El nuevo campo de batalla: cibermercenarios que espían para cualquier gobierno

Tiempo de lectura: 10 min.

Mark Mazzetti, Adam Goldman, Ronen Bergman y Nicole Perlroth

Lun, 25/03/2019 - 07:39

El hombre encargado de la implacable campaña saudita para reprimir disidentes buscaba métodos para espiar a la gente que consideraba como una amenaza para el reino. Y sabía a quién acudir: una empresa israelí que ofrece tecnología desarrollada por exfuncionarios de las agencias de inteligencia.

Era finales de 2017 y Saudi Al Qahtani —en ese entonces asesor cercano del príncipe heredero de Arabia Saudita— estaba persiguiendo a disidentes sauditas de todo el mundo como parte de unos grandes operativos de vigilancia, con los que después fue asesinado el periodista Jamal Khashoggi. En mensajes que intercambió con empleados de la compañía NSO Group, Al Qahtani habló de sus grandes planes para usar las herramientas de vigilancia en todo Medio Oriente y Europa, en países como Turquía, Catar, Francia e Inglaterra.

La dependencia del gobierno saudita en una firma con sede en Israel, su adversario político desde hace décadas, es muestra de una nueva manera de librar conflictos: de manera digital, con pocas reglas y en un mercado de ciberespías por comisión valuado en 12.000 millones de dólares.

Hoy en día hasta los países más pequeños pueden comprar servicios de espionaje digital, lo que les permite realizar operaciones sofisticadas de escuchas vía electrónica o influenciar campañas políticas, algo que en el pasado solo podían hacer los aparatos estatales de Estados Unidos y Rusia. Las corporaciones que quieren escudriñar los secretos de sus competidores o un individuo pudiente que tenga alguna rivalidad también pueden realizar estas operaciones de inteligencia si pagan el precio, como si pudieran tomar de un anaquel digital herramientas de la Mossad o la Agencia de Seguridad Nacional (NSA).

NSO Group y uno de sus competidores, la empresa emiratí DarkMatter, son ejemplo de la proliferación del espionaje privatizado. Una investigación que duró meses por parte de The New York Times, a partir de entrevistas con hackers que trabajan o trabajaron para gobiernos y compañías privadas, así como análisis de documentos, reveló las batallas secretas de este combate digital.

Las compañías han permitido que los gobiernos no solo realicen ciberataques contra grupos terroristas o del narcotráfico sino que, en varios casos, los han habilitado para que ataquen a activistas y periodistas. Hackers capacitados por agencias de espionaje estadounidenses que ahora trabajan en esas empresas han capturado en su red a empresarios y defensores de derechos humanos. Los cibermercenarios que trabajan para DarkMatter han convertido un monitor para bebés en un aparato de espionaje.

Además de DarkMatter y de NSO, está Black Cube, empresa privada de ex agentes de inteligencia israelíes y de la Mossad que fue contratada por Harvey Weinstein

para buscar información comprometedora de las mujeres que lo acusaron de acoso y abuso sexual. También existe Psy-Group, empresa israelí especializada en manipulación por medio de redes sociales que ha trabajado con empresarios rusos y que ofreció sus servicios de bots a la campaña de Donald Trump en 2016.

Algunos creen que se acerca un futuro caótico y peligroso debido a la veloz expansión de este campo de batalla de alta tecnología.

“Hasta el país más pequeño con un presupuesto ajustado puede tener capacidad ofensiva” y realizar ataques en línea contra sus adversarios, dijo Robert Johnston, fundador de la compañía de ciberseguridad Adlumin.

Aprovechar vacíos en la seguridad

Antes de que NSO ayudara al gobierno saudita a vigilar a sus adversarios fuera del reino, antes de que ayudara al gobierno mexicano en su intento por cazar a narcotraficantes y antes de que recaudara millones de dólares en trabajos para decenas de países en seis continentes, la empresa estaba formada por dos amigos ubicados en el norte israelí.

Shalev Hulio y Omri Lavie empezaron la compañía en 2008 con tecnología desarrollada por graduados de la Unidad 8200 de los Cuerpos de Inteligencia de Israel —el equivalente de la NSA para esa nación—. Esa tecnología permitía a las empresas de telefonía celular conseguir acceso de manera remota a los aparatos de sus clientes para fines de mantenimiento.

Los servicios de espionaje de Occidente se enteraron de las capacidades del programa y vieron una oportunidad. En ese entonces los funcionarios estadounidenses y europeos advertían que Apple, Facebook, Google y otros gigantes tecnológicos estaban desarrollando tecnologías con las que criminales y terroristas podrían comunicarse en canales encriptados que las agencias estatales no iban a poder descifrar.

Hulio y Lavie les ofrecían una manera de sortear ese problema al hackear el punto final de esas comunicaciones cifradas, el aparato en sí, aún después de que los datos fueran encriptados.

Para 2011, NSO tenía su primer prototipo, una herramienta de vigilancia celular que la empresa llamó Pegasus. El programa podía hacer algo que parecía imposible:

recopilar enormes cantidades de datos antes inaccesibles desde los teléfonos celulares de manera remota y sin dejar rastro. Llamadas, mensajes de texto, correos, contactos, ubicaciones y cualquier información transmitida por aplicaciones como Facebook, WhatsApp y Skype.

“En cuanto estas compañías interfieren tu teléfono se adueñan de él, tú solo lo estás portando”, explicó Avi Rosen de Kaymera Technologies, empresa de ciberdefensa israelí.

NSO Group pronto consiguió su primer gran cliente de Pegasus: el gobierno de México, en medio de su guerra contra el narcotráfico. Para 2013, NSO había instalado Pegasus en tres agencias mexicanas, de acuerdo con correos obtenidos por el Times. En los correos se estima que la empresa israelí le vendió a México 15 millones de dólares en hardware y software, mientras que México le estaba pagando a la compañía 77 millones para rastrear todos los movimientos y clics de los blancos.

Los productos de NSO fueron importantes en la guerra contra el narcotráfico en México, según cuatro personas que conocen de cerca cómo el gobierno de ese país utilizó Pegasus (todas pidieron mantener su anonimato). Los funcionarios mexicanos han indicado que Pegasus fue clave en ayudar a rastrear y capturar a Joaquín “el Chapo” Guzmán Loera, el narcotraficante que fue condenado en febrero pasado a prisión de por vida tras un juicio en Nueva York.

Poco tiempo después NSO estaba vendiendo sus productos a gobiernos en todos los continentes excepto Antártida. Las herramientas, especialmente Pegasus, ayudaron a desmantelar celdas terroristas y asistieron en investigaciones sobre secuestro de niños y crimen organizado, según entrevistas a oficiales europeos de inteligencia y miembros de los cuerpos policiales.

El espionaje a ciudadanos

Pero el primer cliente de NSO Group, el gobierno mexicano, también usó las herramientas de hackeo para fines más macabros. El gobierno usó los productos de NSO para monitorear a, por lo menos, una veintena de periodistas, a críticos del gobierno, expertos internacionales que investigaban la desaparición de 43 estudiantes y hasta promotores de un impuesto a las bebidas azucaradas, de acuerdo con reportajes del Times.

Los afectados fueron blanco de una serie de mensajes de texto amenazantes que contenían el programa malicioso. Algunos decían que la pareja del destinatario estaba teniendo un amorío; otros que un familiar acababa de fallecer. En un caso, los funcionarios no pudieron infiltrarse en el teléfono de una periodista así que le mandaron el vínculo malicioso a su hijo de 16 años.

NSO afirma que solo comercializa sus productos para investigaciones criminales y de antiterrorismo, pero ninguno de los mexicanos que fueron blancos son sospechosos en alguna investigación penal o de terrorismo.

“La tecnología de NSO ha ayudado a detener delitos y ataques terroristas mortíferos en todo el mundo”, indicó la empresa en un comunicado. “No toleramos el mal uso de nuestros productos y con regularidad revisamos e inspeccionamos los contratos para asegurarnos de que no estén siendo usados para nada más que la prevención o investigación de terrorismo y delitos”.

La compañía ya estableció un comité de ética que determina si puede vender sus programas a los países según sus historiales de respeto a los derechos humanos, a partir de medidores como el Índice de Capital Humano del Banco Mundial. NSO no vendió sus productos a Turquía, por ejemplo, debido a sus antecedentes de derechos humanos, según dijeron empleados actuales y previos de la compañía.

Sin embargo, Turquía está mejor posicionado en ese índice del Banco Mundial que México o Arabia Saudita. Ambos son clientes de NSO. Un portavoz del Ministerio de Defensa de Israel, que debe autorizar los contratos de NSO con cualquier gobierno extranjero, rechazó hacer comentarios.

Una demanda legal del año pasado sostiene que Jamal Khashoggi, el columnista del Washington Post que fue estrangulado y desmembrado en el consulado saudita en Estambul, fue espiado meses antes de su muerte por Arabia Saudita con productos de NSO.

Hasta en casos de abusos evidentes NSO siguió renovando los contratos con ciertos gobiernos. En 2013, por ejemplo, NSO firmó su primer acuerdo con los Emiratos Árabes Unidos (EAU) y menos de un año después se descubrió que el gobierno emiratí había instalado software malicioso en el teléfono celular del destacado activista de derechos humanos Ahmed Mansoor.

Mansoor recibió una oleada de mensajes de texto sospechosos, por lo que llevó su dispositivo con investigadores de seguridad que notaron que los vínculos incluidos en los mensajes eran cebos digitales, que aprovechaban vacíos de seguridad en el software de Apple para apoderarse del teléfono. Los investigadores dijeron que era el programa espía más sofisticado que habían visto en un dispositivo móvil.

Apple lanzó un parche de emergencia para su software. Pero, para ese entonces, Mansoor ya había sido despedido de su trabajo, le habían confiscado su pasaporte y robado su auto, habían hackeado su correo electrónico, retirado 140.000 dólares de su cuenta bancaria, monitoreaban su ubicación y en una semana lo habían golpeado dos veces.

Mansoor actualmente está en una celda de aislamiento por una condena de diez años de prisión, acusado de afectar la unidad nacional emiratí.

Leyes que no contemplan la alta tecnología

La proliferación de empresas que intentan replicar el éxito de NSO y competir en lo que la agencia Moody’s estima es un mercado de 12.000 millones de dólares de programas espía de intercepción legal ha desatado una competencia feroz por veteranos de las agencias de inteligencia más sofisticadas de Estados Unidos, Israel y Rusia. Las empresas incluso se roban a los reclutas entre sí.

DarkMatter, la compañía emiratí, se originó a partir de otra empresa, la estadounidense CyberPoint, que hace años consiguió contratos de los Emiratos Árabes Unidos para reforzar su seguridad contra cibertaques. Muchos de los empleados de CyberPoint habían trabajado en proyectos clasificados de la NSA y de otras agencias de inteligencia estadounidenses.

Pero los emiratíes tenían ambiciones más grandes que las previstas en el contrato y presionaban a los trabajadores de CyberPoint a exceder los límites de la licencia, como descifrar códigos de encriptado y hackear sitios web basados en servidores de Estados Unidos. CyberPoint se rehusó pues eso que habría violado las leyes estadounidenses.

Así que, en 2015, los emiratíes fundaron DarkMatter, empresa que no debía atenerse a las leyes estadounidenses, y atrajeron a media docena de los empleados de Estados Unidos de CyberPoint. Marc Baier, exoficial de una unidad de la NSA que realiza ciberoperaciones ofensivas avanzadas, se volvió uno de los principales

ejecutivos de DarkMatter, que también contrató a varios otros oficiales de la NSA y de la CIA, de acuerdo con un registro de nómina obtenido por el Times.

DarkMatter es básicamente un brazo paraestatal; ha trabajado directamente con agentes de inteligencia emiratíes en misiones de hackeo a ministerios gubernamentales de Turquía, Catar e Irán y de espionaje a disidentes dentro de los EAU. Además, DarkMatter irrumpió en cuentas de Google, Yahoo y Hotmail, de acuerdo con los exempleados entrevistados.

Ni la empresa ni un portavoz del gobierno emiratí contestaron a solicitudes para hacer comentarios. Un abogado de Baier también rechazó hacer comentarios.

El FBI está investigando si empleados estadounidenses previos y actuales de DarkMatter cometieron delitos cibernéticos, según cuatro personas que conocen de cerca la investigación. La pesquisa del FBI se intensificó después de que una exempleada de la NSA que trabajaba para esa firma emiratí alertó a las autoridades estadounidenses.

El caso del Departamento de Justicia está enfocado en temas de fraude cibernético y la posible transferencia ilegal de tecnología de espionaje estadounidense a un país extranjero. Pero los procuradores enfrentan obstáculos serios, desde las posibles consecuencias diplomáticas en la relación de Washington con los EAU hasta las preocupaciones respecto a qué podría revelar el caso de la cooperación entre DarkMatter y las agencias de inteligencia estadounidenses.

Además, las leyes de Estados Unidos son poco claras, están obsoletas o no están bien formuladas para los avances tecnológicos. En su mayoría fueron pensadas para prevenir la venta de armamentos del siglo XX, como misiles o aviones caza. No contemplan las capacidades de ciberataque que pueden afinarse desde una computadora o en las agencias de inteligencia más avanzadas del planeta y después vendidas al mejor postor.

“Lo peor es que estas armas son cada vez más fáciles de conseguir”, dijo Brian Bartholomew, investigador sénior de seguridad en Kaspersky Lab, la empresa de seguridad digital. “Entra mucha gente nueva a esta arena que no sigue las mismas reglas. Es como darle un arma de calibre militar a cualquier persona”.

24 de marzo de 2019

New York Times

Scott Shane colaboró con el reportaje.

https://www.nytimes.com/es/2019/03/24/ciberespionaje-nso-darkmatter/?act...