje contra periodistas

En apenas un año y medio, agencias del gobierno del expresidente priista, registraron en su plataforma Pegasus los celulares de más de 15 mil personas, de las que se pudieron identificar por lo menos 25 periodistas -seis de ellos trabajaban entonces en Proceso.

CIUDAD DE MÉXICO (proceso.com.mx).- El domingo 18 de junio 2017, el New York Times publicó en su primera plana un amplio reportaje que detonó una bomba informativa en México: un reportaje elaborado con datos de la Red en Defensa de Derechos Digitales (R3D) y del Citizen Lab exhibía operaciones de espionaje realizadas por el gobierno de Enrique Peña Nieto con el poderoso spyware Pegasus para intervenir, de manera ilegal, celulares de una decena de periodistas y defensores de derechos humanos en el país, entre ellos Carmen Aristegui e integrantes de su equipo de investigación.

Menos de tres semanas antes de publicarse el texto, una agencia del gobierno mexicano que tiene las características del Centro de Investigación y Seguridad Nacional (Cisen) seleccionó el número de Azam Ahmed, entonces corresponsal del New York Times en México, en la misma plataforma Pegasus desarrollado por la empresa israelí NSO Group.

El número del hombre apareció entre más de 50 mil datos telefónicos seleccionados por agencias gubernamentales clientes de NSO Group que consultó Proceso en el marco del Pegasus Project, una investigación colaborativa que involucra a más de 80 periodistas de 17 medios repartidos en 10 países, coordinada por Forbidden Stories con el apoyo técnico del Security Lab de Amnistía Internacional.

Pero el reportero del New York Times y Carmen Aristegui -quien participó también en Pegasus Project- no fueron los únicos blancos del aparato de espionaje de Peña Nieto: en apenas un año y medio, agencias de su gobierno registraron en sus plataformas Pegasus los celulares de más de 15 mil personas, de las que se pudieron identificar por lo menos 25 periodistas -seis de ellos trabajaban entonces en Proceso y uno, el periodista guerrerense Cecilio Pineda Brito, fue asesinado algunas semanas después-, defensores de derechos humanos, sindicalistas, gobernadores, líderes religiosos, académicos, médicos, militares, personas menores de edad y más de 700 políticos y sus familiares, principalmente de partidos de oposición.

Durante un año y medio, agencias de gobierno de Peña Nieto registraron, en promedio, más de 33 objetivos de ciberespionaje al día, a un ritmo varias veces mayor al de regímenes autoritarios como Arabia Saudita, Marruecos, los Emiratos Árabes Unidos, Ruanda, India, Azerbaiyán, Hungría o Kazajistán, que también fueron clientes de NSO Group.

Resulta imposible afirmar que, en todos los casos, las selecciones derivaron en ataques y que instalaron Pegasus en los teléfonos de sus víctimas. En aquel entonces para conseguir la infección se necesitaba que el usuario diera clic en un vínculo malicioso, enviado en el contenido de un mensaje de texto o un correo electrónico.

Pegasus es un programa desarrollado por la empresa israelí NSO Group, que permite a una agencia de gobierno acceder a prácticamente toda la memoria del teléfono de un objetivo, incluyendo mensajes -SMS, Whatsapp y otras aplicaciones de mensajería-- y correos; también capta la geolocalización, permite consultar el historial, vigilar la geolocalización en cualquier momento, escuchar las llamadas, y tomar el control del micrófono de la cámara cuando lo desee.

Ocho contratos publicados por instituciones y --sobre todo-- por la prensa en los últimos nueve años muestran que tres agencias federales de seguridad operaron la plataforma Pegasus durante el sexenio de Peña Nieto: el Cisen, la Procuraduría General de la República (PGR), a través de la Agencia de Investigación Criminal (AIC), y la Secretaría de la Defensa Nacional (Sedena).

De estas tres agencias, el análisis de los datos del Pegasus Project apuntan a que el Cisen fue la institución que seleccionó a prácticamente todos los periodistas mexicanos; varias fuentes de seguridad consultadas en el marco de esta investigación colaborativa coinciden en que, de los tres clientes oficiales de NSO Group, el Cisen y la Sedena utilizaban Pegasus sin autorización judicial, dejando abierta la puerta a abusos y arbitrariedades.

De los más de 50 mil datos telefónicos a los que tuvieron acceso Forbidden Stories y Amnistía Internacional, más de 15 mil corresponden a México; durante meses, Proceso y los demás medios aliados los analizaron, cruzaron y verificaron, con lo que pudieron identificar, con un alto margen de certeza, qué agencia del Cisen, de la AIC y de la Sedena seleccionaron a algunas víctimas de Pegasus.

Los datos también sugieren la existencia de un cuarto ente, no identificado, que realizó una menor cantidad de ataques pero los dirigió exclusivamente hacia personajes políticos de primer nivel.

En el marco de esta investigación, los medios asociados buscaron por muchas vías distintas una manera de comunicarse con el expresidente Enrique Peña Nieto, entre ellos sus hijos, un exabogado, el PRI y excolaboradores; algunos no contestaron, y otros dijeron que no tenían forma de hacerle llegar un cuestionario.

En respuesta a un cuestionario enviado en el marco de esta investigación internacional, el senador Miguel Ángel Osorio Chong, quien era titular de la Secretaría de Gobernación (Segob) -y por ende responsable del Cisen, negó categóricamente y reiteradamente los hallazgos de esta investigación.

Afirmó que durante su gestión al frente de la Segob, "nunca se autorizó ni se tuvo conocimiento sobre la existencia o el uso del software al que se refieren. También afirmó que "nunca se ordenó ni se tuvo conocimiento del uso de Pegasus, contra nadie".

Sin embargo, en un comunicado emitido en mayo de 2020, la Secretaría de Seguridad y Protección Ciudadana (SSPC) indicó que el Cisen operó Pegasus entre 2014 y 2017, y aclaró que ni el Centro Nacional de Inteligencia (CNI) -que sustituyó el Cisen-- ni la Guardia Nacional "cuentan con el servicio del sistema Pegasus", ya que "el gobierno del Licenciado Andrés Manuel López Obrador decidió no renovar la licencia de operación".

Este trabajo forma parte de una serie de reportajes que Proceso publicará a lo largo de la próxima semana en el marco de Pegasus Project, y que exhibirán la magnitud del espionaje ilegal operado desde el gobierno de Peña Nieto.

Amenazado y espiado

El gobierno de Peña Nieto utilizó de forma masiva el malware, en un sexenio durante el cual el país se convirtió en el lugar más peligroso del mundo para ejercer el periodismo, un terrible lugar del que no ha descendido. Durante los seis años de gobierno de Peña Nieto, la organización Artículo 19 registró 2 mil 502 agresiones contra periodistas -un incremento de 129% en comparación con el gobierno de Felipe Calderón Hinojosa--, los cuales incluyen 47 asesinatos.

Cecilio Pineda Brito, periodista en la conflictiva región de Tierra Caliente, en Guerrero, fue una de estas víctimas. En la tarde del 2 de marzo de 2017, el hombre fue asesinado a balazos por dos personas en moto, mientras esperaba en un autolavado de Ciudad Altamirano que le entregaran su camioneta. Un amigo llegó muy rápido en el lugar, donde Pineda todavía respiraba; la ambulancia tardó más de media hora en llegar, y el periodista estaba muerto cuando el vehículo llegó al hospital.

Escasas semanas antes, a principios de 2017, una agencia del gobierno de Peña Nieto -cuyas características corresponden a la Sedena-- ingresó en dos ocasiones el número de teléfono del celular de Pineda en la plataforma Pegasus.

El día de su asesinato, Pineda había denunciado en su canal de Facebook "Cecilio Pineda, las noticias de un instante" -seguido por cerca de 50 mil personas-- los vínculos entre el diputado local Saúl Beltrán Orozco, expresidente municipal de San Miguel Totolalpan, y Raybel Beltrán Jacobo de Almonte, mejor conocido como "El Tequilero", líder de la banda armada "Los Tequileros", que cometía secuestros y homicidios en la región.

En ese mismo video, el periodista -cuya carrera empezó en 2005 en Despertar del Sur y transitó por colaboraciones de nota roja en El Universal o La Jornada Guerrero-- acusó al gobernador priista de Guerrero, Héctor Astudillo Flores, de proteger a "Los Tequileros" y de encubrir sus crímenes en la región.

En aquel entonces, Pineda recibía amenazas de muerte a diario en sus redes sociales. Sus familiares dicen que su trabajo periodístico le provocaba crisis severas de ansiedad, ataques de pánico e insomnios; el hombre acusaba directamente a políticos, con nombre, apellido y apodo, por sus vínculos con "Los Tequileros".

Pineda había sufrido un atentado el 18 de septiembre de 2015, por el cual entró en el Mecanismo de Protección a Periodistas y Defensores de Derechos Humanos; sin embargo, la instancia y el periodista acordaron cerrar el caso en octubre de 2016, porque Pineda no aceptaba su oferta de "extracción" hacia un refugio seguro.

En la última plática telefónica que sostuvo con sus interlocutores del Mecanismo -cuyo audio fue obtenido en el marco de esta investigación--, Pineda afirmó que se le "complica un poco" y que le parecía "muy precipitado" abandonar la región con su familia, y afirmó: "no salgo, no conocen mi ubicación, porque me he mudado de un lugar a otro (...) no saben donde vivo. Y por lo general tengo mis carros escondidos.

"Tengo contacto directo con militares y estatales, en dado caso que hubiera algún problema (...), yo no tengo problemas con los comandos armados aquí, lo que pasa es que pudiera ser, que este grupo contratara a una persona para asesinarme. También me han dicho que quieren matar al cacique de San Miguel Totolalpan", abundó el periodista, quien refrendó que "el diputado local (Saúl Beltrán Orozco) tiene contacto directo con el gobernador".

Un amigo de Pineda dice que, antes de su asesinato, el periodista había pedido protección al Ejército porque unas personas lo habían visitado en su casa para pedirle mil pesos. Dado el monto relativamente pequeño exigido, un militar aconsejó al hombre que no se los entregara, pues parecía más una manera de localizarle y de tenderle una trampa.

Entrevistado por la periodista Nina Lakhani, en el marco de esta investigación internacional, el fiscal Olea recuerda que las autoridades determinaron que la ejecución de

Pineda fue ordenada por "El Tequilero". Semanas después del asesinato, las autoridades encontraron en Coyuca de Catalán el cuerpo de Luis Armando López Hernández, uno de los dos supuestos autores materiales.

El hombre también narra que, en 2016 y 2018, dos hombres -entre ellos un israelí, parecido según él a la fotografía de Uri Emmanuel Ansbacher, entonces representante de NSO en México-- le enseñaron un programa de intervención de teléfonos que lo convenció, y pidió fondos a la oficina de Astudillo, quien se lo negó en un primer momento, pero en 2018 afirmó que lo compraría.

Días después de atacar con Pegasus a los celulares de Pineda y su novia, la misma agencia del Estado -probablemente la Sedena-- lanzó el programa contra los celulares del gobernador Astudillo y de Xavier Olea Peláez, entonces fiscal de Guerrero; y tres meses después del asesinato de Pineda, la Agencia de Investigación Criminal (AIC) lanzó Pegasus para infectar el celular de Saúl Beltrán Orozco, quien había pedido licencia de su cargo de diputado en mayo de 2017, debido a una investigación que la fiscalía local tenía abierta, por el asesinato de un empleado municipal.

El priista, quien en 2015 fue coordinador local de la campaña de Astudillo, reapareció públicamente en 2018, y en una entrevista con medios dio su caso legal "por terminado"; por su parte, Jacobo Raybel de Almonte, "El Tequilero", murió asesinado en 2019, tras años de cometer crímenes contra la población en total impunidad.

En respuesta a un cuestionario de Forbidden Stories, NSO Group sostuvo que, incluso en el caso de que el teléfono de Pineda haya sido espiado en febrero de 2017, "ello no quiere decir que el cliente de NSO Group o la información recolectada por el software de NSO Group fuera en alguna manera conectada con el asesinato del periodista el mes siguiente".

"Una correlación no es lo mismo que una causa, y los sicarios quienes asesinaron al periodistas pudieron haberse enterado sobre su ubicación en un autolavado público de múltiples maneras sin vinculo con NSO Group, sus tecnologías o sus clientes", abundó.

El caso de Pineda se sumó al de Javier Valdez Cárdenas, reconocido periodista fundador de la revista Río Doce, en Sinaloa, cuyo asesinato a plena luz del día, el 15 de mayo de 2017 en Culiacán, afuera de la sede de la redacción, causó una enorme conmoción en el país, y especialmente en el gremio.

A partir del día siguiente y durante las semanas posteriores, la agencia de gobierno que parece ser el Cisen atacó con Pegasus los celulares de Ismael Bojórquez y Andrés Villarreal, directores Editorial y de Información de la revista, Alejandro Sicairos -fundador de la revista-- y Griselda Triana, la viuda de Valdez, según reportó en su momento el trabajo conjunto de New York Times, R3D y el Citizen. Los números de Bojórquez, Villarel, Sicairos y Triana aparecen entre los datos obtenidos por el Pegasus Project.

Bajo escrutinio

A principios del verano de 2016, cinco integrantes de la revista Proceso fueron seleccionados por el gobierno mexicano en la plataforma Pegasus: Rafael Rodríguez Castañeda, entonces director; Jorge Carrasco, quien era reportero -y es ahora director--, Alejandro Caballero, entonces coordinador del sitio de Internet, así como los reporteros Arturo Rodríguez García y Jenaro Villamil, ahora titular del Sistema Público de Radiodifusión Mexicana (SPR).

"No me sorprenden los intentos de pinchar mi teléfono", reacciona Rodríguez Castañeda al enterarse de la posible tentativa de espionaje. "A lo largo de la larga vida de Proceso, a quienes hemos estado en áreas de responsabilidad periodística en la revista nos han acosado de variadas maneras desde los órganos de seguridad y vigilancia del Estado", abunda.

El exdirector recuerda que, entre los años 70 y 80, Julio Scherer García, el fundador de Proceso -quien fue su maestro-- "fue objeto de un continuo trabajo de espionaje ignominioso por parte de la Dirección Federal de Seguridad y de la Dirección de Investigaciones Políticas, de la Secretaría de Gobernación. Él estaba consciente y nunca perdió la naturalidad para desarrollar su trabajo cotidiano".

Arturo Rodríguez García, por su parte, señala que, en el verano de 2016, se encontraba en Nochixtlán, Oaxaca, para documentar la represión violenta que lanzó el gobierno federal para desalojar un bloqueo carretero -la cual desembocó en la muerte de ocho civiles, por heridas de bala--, cuando recibió un mensaje que decía "No se te vaya a ir la nota", con un vínculo abajo.

"Abrí el link y nada. Si no me equivoco, mi teléfono se apagó y se reinició. Algo así. Después lo reinicié y se comportó raro, se ponía en negro", abunda el reportero. Precisa que en aquel entonces realizaba una cobertura amplia sobre el movimiento social y sus efectos políticos en un contexto de "mucha paranoia gubernamental por lo que se había publicado en los años previos".

Caballero, por su parte, nunca tuvo ninguna sospecha de que pudiera ser blanco de espionaje.

En las semanas siguientes, el gobierno federal continuó sus selecciones de reconocidos periodistas: ingresó el teléfono de la multipremiada periodista Marcela Turati, exreportera de Proceso, de Álvaro Delgado -también reportero de este semanario en aquel entonces--, así como de Alejandra Xanic von Bertrab -galardonada por un premio Pulitzer-- y de Ignacio Rodríguez Reyna, ambos inmersos en el proyecto de creación de la organización Quinto Elemento Lab.

En el dispositivo que usaba en aquel entonces -meses después de publicar su libro sobre el pacto electoral entre Peña Nieto y Felipe Calderón Hinojosa--, Álvaro Delgado recibió un mensaje acompañado por un vinculo malicioso. El mensaje fue enviado en la tarde del 3 de agosto de 2016, y decía: "Hola Álvaro, únicamente paso a saludarte y enviarte esta nota de The Guardian (sic) que parece importante retomar". Dicho mensaje coincide con la selección del número del periodista en los datos telefónicos.

"Siempre supe que podia estar en la lista de periodistas espiados durante el gobierno de Enrique Peña Nieto, como no tuve duda que estuve espiado durante el gobierno de Felipe Calderón, y desde antes (...) he sido un periodista muy crítico del priismo, específicamente del peñismo", dice Delgado en entrevista, y analiza que "El espionaje, cuando se hace de manera ilegal, parte de un régimen autoritario; lo que demuestra este espionaje es el terror que se genera en los ámbitos del poder político sobre resultados de investigaciones periodísticas."

Marcela Turati, fundadora de la Red de Periodistas De a Pie y enlace de periodistas amenazados o desplazados en el país, subraya: "no me vulneraron solo a mí, hay que recordar que 2016 y 2017 fueron los años de los asesinatos de Miroslava Breach y Javier Valdéz. Espiarme a mí, de alguna manera, era espiar a periodistas organizados para enfrentar amenazas y para dar apoyo a periodistas que estaban amenazados, y esto es muy grave".

En estos años, Turati investigaba, entre otros, sobre la desaparición forzada de los 43 normalistas de Ayotzinapa y las masacres de personas migrantes en Tamaulipas. "he sentido vulnerada mi seguridad digital en estos años: desde hackeos, robos de memorias, de bases de computadoras, robos a mi computadora personal, y cosas raras: teníamos bloqueados ciertos IPs, no podíamos entrar a la página del Ejército, cosas así; recibíamos llamadas tratando de desviar nuestras investigaciones, falsas pistas; personas que se presentaban de manera muy rara para dar información que resultaba falsa o peligrosa".

"Por estas fechas también es cuando empezamos a investigar a los mexicanos en vínculo con el caso Odebrecht, y en particular nos centramos sobre el personaje de (Emilio) Lozoya; fue una de nuestras primeras publicaciones con Quinto Elemento Lab", dice Rodríguez Reyna.

Alejandra Xanic, también cofundadora de Quinto Elemento Lab, recuerda que "noté que algo extraño ocurría con mi celular por el contenido de los mensajes de texto; tengo la impresión de que los primeros fueron genéricos, como si fueran SMS de un corporativo, pero después llegaron otros hechos a la medida: en uno me decían ¿no has visto la nota en MILENIO que involucra a Nacho (Rodríguez Reyna) con narcotráfico? refiriéndose a un colega de trabajo".

"El mensaje que capturó mi atención llegó cuando tenía la guardia baja. Mis alumnos en la universidad estaban haciendo algún ejercicio cuando capté en la pantalla del celular que

alguien me escribió algo como: acaba de morir mi mamá, te necesito cerca. Le dí click. El celular comenzó a tener un comportamiento errático. Esto pasó mucho antes de que fuera público el espionaje a otros periodistas y activistas. Me recomendaron deshacerme de él".

La lista no termina aquí: en cuestión de días, esa agencia -probablemente el Cisen-- también trató de intervenir el dispositivo Ricardo Raphael, de la conductora Yuriria Sierra y de Luis Herández Navarro, editor en La Jornada.

"Hay una broma que circula", comenta Hernández: "Que uno sea paranoico no quiere decir no lo persigan. Aparecer en la lista de periodistas espiados confirma que la ironía puede ser la mejor forma de capturar la libertad" (...) detrás del espionaje por parte de poderosos, no solo hay una grave violación al derecho a la privacidad, sino también el reconocimiento de su incapacidad para entender lo que realmente acontece en la sociedad".

Sierra, por su parte, reflexiona que "no tenía ni idea pero tampoco me extraña porque soy periodista en México, y este sistema de Pegasus lo usan aquí desde hace años (...) me molesta porque vulnera el derecho a la privacidad, pero no me asusta".

El gobierno de Peña Nieto también buscó espiar a periodistas cercanos al régimen priista, como el columnista Salvador García Soto, así como Pascal Beltrán del Río, director de Excélsior, Raymundo Riva Palacio, fundador de Eje Central, los columnistas Ricardo Alemán y Pablo Hiriart -quienes cobraron 8 y 5 millones de pesos de publicidad oficial en 2018, respectivamente-- o Lourdes Mendoza, acusada por Emilio Lozoya Austin, el exdirector de Pemex, de recibir regalos y pagos de Luis Videgaray Caso.

Gobierno Espía

El 17 de mayo de 2017, ante los gobernadores de los 32 estados de la República o sus representantes, Peña Nieto adoptó un tono serio, e incluso pidió un minuto de silencio por "todas las personas, periodistas y defensores de derechos humanos que lamentablemente, en el ejercicio de su tarea, de su lucha, han caído en el cumplimiento de ese deber y de esa tarea a la que se han entregado".

Después de un largo discurso en el que habló de su indignación ante la violencia contra la prensa, concluyó: "Lucharé hasta el último día de mi mandato, a fin de fortalecer las condiciones para el ejercicio pleno del periodismo profesional, riguroso y valiente que México necesita", y hasta aseveró: "México tiene que distinguirse por salvaguardar la libertad de prensa. México tiene que distinguirse por proteger a los periodistas y a los defensores de derechos humanos".

Apenas tres meses antes, se había documentado que su gobierno había tratado de espiar a Alejandro Calvillo, el doctor Simón Barquera y Luis Encarnación, todos promotores del impuesto a los refrescos para combatir la grave crisis de diabetes. Y apenas un mes después se publicó el reportaje del New York Times, el cual mostró una magnitud mucho

mayor del espionaje ilegal, y sumó "GobiernoEspía" a la larga de lista de escándalos que mancharon la administración de Peña Nieto.

El reportaje documentó por ejemplo que la periodista Carmen Aristegui, su hijo -entonces menor de edad--, así como los periodistas Sebastián Barragán y Rafael Cabrera, integrantes de su equipo de investigación --quienes revelaron el escándalo de la Casa Blanca de Peña Nieto-- habían sido víctimas de reiteradas tentativas de espionaje a partir de principios de 2015.

Los datos telefónicos del Pegasus Project muestran que el gobierno del mexiquense también ingresó en sus plataformas de Pegasus a una hermana de Aristegui, así como a una de sus asistentes en CNN y su productora en el portal de noticias en Internet Aristegui Noticias, que abrió después de ser expulsada de MVS Radio, propiedad de Joaquín Vargas Guajardo, por presiones políticas.

"Fue una gran sorpresa ver otros cercanos míos en la lista", dice Aristegui, y agrega: "tengo seis hermanos, y al menos uno de ellos, mi hermana, estuvo seleccionada en el sistema (...) mi asistente sabía todo de mí; tenía acceso a mi agenda, a todos mis contactos, las 24 horas y los siete días de la semana".

El reportaje de Ahmed también reveló que el gobierno federal trató de espiar directivos del Centro de Derechos Humanos Juan Agustín Pro (Centro Pro); Juan Pardinas, entonces director del Instituto Mexicano por la Competitividad (IMCO) --ahora director de Reforma-- y Alexandra Zapata; el conductor de Televisa Carlos Loret de Mola, así como los periodistas Daniel Lizárraga y Salvador Camarena, entonces integrantes de la organización Mexicanos Contra la Corrupción y la Impunidad (MCCI).

Días después, la revista Eje Central publicó un reportaje en el cual citó informes internos del Cisen, los cuales reportaban 729 operaciones de espionaje llevadas a cabo entre el 31 de agosto y el 14 de septiembre de 2015 "a través de un malware que tiene capacidades idénticas al de origen israelí, conocido como Pegasus".

Entre los nombres que señalaba el reportaje figuraban los de los periodistas Carmen Aristegui y Raymundo Riva Palacio, así como José Ramón López Beltrán, funcionarios del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), artistas, familiares de políticos, funcionarios de alto nivel -como Alfonso Navarrete Prida, entonces secretario de Trabajo y Previsión Social--, abogados, medios, activistas, sindicalistas, jueces y legisladores.

Después del escándalo, varias víctimas de espionaje interpusieron una denuncia ante la extinta PGR, que abrió una carpeta de investigación. El 12 de julio de 2017, la Relatoría Especial para la Libertad de Expresión de la CIDH exhortó a que la investigación sea "exhaustiva e independiente"; por su lado, la Comisión Nacional de Derechos Humanos

(CNDH) pidió a la Sedena, la PGR y el Cisen que realicen una investigación sobre los abusos de Pegasus "con profesionalismo, exhaustividad, objetividad y diligencia".

Cuatro años después, la ahora Fiscalía General de la República (FGR) aún no ha dado a conocer los resultados de su investigación, ni ha judicializado el caso. La intervención de comunicaciones sin mandato judicial es un delito planteado en el artículo 177 del Código Penal Federal, el cual prevé penas de 6 hasta 12 años de cárcel.

"No podemos decir que esto ya se terminó, porque no sabemos qué ha hecho este gobierno por la denuncia que se puso en el tema de Pegasus, y tampoco vemos una depuración de las estructuras en algunas áreas de la PGR, donde se han albergado las cabecillas de estos grupos dedicados al espionaje", deplora Turati.

"¿Qué alcances tuvo esto? ¿a quiénes sirvieron con este espionaje? ¿cómo vulneró este espionaje el trabajo y la seguridad de personas que luchan por sus derechos ? Pienso en activistas en defensa del territorio, el agua y tantos más que han estado en tan grave riesgo y acecho. ¿A quiénes sirvió? ¿cómo conectan estas tramas diversas? Lo que exhiben es de suma importancia. Faltará tener muy claras respuestas", reflexiona Xanic.

Carmen Aristegui y Sebastián Barragán (Aristegui Noticias), Paloma Dupont de Dichenin (FS), Juan Omar Fierro (Proceso), Nina Lakhani (The Guardian), Lilia Saúl (OCCRP) y Mary Beth Sheridan (Washington Post) colaboraron en la realización de este reportaje.

Fuente:

https://www.proceso.com.mx/nacional/2021/7/18/pena-nieto-el-desenfrenado-espionaje-contra-periodistas-268034.html

El spyware privado israelí solía hackear teléfonos celulares de periodistas, activistas en todo el mundo

El spyware Pegasus de NSO Group, con licencia para gobiernos de todo el mundo, puede infectar teléfonos sin un clic

Actualizado 18 de julio a las 8:15 p.m. Publicado originalmente el 18 de julio de 2021

Un spyware de grado militar con licencia de una firma israelí a los gobiernos para rastrear a terroristas y criminales fue utilizado en intentos y exitosos hacks de 37 smartphones pertenecientes a periodistas, activistas de derechos humanos, ejecutivos de negocios y dos mujeres cercanas al periodista saudí asesinado Jamal Khashoggi, según una investigación de The Washington Post y 16 socios de medios.

Los teléfonos aparecieron en una lista de más de 50.000 números que se concentran en países conocidos para vigilar a sus ciudadanos y también conocidos por haber sido clientes de la firma israelí, NSO Group, líder mundial en la creciente y en gran medida no regulada industria del spyware privado, la investigación encontró.

La lista no identifica quién puso los números en él, o por qué, y se desconoce cuántos de los teléfonos fueron dirigidos o vigilados. Pero el análisis forense de los 37 smartphones muestra que muchos muestran una correlación estrecha entre sellos de tiempo asociados con un número en la lista y la iniciación de la vigilancia, en algunos casos tan breve como unos segundos.

Forbidden Stories, un periodismo sin fines de lucro basado en París, y Amnistía Internacional, un grupo de derechos humanos, tuvo acceso a la lista y la compartieron con las organizaciones de noticias, lo que hizo más investigación y análisis. El Laboratorio de Seguridad de Amnistía hizo los análisis forenses en los teléfonos inteligentes.

Los números de la lista no están atribuidos, pero los reporteros pudieron identificar a más de 1.000 personas que abarcaban más de 50 países mediante investigaciones y entrevistas en cuatro continentes: varios miembros de la familia real árabe, por lo menos 65 ejecutivos de negocios, 85 activistas de derechos humanos, 189 periodistas y más de 600 políticos y funcionarios gubernamentales, incluyendo ministros de gabinete, diplomáticos y oficiales militares y de seguridad. También aparecieron en la lista varios jefes de Estado y primeros ministros.

Entre los periodistas cuyos números aparecen en la lista, que data de 2016, se encuentran reporteros que trabajan en el extranjero para varias organizaciones de noticias líderes, incluyendo un pequeño número de CNN, la Associated Press, Voice of America, el New York Times, el Wall Street Journal, Bloomberg News, Le Monde en Francia, el Financial Times en Londres y Al Jazeera en Qatar.

El objetivo de los 37 teléfonos inteligentes parecería estar en conflicto con el propósito declarado de la licencia de NSO del spyware Pegasus, que la compañía dice que está destinado sólo para el uso en la vigilancia de terroristas y delincuentes principales. Las pruebas extraídas de estos teléfonos inteligentes, reveladas aquí por primera vez, ponen en duda las promesas de la empresa israelí a la policía de sus clientes por abusos de derechos humanos.

El consorcio de medios, titulado Pegasus Project, analizó la lista a través de entrevistas y análisis forense de los teléfonos, y comparando detalles con información previamente reportada sobre NSO. El Laboratorio de Seguridad de Amnistía examinó 67 teléfonos inteligentes donde se sospechaban ataques. De ellos, 23 fueron infectados con éxito y 14 mostraron signos de intento de penetración.

Para los 30 restantes, las pruebas no fueron concluyentes, en varios casos porque los teléfonos habían sido reemplazados. Quince de los teléfonos eran dispositivos Android, ninguno de los cuales mostraba evidencia de infección exitosa. Sin embargo, a diferencia de los iPhones, los Android no registran los tipos de información requeridos para el trabajo de detective de Amnistía. Tres teléfonos Android mostraban signos de segmentación, como mensajes SMS conectados con Pegasus.

Amnistía compartió copias de seguridad de datos en cuatro iPhones con Citizen Lab, que confirmó que mostraban signos de infección por Pegasus. Citizen Lab, un grupo de investigación de la Universidad de Toronto que se especializa en estudiar Pegasus, también llevó a cabo un examen entre pares de los métodos forenses de Amnistía y los encontró sonoros.

En largas respuestas antes de la publicación, NSO llamó a las conclusiones de la investigación exageradas e infundadas. También dijo que no opera el spyware licenciado a sus clientes y "no tiene ninguna visión" en sus actividades específicas de inteligencia.

Después de la publicación, el jefe ejecutivo de NSO Shalev Hulio expresó preocupación en un teléfono entrevista con El Post sobre algunos de los detalles que había leído en las historias del Proyecto Pegasus el domingo, mientras continuaba disputando que la lista de más de 50.000 números de teléfono tenía algo que ver con NSO o Pegasus.

"La empresa se preocupa por periodistas y activistas y la sociedad civil en general", dijo Hulio. "Entendemos que en algunas circunstancias nuestros clientes podrían mal utilizar el sistema y, en algunos casos como lo reportamos en [NSO's] Transparencia y Informe de Responsabilidad, hemos cerrado los sistemas para clientes que han utilizado el sistema de manera errónea. "

Dijo que en los últimos 12 meses la Oficina Nacional de Seguridad había terminado dos contratos sobre denuncias de violaciones de los derechos humanos, pero se negó a nombrar a los países involucrados.

"Cada alegación sobre el uso indebido del sistema se refiere a mí", dijo. "Constituye la confianza que damos a los clientes. Estamos investigando todas las acusaciones. "

NSO describe a sus clientes como 60 agencias de inteligencia, militares y de cumplimiento de la ley en 40 países, aunque no confirmará la identidad de ninguno de ellos, citando obligaciones de confidencialidad de los clientes. El consorcio encontró muchos de los números telefónicos en al menos 10 grupos de países, que fueron sometidos a un análisis más profundo: Azerbaiyán, Bahrein, Hungría, India, Kazajstán, México, Marruecos, Rwanda, Arabia Saudita y los Emiratos Árabes Unidos. Citizen Lab también ha encontrado evidencia de que los 10 han sido clientes de NSO, según Bill Marczak, un investigador senior.

Forbidden Stories organizó la investigación del consorcio mediático, y Amnistía proporcionó análisis y apoyo técnico, pero no tuvo ninguna aportación editorial. Amnistía ha criticado abiertamente el negocio de spyware de NSO y ha apoyado una demanda sin éxito contra la empresa en un tribunal israelí que busca revocar su licencia de exportación. Después de que la investigación comenzó, varios reporteros del consorcio supieron que ellos o sus familiares habían sido atacados con éxito con Pegasus spyware.

Más allá de las intrusiones personales hechas posibles por la vigilancia de los teléfonos inteligentes, el uso generalizado del spyware ha surgido como una amenaza principal para las democracias en todo el mundo, dicen los críticos. Los periodistas bajo vigilancia no pueden reunir de forma segura noticias sensibles sin poner en peligro a sí mismos ni sus fuentes. Los políticos de oposición no pueden trazar sus estrategias de campaña sin los que están en el poder anticipando sus movimientos. Los trabajadores de los derechos humanos no pueden trabajar con personas vulnerables, algunas de las cuales son víctimas

de sus propios gobiernos, sin exponerlas a nuevos abusos.

Por ejemplo, los forenses de Amnistía encontraron pruebas de que Pegasus fue blanco de las dos mujeres más cercanas al columnista saudí Khashoggi, quien escribió para la sección Opiniones de The Post. El teléfono de su prometida, Hatice Cengiz, fue infectado con éxito durante los días posteriores a su asesinato en Turquía el 2 de octubre de 2018, según un análisis forense del Laboratorio de Seguridad de Amnistía. También en la lista estaban el número de dos funcionarios turcos involucrados en la investigación de su desmembramiento por un equipo saudí de éxito. Khashoggi también tenía una esposa, Hanan Elatr, cuyo teléfono fue apuntado por alguien usando Pegasus en los meses antes de su asesinato. Amnistía no pudo determinar si el hack tuvo éxito.

"Esto es un software desagradable, como elocuentemente desagradable", dijo Timothy Summers, un antiguo ingeniero de ciberseguridad en una agencia de inteligencia estadounidense y ahora director de TI en la Universidad Estatal de Arizona. Con él "uno podría espiar a casi toda la población mundial. ... No hay nada malo en la construcción de tecnologías que le permita recopilar datos; es necesario a veces. Pero la humanidad no está en un lugar donde podemos tener tanto poder accesible para cualquiera. "

En respuesta a preguntas detalladas del consorcio antes de la publicación, NSO dijo en una declaración que no operaba el spyware que licenciaba a los clientes y no tenía acceso regular a los datos que recopilan. La compañía también dijo que sus tecnologías han ayudado a prevenir ataques y bombardeos y romper anillos que traficaban en drogas, sexo y niños. "Simply put, NSO El grupo está en una misión de salvar vidas, y la compañía ejecutará fielmente esta misión sin disuadir, a pesar de todos y cada uno de los intentos continuos de desacreditarlo por falsos motivos", dijo NSO. Vuestras fuentes le han proporcionado información que no tiene base fáctica, como lo demuestra la falta de documentación justificativa para muchas de las reclamaciones. "

La empresa negó que su tecnología se utilizara contra Khashoggi, o sus familiares o asociados.

"Como NSO ha declarado anteriormente, nuestra tecnología no estaba asociada de ninguna manera con el atroz asesinato de Jamal Khashoggi. Esto incluye escuchar, monitorear, rastrear o recopilar información. Anteriormente investigamos esta reclamación, inmediatamente después del atroz asesinato, que de nuevo, se está haciendo sin validación. "

Thomas Clare, abogado de difamación contratado por NSO, dijo que el consorcio había "aparentemente malinterpretado y malinterpretado datos de fuentes cruciales sobre los que dependía" y que su informe contenía hipótesis erróneas y errores fácticos.

"NSO El grupo tiene buenas razones para creer que esta lista de "miles de números telefónicos" no es una lista de números apuntados por gobiernos que utilizan Pegasus,

sino que puede ser parte de una lista más grande de números que podrían haber sido utilizados por los clientes de NSO Group para otros propósitos", escribió Clare.

En respuesta a las preguntas de seguimiento, NSO llamó al número de 50.000 "exagerado" y dijo que era demasiado grande para representar números dirigidos por sus clientes. Basándose en las preguntas que se estaban haciendo, dijo NSO, tenía razones para creer que el consorcio estaba basando sus hallazgos "en la interpretación engañosa de los datos filtrados de información básica accesible y sobresaliente, tales como los servicios de HLR Lookup, que no tienen ninguna influencia en la lista de los clientes objetivos de Pegasus o cualquier otro producto de NSO ... Todavía no vemos ninguna correlación de estas listas con nada relacionado con el uso de las tecnologías de NSO Group. "

El término HLR, o Home Location Register, se refiere a una base de datos que es esencial para operar redes de teléfonos celulares. Estos registros mantienen registros en las redes de usuarios de teléfonos celulares y sus ubicaciones generales, junto con otra información de identificación que se utiliza habitualmente en llamadas y textos de enrutamiento. Los servicios de búsqueda de HLR funcionan en el sistema SS7 que los transportistas celulares utilizan para comunicarse entre sí. Los servicios se pueden utilizar como un paso hacia el espionaje de objetivos.

El experto en seguridad de las telecomunicaciones Karsten Nohl, científico jefe de los Laboratorios de Investigación de Seguridad en Berlín, dijo que no tiene conocimiento directo de los sistemas de NSO, pero que las búsquedas de HLR y otras consultas SS7 son ampliamente y económicamente utilizadas por la industria de vigilancia, a menudo por sólo decenas de miles de dólares al año.

"No es difícil conseguir ese acceso. Dados los recursos de NSO, sería una locura asumir que no tienen acceso a SS7 de al menos una docena de países", dijo Nohl. "De una docena de países, puedes espiar al resto del mundo. "

Pegasus fue diseñado hace una década por ex-ciberespías israelíes con habilidades honradas por el gobierno. El Ministerio de Defensa de Israel debe aprobar cualquier licencia a un gobierno que desee comprarla, según declaraciones anteriores de la NSO.

"Como cuestión de política, el Estado de Israel aprueba la exportación de productos cibernéticos exclusivamente a entidades gubernamentales, para uso legal, y sólo con el propósito de prevenir e investigar la delincuencia y la lucha contra el terrorismo, bajo certificados de usuario de uso final o fin proporcionados por el gobierno adquisitivo", dijo el domingo un portavoz del establecimiento de defensa israelí. " En los casos en que se utilicen artículos exportados en violación de licencias de exportación o certificados de uso final, se adoptan medidas apropiadas. "

Los números de una docena de estadounidenses que trabajan en el extranjero se descubrieron en la lista, en todo menos un caso, mientras utilizaban teléfonos registrados

en redes celulares extranjeras. El consorcio no pudo realizar análisis forenses en la mayoría de estos teléfonos. NSO ha dicho desde hace años que su producto no puede ser utilizado para sobreveil teléfonos estadounidenses. El consorcio no encontró evidencia de la penetración exitosa de spyware en los teléfonos con el código de país de los Estados Unidos.

"También estamos de acuerdo con nuestras declaraciones anteriores de que nuestros productos, vendidos a gobiernos extranjeros examinados, no pueden utilizarse para conducir la cibersurveillancia dentro de los Estados Unidos, y ningún cliente ha recibido tecnología que les permita acceder a teléfonos con números estadounidenses", dijo la empresa en su declaración. "Es tecnológicamente imposible y reafirma el hecho de que las afirmaciones de sus fuentes no tienen mérito. "

Cómo funciona Pegasus

Objetivo: Alguien envía lo que se conoce como un enlace de trampa a un teléfono inteligente que persuade a la víctima a tocar y activar – o se activa sin ninguna entrada, como en los hacks más sofisticados "cero-clic".

Infect: El spyware captura y copia las funciones más básicas del teléfono, muestra los materiales de marketing de NSO, grabación de las cámaras y el micrófono y recopilación de datos de ubicación, registros de llamadas y contactos.

Track: El implante informa en secreto que la información a un operativo que puede utilizarla para mapear detalles sensibles de la vida de la víctima.

Apple y otros fabricantes de teléfonos inteligentes están años en un juego de gatos y ratones con NSO y otros fabricantes de spyware.

"Apple condena inequívocamente los ciberataques contra periodistas, activistas de derechos humanos y otros que buscan hacer del mundo un lugar mejor", dijo Ivan Krstić, jefe de Apple Security Engineering and Architecture. "Durante más de una década, Apple ha liderado la industria en la innovación de seguridad y, como resultado, los investigadores de seguridad aceptan que iPhone es el dispositivo móvil de consumo más seguro en el mercado. Los ataques como los descritos son altamente sofisticados, cuestan millones de dólares para desarrollarse, a menudo tienen una corta vida útil de estantería y se utilizan para apuntar a individuos específicos. Si bien eso significa que no son una amenaza para la mayoría abrumadora de nuestros usuarios, seguimos trabajando incansablemente para defender a todos nuestros clientes, y estamos agregando constantemente nuevas protecciones para sus dispositivos y datos. "

Algunas técnicas de intrusión de Pegasus detalladas en un informe de 2016 se cambiaron en cuestión de horas después de que se hicieran públicas, subrayando la capacidad de NSO para adaptarse a las contramedidas.

Pegasus está diseñado para evadir defensas en iPhones y dispositivos Android y dejar pocas huellas de su ataque. Las medidas de privacidad familiares como contraseñas fuertes y cifrado ofrecen poca ayuda contra Pegasus, que puede atacar teléfonos sin ninguna advertencia a los usuarios. Puede leer cualquier cosa en un dispositivo que un usuario pueda, al tiempo que roba fotos, grabaciones, registros de ubicación, comunicaciones, contraseñas, registros de llamadas y publicaciones de redes sociales. Spyware también puede activar cámaras y micrófonos para la vigilancia en tiempo real.

"No hay nada desde un punto de vista de cifrado para proteger contra esto", dijo Claudio Guarnieri, a.k.a "Nex", investigador italiano de 33 años del Laboratorio de Seguridad de Amnistía que desarrolló y realizó los forenses digitales en 37 smartphones que mostraron evidencia de ataques de Pegasus.

Ese sentido de la impotencia hace que Guarnieri, que a menudo se viste de cabeza a mano en negro, se sienta tan inútil como un médico del siglo XIV que enfrenta la Plaga Negra sin ningún medicamento útil. "Primarily estoy aquí sólo para mantener el recuento de muerte", dijo.

El ataque puede comenzar de diferentes maneras. Puede provenir de un enlace malicioso en un mensaje de texto SMS o un iMessage. En algunos casos, un usuario debe hacer clic en el enlace para iniciar la infección. En los últimos años, las compañías de spyware han desarrollado lo que llaman ataques "cero-clic", que entregan spyware simplemente enviando un mensaje al teléfono de un usuario que no produce notificación. Los usuarios ni siquiera necesitan tocar sus teléfonos para que empiecen las infecciones.

Muchos países tienen leyes relativas a la interceptación y la interceptación tradicionales de las comunicaciones, pero pocos tienen salvaguardias eficaces contra las intrusiones más profundas que se pueden lograr mediante la piratería en los teléfonos inteligentes. "Esto es más perverso en un sentido porque realmente ya no se trata de interceptar comunicaciones y escuchar conversación.... Esto cubre a todos y va mucho más allá de eso", dijo Guarnieri. "Ha planteado muchas preguntas no sólo de los derechos humanos, sino incluso de las leyes constitucionales nacionales en cuanto a esto es incluso legal? "

Clare, abogado de NSO, atacó los exámenes forenses como "una recopilación de supuestos especulativos e infundados" basados en supuestos basados en informes anteriores. También dijo, "NSO no tiene conocimiento de las actividades específicas de inteligencia de sus clientes. "

Las conclusiones del Proyecto Pegasus son similares a los descubrimientos anteriores de Amnistía, Citizen Lab y las organizaciones de noticias de todo el mundo, pero el nuevo informe ofrece una visión detallada de las consecuencias personales y la escala de vigilancia y sus abusos.

El consorcio analizó la lista y encontró grupos de números con códigos de país similares y enfoque geográfico que se alinean con informes previos e investigaciones adicionales sobre clientes de NSO en el extranjero. Por ejemplo, México ha sido identificado anteriormente en informes y documentos publicados como cliente de la NSO, y las entradas de la lista están agrupadas por código nacional, código de área y geografía mexicana. En varios casos, los grupos temáticos también contenían números de otros países.

En respuesta a las preguntas de los reporteros, los voceros de los países con agrupaciones o bien denegados Pegasus se utilizaron o negaron que su país había abusado de sus facultades de vigilancia.

La oficina del primer ministro húngaro Viktor Orban dijo que cualquier vigilancia llevada a cabo por esa nación se realiza de acuerdo con la ley.

"En Hungría, las instituciones gubernamentales y no gubernamentales supervisan periódicamente los órganos estatales autorizados a utilizar instrumentos encubiertos", dijo la oficina. "¿Ha hecho las mismas preguntas de los gobiernos de los Estados Unidos de América, Reino Unido, Alemania o Francia? "

Las autoridades marroquíes respondieron: Cabe recordar que las acusaciones infundadas publicadas anteriormente por Amnistía Internacional y transmitidas por Forbidden Stories ya han sido objeto de una respuesta oficial de las autoridades marroquíes, que han rechazado categóricamente esas alegaciones.

Vincent Biruta, ministro de Relaciones Exteriores de Rwanda, también negó el uso de Pegasus.

"Rwanda no utiliza este sistema de software, como se confirmó anteriormente en noviembre de 2019, y no posee esta capacidad técnica en ninguna forma", dijo Biruta. "Estas acusaciones falsas forman parte de una campaña en curso para provocar tensiones entre Rwanda y otros países, y para sembrar desinformación acerca de Rwanda en el plano nacional e internacional. "

¡Qué pregunta! '

Algunos expresaron indignación incluso por la sugerencia de espiar a los periodistas.

Un reportero del diario francés Le Monde que trabaja en el Proyecto Pegasus recientemente planteó tal pregunta al ministro de Justicia húngaro Judit Varga durante una entrevista sobre los requisitos legales para escuchar:

"Si alguien te pidiera que grabes a un periodista o a un oponente, ¿no aceptarías esto? "

¡Qué pregunta! Varga respondió. ¡Esto es una provocación en sí mismo! Un día más tarde, su oficina pidió que esta pregunta y su respuesta a ella "se borraran" de la entrevista.

En el pasado, la NSO ha culpado a sus países clientes por los presuntos abusos. NSO publicó su primer "Transparency and Responsibility Report" el mes pasado, argumentando que sus servicios son esenciales para las agencias de seguridad e inteligencia que tratan de mantenerse al día con el siglo XXI.

"Las organizaciones terroristas, los cárteles de drogas, los traficantes de seres humanos, los anillos de pedófilos y otros sindicatos de delincuentes explotan hoy las capacidades de cifrado fuera de la plataforma ofrecidas por aplicaciones móviles de mensajería y comunicaciones.

"Estas tecnologías proporcionan a los criminales y sus redes un refugio seguro, lo que les permite 'ir oscuro' y evitar la detección, comunicarse a través de sistemas de mensajería móvil impenetrables. Law enforcement and counterterrorism state agencies around the world have struggled to keep up. "

NSO también dijo que realiza exámenes rigurosos de los posibles registros de derechos humanos de los clientes antes de contraerlos e investiga informes de abusos, aunque no citó casos específicos. Afirmó que ha suspendido los contratos con cinco clientes por violaciones documentadas y que la diligencia debida de la empresa le ha costado $100 millones en ingresos perdidos. Una persona familiarizada con las operaciones de la NSO que habló con la condición de anonimato para discutir asuntos de la empresa interna señaló que en el último año la NSO había terminado los contratos con Arabia Saudita y Dubai en los Emiratos Árabes Unidos sobre cuestiones de derechos humanos.

"Pegasus es muy útil para combatir el crimen organizado", dijo Guillermo Valdes Castellanos, jefe de la agencia de inteligencia interna de México CISEN entre 2006 y 2011. "Pero la falta total de cheques y balances [en las agencias mexicanas] significa que termina fácilmente en manos privadas y se utiliza para obtener ganancias políticas y personales. " México fue el primer cliente extranjero de NSO en 2011, menos de un año después de que la firma fue fundada en Silicon Valley de Israel, en el norte de Tel Aviv.

En 2016 y 2017, más de 15.000 mexicanos aparecieron en la lista examinada por el consorcio de medios, entre ellos al menos 25 reporteros que trabajaban para los principales medios de comunicación del país, según los registros y entrevistas.

Una de ellos fue Carmen Aristegui, una de las periodistas de investigación más destacadas del país y colaboradora habitual en la CNN. Aristegui, que se ve amenazada de manera rutinaria por exponer la corrupción de políticos y cárteles mexicanos, fue previamente revelada como objetivo de Pegasus en varios informes de medios. En ese momento, dijo en una entrevista reciente, que su productor también fue blanco. Los nuevos registros y

forenses muestran que los enlaces Pegasus fueron detectados por teléfono de su asistente personal.

"Pegaso es algo que viene a tu oficina, a tu casa, a tu cama, a cada rincón de tu existencia", dijo Aristegui. "Es una herramienta que destruye los códigos esenciales de la civilización."

A diferencia de Aristegui, el reportero independiente Cecilio Pineda era desconocido fuera de su estado sureño de Guerrero. Su número aparece dos veces en la lista de 50.000. Un mes después de la segunda lista, fue abatido mientras estaba acostado en una hamaca en un lavado de coches mientras esperaba su coche. No está claro qué papel, si lo hay, la capacidad de Pegasus de geolocalizar sus objetivos en tiempo real contribuyó a su asesinato. México es uno de los países más mortíferos para periodistas; 11 fueron asesinados en 2017, según Reporteros sin Fronteras.

"Incluso si Forbidden Stories tuviera razón en que un cliente del Grupo NSO en México apuntara al número de teléfono del periodista en febrero de 2017, eso no significa que el cliente del Grupo NSO o los datos recogidos por el software del Grupo NSO estuvieran conectados de ninguna manera al asesinato del periodista el mes siguiente", escribió Clare, abogado de NSO en su carta a Forbidden Stories. "La corrupción no es igual a la causa, y los hombres armados que asesinaron al periodista pudieron haber conocido su ubicación en un lavado de coches público a través de cualquier número de medios no relacionados con NSO Group, sus tecnologías, o sus clientes. "

El Ministerio de Seguridad Pública de México reconoció el año pasado que la agencia de inteligencia nacional, CISEN y la oficina del Fiscal General adquirieron Pegasus en 2014 y suspendieron su uso en 2017 cuando la licencia venció. Los medios mexicanos también han informado que el Ministerio de Defensa utilizó el spyware.

El legado de Snowden

La próspera industria internacional de spyware data de décadas atrás, pero consiguió un impulso después de la revelación sin precedentes de documentos de la Agencia Nacional de Seguridad altamente clasificados por el contratista Edward Snowden. Ellos revelaron que la NSA podría obtener las comunicaciones electrónicas de casi cualquier persona porque tenía acceso secreto a los cables transnacionales que transportaban tráfico de Internet en todo el mundo y datos de compañías de Internet como Google y compañías gigantes de telecomunicaciones como AT&T.

Incluso los aliados de Estados Unidos en Europa se sorprendieron con la escala completa del espionaje digital estadounidense, y muchas agencias de inteligencia nacionales se pusieron a trabajar para mejorar sus propias capacidades de vigilancia. Las firmas con fines lucrativos que cuentan con jubilados de los servicios de inteligencia vieron un mercado lucrativo libre de las normas gubernamentales y la supervisión impuestas a otras industrias

La dramática expansión del cifrado de extremo a extremo por parte de Google, Microsoft, Facebook, Apple y otras grandes empresas tecnológicas también incitaron a los agentes de la ley y los funcionarios de inteligencia a que se quejaran de que habían perdido el acceso a las comunicaciones de objetivos criminales legítimos. Eso a su vez generó más inversión en tecnologías, como Pegasus, que funcionaron apuntando a dispositivos individuales.

"Cuando construyes un edificio, quieres asegurarte de que el edificio se mantenga, así que seguimos ciertos protocolos", dijo Ido Sivan-Sevilla, experto en cibergobernabilidad en la Universidad de Maryland. Al promover la venta de herramientas de vigilancia privada no reguladas, "incentivamos edificios de construcción que pueden ser rotos. Estamos construyendo un monstruo. Necesitamos un tratado de normas internacionales que diga que ciertas cosas no están bien."

Sin normas y reglas internacionales, existen ofertas secretas entre empresas como NSO y los países que prestan servicios.

El uso sin trabas de un spyware militar como Pegasus puede ayudar a los gobiernos a suprimir el activismo cívico en un momento en que el autoritarismo está en aumento en todo el mundo. También da a los países sin la sofisticación técnica de naciones líderes como Estados Unidos, Israel y China la capacidad de conducir ciberespionaje digital mucho más profundo que nunca.

Tu cuerpo deja de funcionar'

Azerbaiyán, aliado de Israel desde hace mucho tiempo, ha sido identificado como cliente de la NSO por Citizen Lab y otros. El país es una kleptocracia de gestión familiar sin elecciones libres, sin sistema judicial imparcial y sin medios de comunicación independientes. El antiguo territorio soviético ha sido gobernado desde que la Unión Soviética colapsó hace 30 años por la familia Aliyev, cuyo robo de los planes de riqueza y blanqueo de dinero del país en el extranjero ha dado lugar a embargos extranjeros, sanciones internacionales y acusaciones penales.

A pesar de las dificultades, aproximadamente tres docenas de periodistas azerbaiyanos siguen documentando la corrupción de la familia. Algunos se esconden dentro del país, pero la mayoría fueron forzados al exilio donde no son tan fáciles de capturar. Algunos trabajan para la Radio Free Europe/Radio Liberty, con sede en Praga, que fue expulsada del país en 2015 para su presentación. Los demás trabajan para una organización sin fines de investigación denominada Proyecto de denuncias contra la delincuencia organizada y la corrupción, con sede en Sarajevo, la capital bosnia, y es uno de los asociados del Proyecto Pegasus.

El principal periodista investigador de la región es Khadija Ismayilova, a quien el régimen ha trabajado durante un decenio para silenciar: Se plantó una cámara secreta en su pared de apartamento, tomó videos de su tener sexo con su novio y luego los publicó en Internet en

2012; fue arrestada en 2014, juzgada y condenada por la superación de impuestos y otros cargos, y retenida en celdas de prisión con delincuentes endurecidos. Tras la indignación mundial y la intervención de alto perfil del abogado de derechos humanos Amal Clooney, fue liberada en 2016 y sometida a una prohibición de viajar.

"Es importante que la gente vea ejemplos de periodistas que no se detienen porque fueron amenazados", dijo Ismayilova en una entrevista reciente. "Es como una guerra. Dejas tu trinchera, entonces entra el atacante... Usted tiene que mantener su posición, de lo contrario se tomará y entonces usted tendrá menos espacio, menos espacio, el espacio se reducirá y entonces usted encontrará difícil respirar."

El mes pasado, su salud falló, se le permitió salir del país. Colleagues arregló para probar su teléfono inteligente inmediatamente. Forenses por Security Lab determinaron que Pegasus había atacado y penetrado su dispositivo numerosas veces desde marzo de 2019 hasta mayo de este año.

Había asumido algún tipo de vigilancia, dijo Ismayilova, pero todavía estaba sorprendida por el número de ataques. "Cuando piensas que tal vez hay una cámara en el baño, tu cuerpo deja de funcionar", dijo. "Yo pasé por esto, y durante ocho o nueve días no pude usar el inodoro, en ningún lugar, ni siquiera en lugares públicos. Mi cuerpo dejó de funcionar."

Dejó de comunicarse con la gente porque el que habló terminó hostigado por los servicios de seguridad. "No confías en nadie, y luego tratas de no tener planes a largo plazo con tu propia vida porque no quieres que ninguna persona tenga problemas por tu culpa. "

La confirmación de la penetración de Pegasus la arrastró. "Mis miembros de la familia también son victimizados. Las fuentes son victimizadas. Personas He estado trabajando con gente que me dijo que sus secretos privados son victimizados", dijo.
"Es despreciable. ... No sé quién más ha estado expuesto por mí, quién más está en peligro por mí.."

¿El ministro es paranoico o sensible?

El miedo a la vigilancia generalizada impide a los ya difíciles mecánicos del activismo cívico.

"A veces, ese miedo es el punto", dijo John Scott-Railton, investigador senior de Citizen Lab, quien ha investigado ampliamente a Pegasus. "La dificultad psicológica y la autocensura que causa son herramientas clave de los dictadores y autoritarios modernos."

Cuando Siddharth Varadarajan, cofundador del Wire, una salida en línea independiente en la India, supo que el análisis del laboratorio de seguridad mostró que su teléfono había sido atacado y penetrado por Pegasus, su mente corrió inmediatamente a través de sus fuentes sensibles. Pensó en un ministro del gobierno del Primer Ministro Narendra Modi que había mostrado una preocupación inusual sobre la vigilancia cuando se reunieron.

El ministro primero movió la reunión de un lugar a otro en el último momento, luego se apagó el teléfono y le dijo a Varadarajan que hiciera lo mismo.

Luego "los dos teléfonos fueron puestos en una habitación y la música fue puesta en esa habitación... y pensé: 'Chico, este tipo es realmente paranoico. Pero tal vez estaba siendo sensible", dijo Varadarajan en una entrevista reciente.

Cuando los forenses mostraron que su teléfono había sido penetrado, él sabía el sentimiento mismo. "Te sientes violado, no hay duda de ello", dijo. "Esta es una intrusión increíble, y los periodistas no deben tener que lidiar con esto. Nadie debería tener que lidiar con esto."

Fuente:

https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones/?itid=hp-top-table-main

Q&A A guide to "spyware"

Vigilancia invisible: Cómo spyware está secretamente hackeando teléfonos inteligentes

https://yewtu.be/watch?v=R0RVl7bghj8

Takeaways from the Pegasus Project

El spyware de grado militar alquilado por la firma israelí NSO Group a gobiernos para el seguimiento de terroristas y criminales fue utilizado en intentos y exitosos hacks de 37 teléfonos inteligentes pertenecientes a periodistas, activistas de derechos humanos, ejecutivos de negocios y las dos mujeres más cercanas al periodista saudí asesinado Jamal

Khashoggi, según una investigación de The Washington Post y 16 socios de medios liderados por la organización sin fines de lucro Forbidden Stories.

Forbidden Stories y Amnistía Internacional, un grupo de derechos humanos, tuvieron acceso a una lista de más de 50.000 números y la compartieron con las organizaciones de noticias, que realizaron nuevas investigaciones y análisis. El Laboratorio de Seguridad de Amnistía hizo un examen forense de los teléfonos.

Aquí están los principales secuestradores de la investigación:

Teléfonos identificados de una lista de esguinces: Treinta y siete teléfonos inteligentes dirigidos aparecieron en una lista de más de 50.000 números que se concentran en países conocidos para vigilar a sus ciudadanos y también conocidos por haber sido clientes de NSO Group, un líder mundial en la creciente y en gran parte no regulada industria de spyware privado, la investigación encontró. La lista no identifica quién puso los números en él, o por qué, y se desconoce cuántos de los teléfonos fueron dirigidos o vigilados. Pero el análisis forense de los 37 teléfonos muestra que muchos muestran una estrecha correlación entre sellos de tiempo asociados con un número en la lista y la iniciación de intentos de vigilancia, en algunos casos tan breve como unos segundos.

Políticos, periodistas, activistas encontrados en la lista: Los números de la lista no están atribuidos, pero los reporteros pudieron identificar a más de 1.000 personas que abarcaban más de 50 países mediante investigaciones y entrevistas en cuatro continentes: varios miembros de la familia real árabe, por lo menos 65 ejecutivos de negocios, 85 activistas de derechos humanos, 189 periodistas y más de 600 políticos y funcionarios gubernamentales, incluyendo ministros de gabinete, diplomáticos y oficiales militares y de seguridad, así como 10 primeros ministros, tres presidentes y un rey. El propósito de la lista no puede determinarse de manera concluyente.

La empresa dice que policía a sus clientes por abusos: El objetivo de los 37 teléfonos inteligentes parecería estar en conflicto con el propósito declarado de la licencia de NSO del spyware Pegasus, que la compañía dice que está destinado sólo para el uso en la vigilancia de terroristas y delincuentes principales. Las pruebas extraídas de estos teléfonos inteligentes, reveladas aquí por primera vez, ponen en duda las promesas de la empresa israelí a la policía de sus clientes por abusos de derechos humanos. NSO El Jefe Ejecutivo Shalev Hulio dijo el domingo que estaba "muy preocupado" por los informes de The Post. "Estamos comprobando cada denuncia, y si algunas de las acusaciones son ciertas, tomaremos medidas severas, y terminaremos contratos como lo hicimos en el pasado". Agregó: "Si alguien hacía algún tipo de vigilancia sobre los periodistas, aunque no fuera por Pegasus, es inquietante."

Apple iPhone mostró ser vulnerable: El descubrimiento de una lista de números telefónicos de 37 smartphones que habían sido penetrados o atacados con Pegasus spyware alimenta el debate sobre si Apple ha hecho lo suficiente para garantizar la

seguridad de sus dispositivos, popularizó el mundo por su reputación de resistir los intentos de piratería. Treinta y cuatro de los 37 eran iPhones.

Los nuevos detalles de la piratería tienen implicaciones mundiales: Entre los 37 teléfonos confirmados que han sido blanco, 10 estaban en la India y otros cinco en Hungría, la mayoría vinculados a periodistas, activistas o empresarios. La conclusión añadirá preocupaciones sobre la vigilancia del gobierno extralegal realizada con spyware privado en ambos países. Cientos más de India y Hungría aparecen en la lista global más amplia. Un tercer país, México, fue el hogar de casi un tercio de los números de la lista, añadiendo preguntas sobre su uso pasado del software Pegasus. Cada país dice que actúa legalmente en la realización de cualquier actividad de vigilancia.

Una princesa corrió para escapar: En los años transcurridos desde que los comandos arrastraron a la Princesa Latifa, hija del gobernante de Dubái, desde su yate en el Océano Índico en 2018, sus amigos y asociados se han preguntado: ¿Cómo se ha frustrado su cuidadoso plan de escape? Una nueva investigación muestra que en los días después de su desaparición, su número de teléfono y los de amigos fueron añadidos a una lista que también incluye números de teléfonos dirigidos por el poderoso spyware Pegasus. Los números para la esposa despreocupada del gobernante, la Princesa Haya, y miembros de su equipo legal y de seguridad también fueron introducidos en la lista cuando huyó más tarde a Londres. La vigilancia de las princesas fue entre las razones por las que el dueño del spyware, NSO Group, rescindió el contrato de Dubai, una persona familiarizada con las operaciones de la empresa dijo The Post.

Fuente:

https://www.washingtonpost.com/investigations/2021/07/18/takeaways-nso-pegasus-project/

Revelado: la filtración descubre abuso mundial de armas de cibervigilancia

Spyware vendido a regímenes autoritarios utilizados para atacar a activistas, políticos y periodistas, los datos sugieren

Los activistas de derechos humanos, periodistas y abogados de todo el mundo han sido blanco de gobiernos autoritarios usando software de piratería vendido por la compañía de vigilancia israelí NSO Group, según una investigación de una fuga masiva de datos.

La investigación de The Guardian y otras 16 organizaciones de medios sugiere un abuso generalizado y continuado del spyware de la piratería de NSO, Pegasus, que la compañía insiste que sólo está destinado a usar contra criminales y terroristas.

Pegasus es un malware que infecta a los dispositivos iPhones y Android para permitir a los operadores de la herramienta extraer mensajes, fotos y correos electrónicos, grabar llamadas y activar secretamente los micrófonos.
La filtración contiene una lista de más de 50.000 números de teléfono que, se cree, han sido identificados como los de personas de interés por los clientes de NSO desde 2016.

Forbidden Stories, una organización mediática sin fines de lucro de París, y Amnistía Internacional tuvo acceso inicialmente a la lista filtrada y acceso compartido con socios de medios como parte del proyecto Pegasus, un consorcio de información

La presencia de un número de teléfono en los datos no revela si un dispositivo fue infectado con Pegasus o sujeto a un intento de hackeo. Sin embargo, el consorcio cree que los datos son indicativos de los posibles objetivos que los clientes del gobierno de NSO identificaron antes de posibles intentos de vigilancia.

Guía rápida

¿Qué hay en los datos del proyecto Pegasus?

¿Qué hay en la filtración de datos?

La filtración de datos es una lista de más de 50.000 números telefónicos que, desde 2016, se cree que han sido seleccionados como personas de interés por clientes gubernamentales del NSO Group, que vende software de vigilancia. Los datos también contienen el tiempo y la fecha en que los números fueron seleccionados o ingresados en un sistema. Forbidden Stories, una organización de periodismo sin fines de lucro de París, y Amnistía Internacional inicialmente tuvo acceso a la lista y acceso compartido con 16 organizaciones de medios, incluyendo el Guardian. Más de 80 periodistas han trabajado juntos durante varios meses como parte del proyecto Pegasus. El Laboratorio de Seguridad de Amnistía, socio técnico del proyecto, hizo los análisis forenses.

¿Qué indica la filtración?

El consorcio cree que los datos indican los objetivos potenciales de los clientes del gobierno de NSO identificados con antelación de la posible vigilancia. Si bien los datos son una indicación de intención, la presencia de un número en los datos no revela si hubo un intento de infectar el teléfono con spyware como Pegasus, la herramienta de vigilancia de firmas de la empresa, o si algún intento tuvo éxito. La presencia en los datos de un número muy pequeño de líneas de tierra y números estadounidenses, que NSO dice que son "técnicamente imposibles" de acceder con sus herramientas, revela que algunos objetivos fueron seleccionados por los clientes de NSO, aunque no pudieron infectarse con Pegasus. Sin embargo, los exámenes forenses de una pequeña muestra de teléfonos móviles con números en la lista encontraron correlaciones estrechas entre el tiempo y la fecha de un número en los datos y el comienzo de la actividad Pegasus - en algunos casos tan poco como unos segundos.

¿Qué revela el análisis forense?

Amnistía examinó 67 teléfonos inteligentes en los que se sospechaba que se habían cometido ataques. De ellos, 23 fueron infectados con éxito y 14 mostraron signos de intento de penetración. Para los 30 restantes, las pruebas eran inconclusivas, en varios casos porque los teléfonos habían sido reemplazados. Quince de los teléfonos eran dispositivos Android, ninguno de los cuales mostraba evidencia de infección exitosa. Sin embargo, a diferencia de los iPhones, los teléfonos que usan Android no registran el tipo de

información necesaria para el trabajo de detective de Amnistía. Tres teléfonos Android mostraban signos de segmentación, como mensajes SMS conectados con Pegasus.

Amnistía compartió "copias de respaldo" de cuatro iPhones con Citizen Lab, un grupo de investigación en la Universidad de Toronto que se especializa en estudiar Pegasus, lo que confirmó que mostraban signos de infección por Pegasus. Citizen Lab también llevó a cabo una revisión por pares de los métodos forenses de Amnistía, y los halló sonoros.

¿Qué clientes de NSO estaban seleccionando números?

Si bien los datos se organizan en grupos, indicativos de clientes individuales de la NSO, no dice cuál cliente de la NSO fue responsable de seleccionar un número determinado. NSO afirma vender sus herramientas a 60 clientes en 40 países, pero se niega a identificarlos. Al examinar detenidamente la pauta de los clientes individuales en los datos filtrados, los asociados de los medios de comunicación pudieron identificar a 10 gobiernos que se consideraban responsables de seleccionar los objetivos: Azerbaiyán, Bahrein, Kazajstán, México, Marruecos, Rwanda, Arabia Saudita, Hungría, India y los Emiratos Árabes Unidos. Citizen Lab también ha encontrado evidencia de que los 10 son clientes de NSO.

¿Qué dice NSO Group?

Puede leer la declaración completa de NSO Group aquí.
https://www.theguardian.com/news/2021/jul/18/response-from-nso-and-governments

La compañía siempre ha dicho que no tiene acceso a los datos de los objetivos de sus clientes. A través de sus abogados, NSO dijo que el consorcio había hecho "suposiciones incorrectas" sobre las cuales los clientes utilizan la tecnología de la empresa. Dijo que el número de 50.000 fue "exagerado" y que la lista no podía ser una lista de números "tratados por los gobiernos que utilizan Pegasus". Los abogados dijeron que NSO tenía razones para creer que la lista a la que se accede por el consorcio "no es una lista de números dirigidos por gobiernos que utilizan Pegasus, sino que puede ser parte de una lista más grande de números que podrían haber sido utilizados por los clientes del Grupo NSO para otros fines". Dijeron que era una lista de números que cualquiera podía buscar en un sistema de código abierto. Después de más preguntas, los abogados dijeron que el consorcio basó sus hallazgos "sobre la interpretación engañosa de datos filtrados de información básica accesible y sobresaliente, tales como los servicios de HLR Lookup, que no tienen ninguna relación con la lista de objetivos de los clientes de Pegasus o cualquier otro producto de NSO ... todavía no vemos ninguna correlación de estas listas con nada relacionado con el uso de las tecnologías del Grupo NSO". Después de la publicación, explicaron que consideraban un blanco como un teléfono que era objeto de una infección exitosa o tentativa (pero fallida) por Pegasus, y reiteraron que la lista de 50.000 teléfonos era demasiado grande para que representara objetivos de Pegasus. Ellos dijeron que el hecho que un numero apareciera en la lista, de ninguna manera indicaba si habian sido seleccionados para vigilancia usando Pegasus.

¿Qué son los datos de búsqueda de HLR?

El término HLR, o registro de ubicación en casa, se refiere a una base de datos que es esencial para operar redes de teléfonos móviles. Estos registros mantienen registros en las redes de usuarios telefónicos y sus ubicaciones generales, junto con otra información de identificación que se utiliza habitualmente en llamadas y textos de enrutamiento. Los expertos en telecomunicación y vigilancia dicen que los datos de HLR a veces se pueden utilizar en la fase temprana de un intento de vigilancia, al identificar si es posible conectarse a un teléfono. El consorcio entiende que los clientes de NSO tienen la capacidad a través de una interfaz en el sistema Pegasus para realizar consultas de búsqueda HLR. No está claro si los operadores de Pegasus están obligados a realizar investigaciones de búsqueda de HRL a través de su interfaz para utilizar su software; una fuente de NSO destacó que sus clientes pueden tener diferentes razones - no relacionadas con Pegasus - para realizar búsquedas de HLR a través de un sistema NSO.

El análisis forense de un pequeño número de teléfonos cuyos números aparecieron en la lista filtrada también mostró más de la mitad tenía rastros del spyware Pegasus.

El Guardián y sus socios mediáticos revelarán las identidades de personas cuyo número apareció en la lista en los próximos días. Incluyen cientos de ejecutivos de negocios, personalidades religiosas, académicos, empleados de ONG, funcionarios sindicales y funcionarios gubernamentales, incluyendo ministros de gabinete, presidentes y primeros ministros.

La lista también contiene el número de familiares cercanos del gobernante de un país, sugiriendo que el gobernante puede haber instruido a sus agencias de inteligencia para explorar la posibilidad de supervisar a sus propios familiares.

Las revelaciones comienzan el domingo, con la revelación de que el número de más de 180 periodistas se enumeran en los datos, incluyendo reporteros, editores y ejecutivos del Financial Times, CNN, el New York Times, Francia 24, el economista, Associated Press y Reuters.

El número de teléfono de un reportero mexicano independiente, Cecilio Pineda Birto, fue encontrado en la lista, aparentemente de interés para un cliente mexicano en las semanas anteriores a su asesinato, cuando sus asesinos pudieron localizarlo en un lavado de autos. Su teléfono nunca se ha encontrado así que no se ha podido determinar si se infectó.

NSO dijo que incluso si el teléfono de Pineda había sido apuntado, no significaba que los datos recogidos de su teléfono contribuyeran de ninguna manera a su muerte, subrayando que los gobiernos podrían haber descubierto su ubicación por otros medios. Fue entre al menos 25 periodistas mexicanos, aparentemente seleccionados como candidatos para la vigilancia durante un período de dos años.

Sin un examen forense de dispositivos móviles, es imposible decir si los teléfonos fueron sometidos a un intento de hackeo o exitoso usando Pegasus.

NSO siempre lo ha mantenido "no opera los sistemas que vende a clientes gubernamentales examinados, y no tiene acceso a los datos de los objetivos de sus clientes".

En declaraciones emitidas por sus abogados, la NSO negó "falsas reclamaciones" sobre las actividades de sus clientes, pero dijo que "continuaría investigando todas las afirmaciones creíbles de uso indebido y tomar medidas apropiadas". Dijo que la lista no podría ser una lista de números "tratados por los gobiernos usando Pegasus", y describió la figura de 50.000 como "exagerado".

La empresa vende sólo a agencias militares, policiales y de inteligencia en 40 países sin nombre, y dice que ve rigurosamente los registros de derechos humanos de sus clientes antes de permitirles utilizar sus herramientas de espionaje.

El Ministro de Defensa de Israel regula estrechamente las OSN, otorgando licencias individuales de exportación antes de que su tecnología de vigilancia pueda venderse a un nuevo país.

El mes pasado, NSO publicó un informe de transparencia en el que afirmaba tener un enfoque líder en la industria de los derechos humanos y publicó extractos de contratos con clientes que estipulaban que sólo debían utilizar sus productos para investigaciones penales y nacionales de seguridad.

No hay nada que indique que los clientes de NSO no utilizaron también Pegasus en investigaciones de terrorismo y delitos, y el consorcio también encontró números en los datos pertenecientes a presuntos delincuentes.

Sin embargo, la amplia gama de números de la lista pertenecientes a personas que aparentemente no tienen conexión con la delincuencia sugiere que algunos clientes de la NSO están violando sus contratos con la empresa, espiando a activistas prodemocracia y periodistas que investigan la corrupción, así como opositores políticos y críticos gubernamentales.

Esa tesis está respaldada por análisis forenses en los teléfonos de una pequeña muestra de periodistas, activistas de derechos humanos y abogados cuyos números aparecieron en la lista filtrada. La investigación, realizada por el Laboratorio de Seguridad de Amnistía, socio técnico del proyecto Pegasus, encontró rastros de actividad Pegasus en 37 de los 67 teléfonos examinados.
El análisis también descubrió algunas correlaciones secuenciales entre el tiempo y la fecha se introdujo un número en la lista y el inicio de la actividad Pegasus en el dispositivo, que en algunos casos ocurrió sólo unos segundos después.

Amnistía compartió su trabajo forense en cuatro iPhones con Citizen Lab, un grupo de investigación de la Universidad de Toronto que se especializa en estudiar Pegasus, lo que confirmó que mostraba signos de infección por Pegasus. Citizen Lab también llevó a cabo una revisión entre pares de los métodos forenses de Amnistía, y los encontró sonoros.

El análisis del consorcio de los datos filtrados identificó al menos 10 gobiernos que se creían clientes de la NSO que estaban entrando en un sistema: Azerbaiyán, Bahrein, Kazajstán, México, Marruecos, Rwanda, Arabia Saudita, Hungría, India y Emiratos Árabes Unidos (EAU).

El análisis de los datos sugiere que el país cliente de la NSO que más números seleccionaron -más de 15.000- fue México, donde se sabe que varias agencias gubernamentales diferentes han comprado Pegasus. Tanto Marruecos como los Emiratos Árabes Unidos seleccionaron más de 10.000 números, el análisis sugirió.

Los números de teléfono que fueron seleccionados, posiblemente antes de un ataque de vigilancia, abarcaron más de 45 países en cuatro continentes. Hubo más de 1.000 números en países europeos que, según el análisis, fueron seleccionados por clientes de la NSO.

La presencia de un número en los datos no significa que hubo un intento de infectar el teléfono. NSO dice que había otros propósitos posibles para que los números se registraran en la lista.

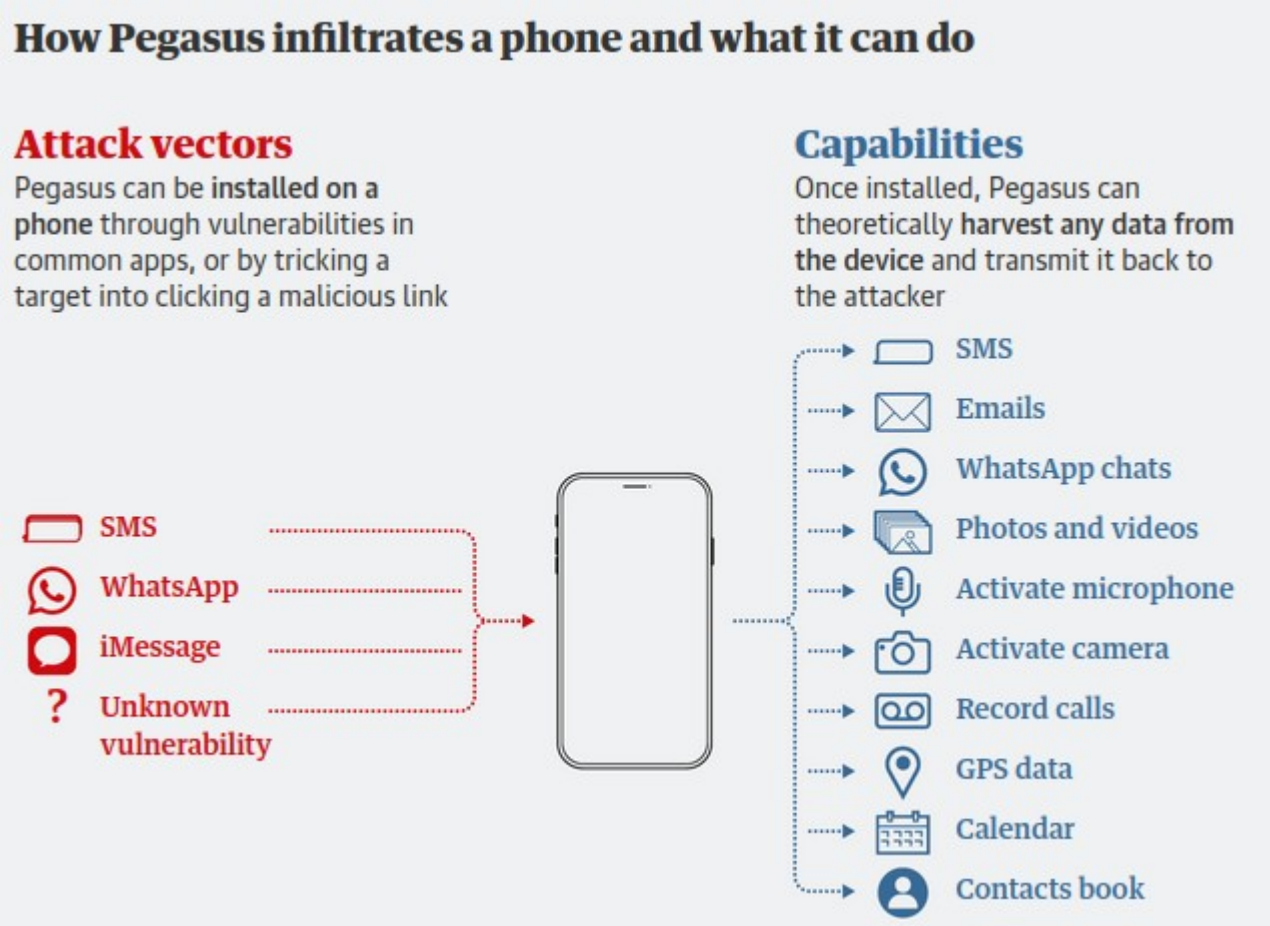
Rwanda, Marruecos, India y Hungría negaron haber utilizado Pegasus para hackear los teléfonos de los individuos nombrados en la lista. Los gobiernos de Azerbaiyán, Bahrein, Kazajstán, Arabia Saudita, México, Emiratos Árabes Unidos y Dubai no respondieron a las invitaciones a formular observaciones.

Es probable que el proyecto Pegasus estimule debates sobre la vigilancia gubernamental en varios países sospechosos de utilizar la tecnología. La investigación sugiere que el gobierno húngaro de Viktor Orbán parece haber implementado la tecnología de NSO como parte de su llamada guerra contra los medios de comunicación, dirigiendo a periodistas de investigación en el país, así como el círculo cercano de uno de los pocos ejecutivos de medios independientes de Hungría.

Los datos filtrados y los análisis forenses también sugieren que la herramienta espía de NSO fue utilizada por Arabia Saudita y su aliado cercano, los EAU, para apuntar los teléfonos de asociados cercanos del periodista asesinado de Washington Post Jamal Khashoggi en los meses posteriores a su muerte. El fiscal turco que investigaba su muerte también era un candidato para atacar, sugiere la fuga de datos.

Claudio Guarnieri, que dirige el Laboratorio de Seguridad de Amnistía Internacional, dijo que una vez que un teléfono estaba infectado con Pegasus, un cliente de NSO podría en efecto tomar el control de un teléfono, permitiéndoles extraer los mensajes, llamadas, fotos

y correos electrónicos de una persona, activar secretamente cámaras o micrófonos, y leer el contenido de aplicaciones de mensajería cifradas como WhatsApp, Telegram y Signal.



Al acceder a los sensores de GPS y hardware en el teléfono, agregó, los clientes de NSO también podrían asegurar un registro de los movimientos pasados de una persona y rastrear su ubicación en tiempo real con precisión de punta, por ejemplo estableciendo la dirección y la velocidad en la que viajaba un coche.

Los últimos avances en la tecnología de NSO le permiten penetrar teléfonos con ataques "cero-clic", lo que significa que un usuario ni siquiera necesita hacer clic en un enlace malicioso para que su teléfono esté infectado.

Guarnieri ha identificado evidencia NSO ha estado explotando vulnerabilidades asociadas con iMessage, que viene instalado en todos los iPhones, y ha sido capaz de penetrar incluso el iPhone más actualizado que ejecuta la última versión de iOS. El análisis forense de su equipo descubrió las infecciones exitosas y tentativas de Pegasus de teléfonos tan recientemente como este mes.

Apple dijo: "Los investigadores de seguridad aceptan que iPhone es el dispositivo móvil de consumo más seguro y seguro del mercado. "

NSO se negó a dar detalles específicos sobre sus clientes y la gente a la que se dirigían.

Sin embargo, una fuente familiarizada con el asunto dijo que el promedio de objetivos anuales por cliente era de 112. La fuente dijo que la compañía tenía 45 clientes por su spyware Pegasus.

Fuente :

https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus

Otro artículo que queda por traducir :

Forensic Methodology Report: How to catch NSO Group's Pegasus

https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/

Zuboff Shoshana - La Era Del Capitalismo De La Vigilancia

https://publicar.argentina.indymedia.org/?p=6666