# Los vínculos de NSO o cómo los mercados financieros desataron a Pegasus

Por: Roger Suso
Globalizacion, 28 de julio 2021
El Salto 25 julio, 2021

Región: Mundo
Tema: Espionaje

*Cómo nació y se financió NSO, la compañía israelí responsable de Pegasus, un programa que abre la puerta a la filtración de todo tipo de datos personales y materiales de los usuarios de un teléfono móvil. Francisco Partners es una empresa de capital de inversión centrada exclusivamente en inversiones en tecnología y negocios tecnológicos.*

Desde su fundación en 1999 en San Francisco, la compañía ha recaudado alrededor de 24.000 millones de dólares y ha invertido en más de 275 empresas de tecnología, según su sitio web.

De acuerdo con Bloomberg Businessweek, Francisco Partners está relacionada con el destacado fondo de capital de riesgo de Silicon Valley Sequoia Capital y ha trabajado con el fondo de cobertura (hedge funds) Elliott Management Corporation. En 2018, Francisco Partners anunció que el banco de inversión y uno de los más grandes tenedores de viviendas del mundo,  Blackstone, y el banco Goldman Sachs adquirieron una participación minoritaria en la empresa. Lo que Francisco Partners hace, ha pasado siempre desapercibido por el gran público. La empresa tampoco publicita a lo que se dedica y sus materiales de marketing no incluyen ninguna mención a los negocios destapados que realiza con algunos de los gobiernos más represivos del mundo.

En 2006, Francisco Partners invirtió en la empresa de tecnología y seguridad informática de Silicon Valley, Blue Coat Systems. En poco tiempo los ingresos de Blue Coat Systems aumentaron enormemente, a 496 millones de dólares, en 2010, según Bloomberg Businessweek. Hoy la empresa ya no existe. En 2011, como desveló un grupo de investigadores de la Universidad de Toronto agrupados en el instituto Citizen Lab, dispositivos de Blue Coat Systems, usados para bloquear páginas web y registrar las visitas, llegaron a Siria, un país sujeto a estrictos embargos comerciales de Estados Unidos, y estaban siendo utilizados por el gobierno de Bashar al-Assad. La tecnología de Blue Coat Systems se utilizó también en otros países sujetos a sanciones estadounidenses.

En marzo de 2014, Francisco Partners adquirió por 130 millones de dólares una participación mayoritaria en la empresa israelí con sede en Herzliya, NSO Group. Francisco Partners, que a la vez era propietaria de otras empresas de tecnología Deep Packet Inspection y ciberinteligencia como Procera Networks o Sandvine, vendió su participación de NSO Group en febrero de 2019, recibiendo alrededor de un billón de dólares, de acuerdo con Reuters. Omri Lavie i Shalev Hulio, cofundadores de NSO Group, con la participación de la empresa de capital de inversión londinense Novalpina Capital, recompraron su propia compañía.

El nombre de NSO Group empezó sonar a raíz de la segunda detención, el año 2014 en

México, de Joaquín “El Chapo” Guzmán, líder del Cártel de Sinaloa y considerado entonces el hombre más buscado del mundo. Ese año el periódico *Haaretz* publicó que en 2012, el gobierno mexicano firmó un acuerdo de 20 millones de dólares con NSO Group “para luchar contra el narcotráfico” siendo el principal producto de la empresa de software espía (o spyware), Pegasus, clave en la detención de Guzmán.

Pero bajo el mandato de Enrique Peña Nieto, entidades gubernamentales intervinieron miles de teléfonos de políticos: el del ahora presidente Andrés Manuel López Obrador y su círculo cercano hasta el de los familiares de las 43 víctimas del caso Ayotzinapa. El NSO Group también fue mencionado con los casos del hackeo del móvil del bloguero emiratí Ahmed Mansoor y del smartphone de Jeff Bezos, dueño de Amazon y de *The Washington Post* —periódico donde escribía el disidente saudí asesinado Jamal Khashoggi—. El hackeo se habría producido después de una cena en Los Ángeles el 2018 de Bezos con el príncipe heredero de Arabia Saudí Mohamed Bin Salman, viceprimer ministro además, de un país que adquirió el software israelí en noviembre de 2017.

**La criptografía, influenciada por los intereses de la inteligencia de Estados Unidos**

El programa Pegasus, oficialmente dirigido a “combatir el crimen y el terrorismo” y disponible “sólo” para gobiernos, se aprovecha de debilidades de seguridad para hackear dispositivos y teléfonos móviles. Esto incluye el monitoreo y geolocalización de llamadas en tiempo real; la recopilación de correos electrónicos, contactos, nombres de usuario, contraseñas, notas y fotografías, videos y grabaciones de sonido; publicaciones en redes sociales; registros de llamadas e incluso mensajes en aplicaciones de mensajería encriptada; así como activar micrófonos y cámaras y enviar archivos a dispositivos sin la aprobación o conocimiento de los usuarios. Pegasus puede acceder a todo el contenido de conversaciones en Gmail, Facebook, WhatsApp, Telegram, iMessage, Signal o Skype. Todas las aplicaciones. Aún así, uno de los mayores problemas es que no sabemos qué es lo último que Pegasus puede y no puede hacer.

La encriptación E2EE, ampliamente adoptada tras las revelaciones de Edward Snowden en 2013 sobre la red de vigilancia mundial, no es útil contra Pegasus, diseñado para introducirse en dispositivos iPhone y Android, capaz de leer el programa de descodificación. “La complejidad y la mala calidad de la tecnología de comunicaciones actual significa que la criptografía y la privacidad son una estafa, un truco de marketing. ¿A quién le importa el súper algoritmo de cifrado cuando el teléfono móvil está lleno de agujeros?”, espetó en Twitter el periodista Yasha Levine, autor del libro *Surveillance Valley: The Secret Military History of the Internet*.

Además, Levine asegura que Signal fue creado y financiado a través de Radio Free Asia, un subproducto de la CIA cuya historia se remonta a 1951 como una extensión de su red mundial de radio de propaganda anticomunista.

La filtración esta semana de una base de datos telefónicos sobre el uso de Pegasus contra activistas y periodistas en todo el mundo indica que clientes gubernamentales de NSO Group los habrían seleccionado para vigilados y controlarlos. Amnistía Internacional y la organización sin ánimo de lucro de medios de comunicación Forbidden Stories, con sede en París, fueron las primeras en acceder a la lista filtrada, antes de compartirla con los medios asociados al Proyecto Pegasus, un consorcio de información. En la lista se encuentra Ignacio Cembrero, colaborador de *El Confidencial,* y especializado en la cobertura del Magreb.

“Aunque la empresa [NSO Group] afirma que su software espía sólo se utiliza en investigaciones penales y de terrorismo, es evidente que su tecnología facilita la comisión de abusos sistemáticos y que saca provecho de violaciones de derechos humanos generalizadas”, sostiene Agnès Callamard, secretaria general de Amnistía Internacional.

**La huella de Pegasus en Cataluña**

Aunque no aparece en el listado que pasó Amnistía Internacional, hace un año, la compañía israelí ya fue protagonista por el uso de Pegasus para espiar periodistas, activistas y políticos en Catalunya.

Una investigación conjunta de *El País* y *The Guardian* reveló que Pegasus fue la herramienta elegida para penetrar, en 2019, a través de WhatsApp en los teléfonos de varios líderes independentistas catalanes: el entonces presidente del Parlamento catalán, Roger Torrent, el exconseller de Acción Exterior y concejal del ayuntamiento de Barcelona Ernest Maragall —ambos de ERC— y la exdiputada de la CUP exiliada en Suiza Anna Gabriel. Además, según eldiario.es en la lista de espionajes confirmados estaban el entonces conseller de Políticas Digitales y Administración Pública de la Generalitat, Jordi Puigneró (por esas fechas en PDeCAT); el director técnico del Consell per la República (organismo radicado en Waterloo) Sergi Miquel, y el activista de la Asamblea Nacional Catalana y empleado en la Diputación de Tarragona Jordi Domingo.

Aunque a este programa espía sólo tienen acceso los gobiernos o agencias de inteligencia asociadas, el gobierno español aseguró que nunca han contratado los servicios de NSO Group. No obstante, un antiguo empleado de NSO Group sí aseguró a Motherboard que España es cliente desde el año 2015. Por su parte, *Público* señaló que, en el marco de la llamada Operación Cataluña, bajo instrucciones directas del entonces ministro del Interior Jorge Fernández Díaz, el aparato estatal usó un programa similar, de la empresa Rayzone Group —vinculada a NSO Group— para espiar a los políticos soberanistas catalanes.

Además, investigadores de ciberseguridad de Microsoft y el Citizen Lab sostienen, en un informe presentado en julio de este año, que el spyware de otra empresa israelí, Candiru, ha sido utilizado para infectar los ordenadores y teléfonos de políticos, activistas de derechos humanos, periodistas, abogados, académicos y disidentes políticos a través de phishing en dominios falsos disfrazados de Amnistía Internacional o del movimiento Black Lives Matter. Como NSO, Candiru tiene su origen en la Unidad 8200, la unidad militar de inteligencia de las Fuerzas de Defensa de Israel. Entre las personas espiadas con Candiru, empresa de Tel Aviv dedicada a vender programas espía a gobiernos, estaría Carles Puigdemont.

Estas empresas insisten en que su tecnología es fundamental en la batalla contra el crimen y que sus productos salvan vidas. Pero su éxito ha llevado a lo que Ilya Lozovsky, editor del consorcio periodístico OCCRP, llama una “democratización” del acceso a software espía sofisticado. Si antes estaba disponible solo para los pocos servicios de inteligencia de élite, ahora puede ser comprado por todos los gobiernos del mundo.

Muchos de los abusos, infiltraciones, vigilancias y espionajes relacionados con estas tecnologías a personas y grupos que cuestionan el orden social establecido no hubieran sido posibles sin el apoyo de empresas de capital de inversión y recursos como Francisco Partners, fuertemente influenciada por los intereses geopolíticos de la inteligencia de Estados Unidos. Paradigmático es el caso de David Zolet. Según Forensic News, Zolet trabajó con los principales funcionarios de la administración de Donald Trump en una red

nacional encriptada mientras era uno de los dos directores de la empresa Westbridge Technologies, la sucursal estadounidense de NSO Group. Estados Unidos e Israel, de la alianza a la simbiosis.

**Roger Suso**