El programa **Pegasus** de la empresa israelí NSO, que supuestamente sirvió para espiar a activistas, periodistas y opositores del mundo entero, es un sistema muy sofisticado que explota constantemente las vulnerabilidades de los teléfonos móviles inteligentes (*smartphones*).

Una vez se introduce en el teléfono móvil, Pegasus exporta los datos del usuario (correos electrónicos, mensajería, fotografías, etc) hacia páginas de internet creadas por NSO, que se renuevan constantemente para evitar ser detectadas.

Es “como si dejaras tu teléfono en manos de otra persona”, advierte Alan Woodward, profesor en ciberseguridad de la Universidad de Surrey (Reino Unido).

Esta transmisión de información pasa completamente desapercibida para el usuario y es muy difícil encontrar cualquier prueba de este espionaje en los teléfonos Android. Por este motivo, la investigación de Amnistía Internacional, revelada el domingo, se basó en móviles Apple.

-¿Cómo se piratea el teléfono de la víctima?-

En su controvertido pasado, muy bien documentado por Amnistía, NSO utilizó SMS trampa, *bugs* en Whatsapp, en iMessage, Apple Music...

Hace unos años, se requería una acción del usuario, como clicar en un enlace, para que se

produjera el pirateo del teléfono.

Pero ahora ya ni siquiera se necesita este gesto del propietario para que Pegasus pueda introducirse en su *smartphone*.

-¿Cómo NSO encuentra fallos en los teléfonos para introducirse en ellos?-

Con más de mil empleados, NSO es una gran empresa que tiene contratados a piratas informáticos de élite y esto le permite encontrar constantemente fallos en los teléfonos para introducirse en ellos.

Según expertos, también suele recurrir al “mercado negro” en el que investigadores en ciberseguridad, con muy poca moral, suelen comercializar las fallas que sirven como puerta de entrada.

Las fallas más apreciadas se conocen como *zero days* y se trata de errores que nadie antes había detectado y que resultan difíciles de solucionar.

Según Bastien Bobe, director técnico en el sur de Europa de Lookout, editora de un programa de protección de *smartphones*, los *zero days* más valioso pueden comercializarse por hasta 2 millones de dólares en iOS (sistema operativo de Apple) y 2.5 millones en Android.

-¿Se puede evitar este tipo de espionaje?-

Sí y no.

Algunas precauciones sencillas pueden dificultar el pirateo, como actualizar su teléfono o apagarlo una vez al día, dado que este tipo de acciones dificultan el funcionamiento de estos

programas de espionaje.

También pueden comprarse algunos programas para mejorar la seguridad del móvil, pero estos cuentan con pocos usuarios, “ya que la gente se siente más segura con su teléfono que con el ordenador”, lamenta Bobe.

Según reconoce este especialista, ninguna acción garantiza una protección total.

“Si alguien quiere hacerse con el control de un *smartphone* y dispone de medios importantes para ello (...), como varios millones o decenas de millones, lo conseguirá”, afirma.

Por este motivo, recomienda que aquellas personas que disponen de informaciones sensibles o codiciadas es mejor que utilicen viejos teléfonos móviles no inteligentes.

Reportan que el móvil del presidente de Francia fue un objetivo de un ‘software’ de vigilancia por parte de Marruecos

Uno de los números de móvil que el presidente francés, Emmanuel Macron, ha utilizado desde al menos 2017 se encuentra en la lista de números seleccionados por un servicio de seguridad de Marruecos para el 'hackeo' potencial mediante el 'software' de espionaje israelí Pegasus, **i nforma**
Le Monde.

El medio francés también ha revelado que los números de teléfono de **Edouard Philippe**, entonces primer ministro, así como de otros
catorce miembros del Gobierno
francés, se convirtieron en objetivos del 'spyware' por decisión del servicio secreto de Rabat a partir de marzo de 2019.

Estos números forman parte de una lista de más de **50.000 números** obtenidos por la

organización periodística sin fines de lucro
Forbidden Stories
, con sede en Francia, y el grupo de derechos humanos
Amnistía Internacional
, que ha sido compartida con 17 medios de comunicación, entre ellos Le Monde.

La investigación realizada por estas entidades concluye que el 'software' espía Pegasus, cuya licencia vende la empresa de vigilancia israelí **NSO Group** a los gobiernos para que rastreen a terroristas y criminales, fue utilizado para 'hackear' los teléfonos inteligentes de periodistas, activistas, ejecutivos de negocios y políticos en todo el mundo.

Los números de la lista no están atribuidos, pero se logró identificar a más de 1.000 personas en más de 50 países, entre ellos varios miembros de la familia real de Arabia Saudita, al menos 65 ejecutivos de negocios, 85 activistas de derechos humanos, 189 periodistas y **dos mujeres cercanas al periodista**
saudita Jamal
Khashoggi,
asesinado en 2018. La lista también contiene los
números de varios jefes de Estado y primeros ministros
, y los de más de 600 políticos y funcionarios gubernamentales, incluidos ministros de gabinete, diplomáticos y oficiales militares y de seguridad.

Entre los periodistas cuyos números están en la lista, los hay que trabajan para los medios estadounidenses CNN, Associated Press, Voice of America, The New York Times, The Wall Street Journal y Bloomberg News, así como para el francés Le Monde, el Financial Times británico y Al Jazeera, de Catar, entre otros.

Según la investigación, varios de los números de la lista **se concentraron en 10 países**: Azerbaiyán, Baréin, Hungría, India, Kazajistán, México, Marruecos, Ruanda, Arabia Saudita y los Emiratos Árabes Unidos. Se descubrió también que esas 10 naciones han sido clientes de NSO Group.

Análisis: ¿Cómo intenta Pegasus intervenir tu teléfono?

Eliana Gilet

La investigación coordinada por las organizaciones no gubernamentales Forbbiden Stories y Amnistía Internacional que se compartió con 17 medios de comunicación reveló que al menos diez gobiernos del mundo han utilizado la plataforma Pegasus, de la empresa israelí NSO Group, para intentar intervenir los teléfonos de más de 180 periodistas.

Según la información publicada, pudo identificarse que al menos veinte y cinco fueron de México, los casos tuvieron lugar durante los años 2016 y 2017, durante el Gobierno de Enrique Peña Nieto. Dichos periodistas formaban parte de las redacciones de la revista Proceso, del equipo de Carmen Aristegui, del diario La Jornada y de Quinto Elemento Lab, entre otros. La lista incluye a Cecilio Pineda, periodista asesinado en Iguala, Guerrero, el 2 de marzo de 2017.

Sputnik conversó con Alejandra Xanic, fundadora de Quinto Elemento Lab, una de las periodistas mexicanas que sufrió un intento de intervención telefónica con el malware Pegasus, en el año 2016.

"Lo que más me asombró de esta nueva revelación sobre Pegasus fue su escala. Fue impresionante que estuviésemos bajo vigilancia entonces, nos sentimos vulnerables pero esta la dimensión de esta nueva revelación tiene unos alcances que, me pregunto ¿por qué un Estado hace eso?", dijo Xanic en entrevista con Sputnik.

Los 180 periodistas forman parte de una amplia lista de más de 50.000 teléfonos analizados por el consorcio de investigación que sufrieron intentos de intervención con el programa israelí en más de 50 países.

Un mensaje raro

Alejandra Xanic tiene que hacer memoria para recordar los detalles de los episodios que hoy son la evidencia de un intento de intervención de su teléfono celular ocurrido en 2016, según lo comprobó primero Citizen Lab y Social Tic; y ahora, la investigación de marras.

"No recuerdo las fechas exactas, pero sí recuerdo que estaba reporteando el caso de la masacre de Allende, Coahuila, que involucraba a narcotraficantes, rozaba a la DEA (la Agencia antidrogas de Estados Unidos) y al Gobierno mexicano. Fue en el curso de ese año que empecé a notar que llegaban SMS raros", dijo la periodista de amplia trayectoria en México y a nivel internacional.

Relató que ella no está suscrita a ningún tipo de servicio que utilice mensajes de texto, y que el primero que le llamó la atención venía disfrazado como uno de UnoTV, una cadena de noticias que suele enviar los titulares del día por SMS a los teléfonos sin que uno haya pedido tal servicio, adjuntando una liga para acceder a las notas.

"UnoTv me enviaba mensajes que jamás abría, pero en alguno hice click y me pareció que la liga no era la correcta y lo cerré de inmediato. Más adelante, me llegaron más mensajes extraños, uno decía "ya viste la nota que salió en Milenio, involucran a Nacho en corrupción o lavado de dinero", recordó Xanic.

Nacho es Ignacio Rodríguez Reyna, otro de los fundadores de Quinto Elemento Lab, quien también figura dentro de la lista de periodistas cuyos teléfonos fueron blanco del intento de intervención con Pegasus. Lo primero que hizo la reportera al recibir esa información fue, obviamente, confirmarlaю

"Revisé Milenio y no había nada. Como no entendí de qué se trataba ese mensaje, no lo abrí, nada más lo vi en la pantalla cuando llegó", explicó. Al tiempo, ocurrió un nuevo episodio que le permitió a Xanic comprender un elemento clave en la forma en que Pegasus funciona.

El tercer mensaje de texto extraño que recuerda haber recibido decía: "Murió mi mamá, quisiera que me acompañes en el velorio, quiero que estés conmigo".

"Como ya estoy en edad que nuestros papás están mayores, lo abrí y le hice click", explicó.

"Lo que me asombró fue la confección de estos mensajes casi de sastrería fina, bien pensados. ¿Qué nivel de conocimiento sobre una tienen para poder mandar estos mensajes personalizados, más allá de los falsos mensajes corporativos?", se preguntó la periodista mexicana.

Ciber inseguros

Tras recibir los mensajes carnada y tras haberle dado click a alguno de ellos, el teléfono de Xanic comenzó a tener un comportamiento errático, se sobrecalentaba, se acababa muy rápido su batería.

"Perdía el control del aparato, se reiniciaba solo", recordó. A Rodríguez Reyna comenzó a pasarle lo mismo, y juntos acudieron a consultar con Social Tic, una organización dedicada a la seguridad y a los derechos digitales.

Ellos fueron los primeros en comentarles de la existencia del malware Pegasus, y les mencionaron que posiblemente habían sido víctimas del mismo. Esto sucedió antes de la publicación que el New York Times, el 18 de junio de 2017, que reveló por primera vez el uso en México de este malware contra reporteros de alto nivel.

"Lo que nos recomendaron en ese momento fue destruir el aparato, yo no guardé nada ni capturas de pantalla. Nacho (Rodríguez) sí preservó su teléfono y ahora lo prestó a Forbbiden Stories para el análisis forense", explicó.

Para la periodista, la vulneración tiene "repercusiones y alcances enormes", pero lo impresionante fue la evidencia de que entre los espiados hay víctimas del propio Estado, como los padres de los 43 estudiantes de magisterio desaparecidos de Ayotzinapa.

"Es incomprensible", señaló.

"Esto plantea un problema mucho más amplio. Ahorita fueron 50.000 números listados pero el gran tema de fondo son las libertades y los derechos digitales de las personas. Los teléfonos pueden ser un dispositivo vulnerable y de fondo, está la discusión sobre la vigilancia masiva, cómo y quién controla, pone límites y vigila", apuntó.

Para Xanic, aún falta conocer mucho más al respecto de esta noticia que tuvo efecto de una bomba a nivel mundial, sobre todo, qué implicaciones y consecuencias han tenido estas intervenciones clandestinas de los teléfonos de tanta gente.

"Es importante saber qué consecuencias tuvieron estos actos específicos de intromisión, a quién sirvieron, para quién era esa información y quién la uso. Sobre todo, qué consecuencias tuvo su uso", concluyó.