Represión y venta de datos: el espía en tu móvil

Por: Genoveva López, Álvaro Lorite. 12/08/2021

Las grandes empresas y los Estados han desarrollado diversas técnicas de espionaje a través de los teléfonos móviles. Los datos obtenidos son utilizados para fines comerciales o represivos.

Vigilancia y espionaje son las dos caras de una moneda. La moneda es el software imbricado en las vértebras de tu dispositivo digital. La cara es la vigilancia masiva y acumulación de datos para elaborar perfiles comerciales y segmentar publicidad, por ejemplo, para recomendarte la música que no sabías que querías escuchar. La cruz es el acceso total a todos los resquicios de tu vida para tenerte bajo el punto de mira, desacreditarte públicamente, encarcelarte o matarte si hace falta.

“Nos hemos acostumbrado acá en México, pero nos han intervenido a 15.000 personas en todo el mundo, es una barbaridad, es monstruoso”, dice el periodista mexicano Ignacio Rodríguez Reyna, una de esas personas espiadas. El informe publicado por *Forbidden Stories* en colaboración con Amnistía Internacional y otros medios revela que gobiernos de todo el mundo contrataron el software Pegasus a la empresa israelí NSO Group para espiar a activistas, periodistas, disidentes políticos o defensores de derechos humanos en países como México, Marruecos o Arabia Saudí. Con todo, la empresa israelí dice que se dedica a hacer del mundo “un lugar mejor”.

Vulnerabilidades en tu móvil

Cada vez a más gente le resulta familiar la siguiente conversación: “Ayer hablamos de estas zapatillas y hoy me han salido en Instagram. Estoy segura de que el móvil me espía”. Pero, de todo lo que decimos, ¿qué espían exactamente las plataformas? Juan Tapiador es investigador y profesor de seguridad informática en la Universidad Carlos III de Madrid y hace unos años publicó junto con otros colegas un estudio titulado *An Analysis of Pre-installed Android Software* (Un análisis del software preinstalado de Android), en 2019. Buscaban confirmar mediante métodos científicos esa “evidencia anecdótica” que tenía cada vez más gente respecto a sus

teléfonos móviles. El grupo de investigación desarrolló una aplicación que distribuyó a través de contactos y redes sociales. La aplicación, *Firmware Scanner*, le hacía una foto a todo aquello que viniese preinstalado en los teléfonos Android. Su sospecha era que muchas aplicaciones preinstaladas en dichos teléfonos extraían datos de los usuarios y usuarias. A través de contactos y redes sociales, consiguieron que muchísima gente se descargase *Firmware Scanner* y recogieron cientos de miles de fotografías de las tripas de los teléfonos. “Nos encontramos una confirmación a una escala inusitada, de cosas que eran más o menos conocidas, pero no hasta ese nivel”, afirma Tapiador. La vigilancia era masiva.

Tapiador explica que en la cadena de suministro intervienen muchos agentes: el que fabrica los circuitos, el que los integra, el que mete la cámara o el que introduce el micrófono, por mencionar algunos. “Lo que conocemos como fabricantes, la marca que te vende el dispositivo, en realidad son integradores, y su papel es ensamblar las partes previamente fabricadas por subcontratas”, afirma el informático. La cadena no atañe solo al hardware, sino que continúa hasta los operadores telefónicos, que también manipulan los teléfonos móviles e implementan aplicaciones de software cuya finalidad es conseguir datos de los usuarios. “En todo ese proceso como parte del esquema de monetización, que es pervasivo en internet y que tiene que ver con la recolección de datos, están presentes muchísimos agentes que introducen componentes software”, afirma el investigador. En la cadena de ensamblaje de los teléfonos, no se sabe qué agente introduce qué software. No hay ninguna trazabilidad y ninguna regulación que les obligue a informar sobre ello.

Las motivaciones son diversas, pero principalmente suelen atender a dos principios: conseguir una predominancia del mercado, como es el ejemplo de Facebook, que lo que quiere es estar presente en todos los teléfonos posibles y monetizar los datos de los usuarios, o lo que es lo mismo, obtener telemetría del dispositivo para luego vender esa información. Muchas de estas aplicaciones preinstaladas son las que ofrecen puertas traseras abiertas o vulnerabilidades por las que pueden entrar muy fácilmente softwares como Pegasus.

Realizando una mínima interacción como coger una llamada o hacer un clic en un enlace, la puerta trasera del teléfono se abre sin que nos enteremos. Aunque el software destinado al espionaje es distinto al que usan las empresas para recopilar datos, son estas funcionalidades de base las que permiten que el espionaje sea tan sencillo. Según el análisis forense de Amnistía Internacional, en el caso de los iPhone 11 y 12 el virus se propagaba a través del envío de un simple mensaje sin

necesidad de hacer ningún clic.

“Yo ya me había dado cuenta en 2017 de que mi teléfono estaba intervenido y dejé de usarlo, pero lo guardé. Cuando me contactaron en 2020 desde *Forbidden Stories* les doné mi móvil para que hicieran el trabajo forense para su investigación. Desde aquel entonces trato de ser más cuidadoso, uso correos encriptados y aplicaciones seguras, pero la verdad es que hay tal vulnerabilidad que de una manera u otra van a conseguirlo”, relata Rodríguez Reyna. “No solamente tuvieron acceso a todas mis conversaciones, contactos, correos, anotaciones o a las fotos que tomé, pudieron encender mi cámara o mi micrófono en mis situaciones íntimas y personales. Tienen un acceso al control de mi dispositivo en tiempo real. Esto no solo nos coloca en riesgo a nosotros, coloca en riesgo físico a nuestras fuentes. Coloca en la indefensión y susceptibilidad de ser chantajeados por actos de nuestra vida privada que nos ridiculicen o nos quiten credibilidad o cualquier asomo de dignidad”, añade.

Y qué más me da si yo no soy nadie

“Las empresas no están interesadas en las fotografías de tus gatitos ni en las conversaciones ni en los mensajes, eso no sucede”, informa Tapiador, “pero los metadatos son muy buenos predictores de los comportamientos”. La información que recogen las aplicaciones móviles es muy valiosa para luego cruzarla con la navegación web y construir perfiles que durante muchos años se han venido utilizando para dar servicios de publicidad dirigida. “Esta es la gasolina que ha movido internet durante la última década y algo”, afirma este investigador en seguridad informática.

En julio de 2020, los nombres de NSO Group y Pegasus volvieron a llenar los medios nacionales gracias al estudio del instituto de ciberseguridad de la Universidad de Toronto, el Citizen Lab, que publicó que diversas figuras públicas del independentismo catalán como Roger Torrent —entonces president del Parlament— fueron espiadas por Pegasus. A pesar de que el Gobierno, a través del CNI y de los Ministerios de Interior y Defensa, negó rotundamente estar involucrado, la empresa NSO Groups ha manifestado que los únicos clientes de su producto estrella de espionaje son gobiernos. Un extrabajador afirmó que España llevaba siendo cliente de NSO Groups desde 2015.

“En el caso del espionaje sí les interesan tus fotos de gatitos”, bromea Tapiador

haciendo alusión a la última megafiltración de 15.000 personas espiadas. “El caso de NSO Group y Pegasus es un animal totalmente distinto [a la vigilancia comercial]. Son empresas que trabajan con cuerpos y fuerzas de seguridad del Estado porque los países tienen una necesidad de monitorizar los dispositivos de lo que ellos consideran objetivos”, comenta Tapiador.

Virginia Álvarez es responsable de investigación y política interior en Amnistía Internacional. “La empresa decía que el software solo se utilizaba para ciberterrorismo, para localizar delincuentes, pero Amnistía ha empezado a tener información de que este software se estaba utilizando para cometer violaciones de derechos humanos y la intromisión al derecho a la intimidad es un delito”, nos recuerda la activista y portavoz de Amnistía Internacional España.

Cecilio Pineda es un periodista mexicano que fue asesinado a los pocos días de que Pegasus entrase en su móvil. Según The Guardian, a pesar de que no hay pruebas vinculantes, la hipótesis principal señala que se usó el virus para localizarlo

Rodríguez Reyna es uno de los fundadores de 5º Elemento Lab, una organización que se dedica al periodismo de investigación. Tres de sus miembros fueron infectados por Pegasus. “Cuando nos empezaron a vigilar estábamos trabajando en la ramificación mexicana de la trama de corrupción Odebrecht”, cuenta. Esta es una de las mayores tramas de corrupción de la historia reciente de América Latina y tiene como centro de operaciones a la constructora brasileña Odebrecht, que ha realizado sobornos a figuras importantes de 12 gobiernos del continente. “Nosotros señalamos a Emilio Lozoya, figura cercana a Peña Nieto [expresidente mexicano], consejero de OHL en México, como la puerta de entrada de la constructora brasileña al país a través de sobornos. Además, una compañera nuestra estaba creando el primer mapa de las 2.000 fosas clandestinas de personas asesinadas y desaparecidas por el Estado”, relata. Según datos oficiales, se cifran en 80.000 las desaparecidas en los últimos 15 años en México.

Cecilio Pineda es un periodista mexicano que fue asesinado a los pocos días de que Pegasus entrase en su móvil. Según *The Guardian*, a pesar de que no hay pruebas vinculantes, la hipótesis principal señala que se usó el virus para localizarlo. Otro caso conocido en México fue el de uno de los asesores legales en la lucha por esclarecer el crimen de los 43 estudiantes desaparecidos de Ayotzinapa. Su teléfono fue intervenido, se sacó una frase de contexto y se difundió en redes a través de cuentas falsas haciendo creer que había traicionado al movimiento, lo cual provocó

una fractura real en el mismo.

La industria global de vigilancia y espionaje

“Es toda una industria la que hay detrás de esto. Siento que estamos ante una indefensión casi absoluta y es algo terrible”, reflexiona Reyna. El coste de infectar un teléfono en México, según los datos publicados, sería de alrededor de 64.000 dólares, y el Gobierno se gastó 32 millones en espiar a 500 personas de interés. Un amplio número de especialistas considera que es necesaria más regulación para controlar el acceso a los dispositivos tecnológicos, especialmente los teléfonos. Ya sea en el ámbito de la vigilancia y el acceso a metadatos, ya sea en el caso del espionaje y el acceso a datos.

Tapiador afirma que no hay una regulación que obligue a decir qué proveedor de la cadena de suministro introduce software en los dispositivos móviles. “Un problema de este mundo del *databrokering* es que es muy oscuro, no es nada transparente”, advierte. Para las leyes de protección de datos de usuarios la transparencia es muy importante, saber qué datos se recopilan y con qué fines, y “en los casos de las aplicaciones de software preinstaladas, no existe”, sentencia el investigador.

Virginia Álvarez afirma que existe una falta de control absoluta. “Mientras no haya un marco regulador que no evite el mal uso del software de espionaje, Amnistía seguirá pidiendo su no comercialización”. Dario Castañé, del Partido Pirata de Catalunya, considera que “habría que establecer una prohibición a la compra y venta de software para espionaje, así como revertir y anular toda iniciativa que vaya a minar la confidencialidad de las conversaciones, ya sea mediante filtros de subida, control de mensajes o puertas traseras en los algoritmos de cifrado”.

“Es el momento de detenernos y preguntarnos qué está pasando. Estamos ante un monstruo tecnológico que tiene muchos brazos, una dictadura o dictablanda capaz de mover el poder en cualquier lugar del planeta”, reflexiona un periodista mexicano espiado

Sin embargo, cuando hablamos de espionaje, se cruzan los intereses geopolíticos de los Estados en la propia regulación. Desde NSO han manifestado que la publicación “es tendenciosa y tiene una clara motivación comercial y que, en cualquier caso, no ha sido la empresa la que ha hecho uso del software”. No deja de

ser interesante, tal y como señala un artículo del *Financial Times*, que los países clientes de NSO como Emiratos Árabes o Arabia Saudí son aliados recientes con los que han crecido las relaciones con Israel. Países como Hungría, India o Ruanda aparecen también en el informe, en momentos en los que el ex primer ministro, Benjamin Netanyahu, buscaba alianzas con líderes ultraderechistas en estos países.

En su informe *Operando desde las sombras,* publicado a principios de julio, Amnistía Internacional sostiene que existe toda una industria de empresas dedicadas al espionaje. Otras de las empresas que fueron contratadas por el Gobierno de México son Hacking Team (Italia) o Rayzone Group (Israel). También podemos encontrar a empresas vinculadas a grandes controversias como Clearview AI, envuelta en un escándalo por almacenar millones de fotos de redes sociales. O Palantir, la máquina de espiar de Silicon Valley relacionada con varias operaciones al margen de la legalidad. Todas ellas son compañías multimillonarias. Según el informe de Amnistía, el campo de juego de los productos de espionaje ha venido delimitado por las decisiones de diferentes Estados que han permitido autorizaciones legales que se saltan los derechos humanos básicos para poder aplicarlas tanto fuera como dentro de sus territorios.

No obstante, hay que tener en cuenta que la tecnología que lo permite está en manos de dichas compañías. “Es el momento de detenernos y preguntarnos qué está pasando. Estamos ante un monstruo tecnológico que tiene muchos brazos, una dictadura o dictablanda capaz de mover el poder en cualquier lugar del planeta”, reflexiona Rodríguez Reyna.

LEER EL ARTICULO ORIGINAL PULSANDO AQUÍ

Fotografía: El salto diario

Fecha de creación
2021/08/12