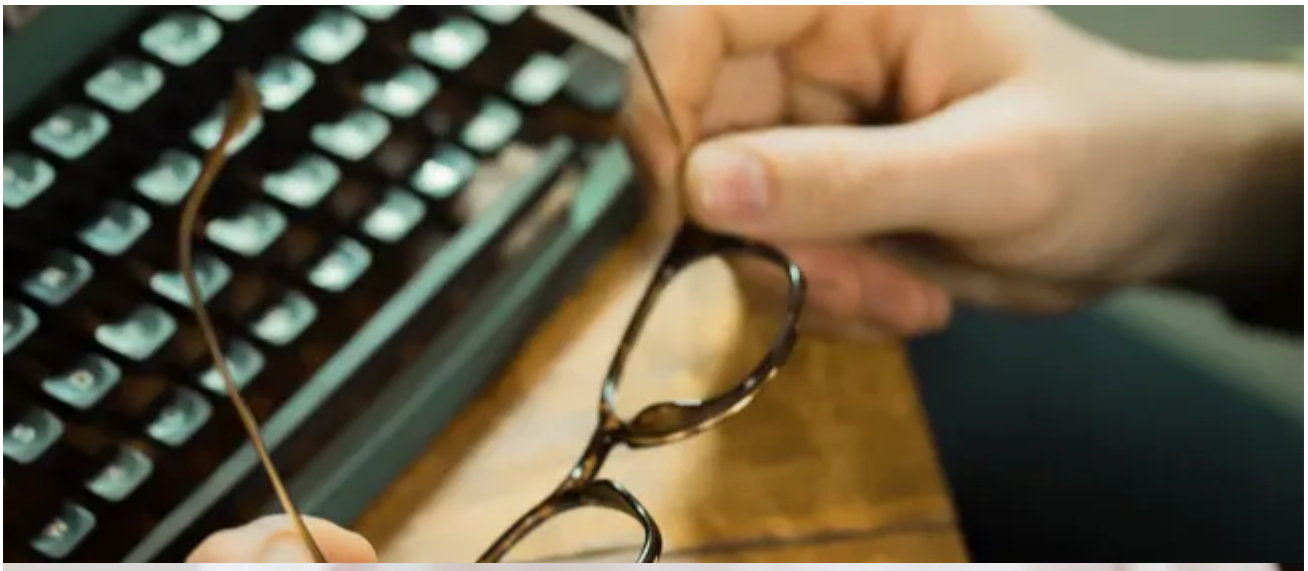
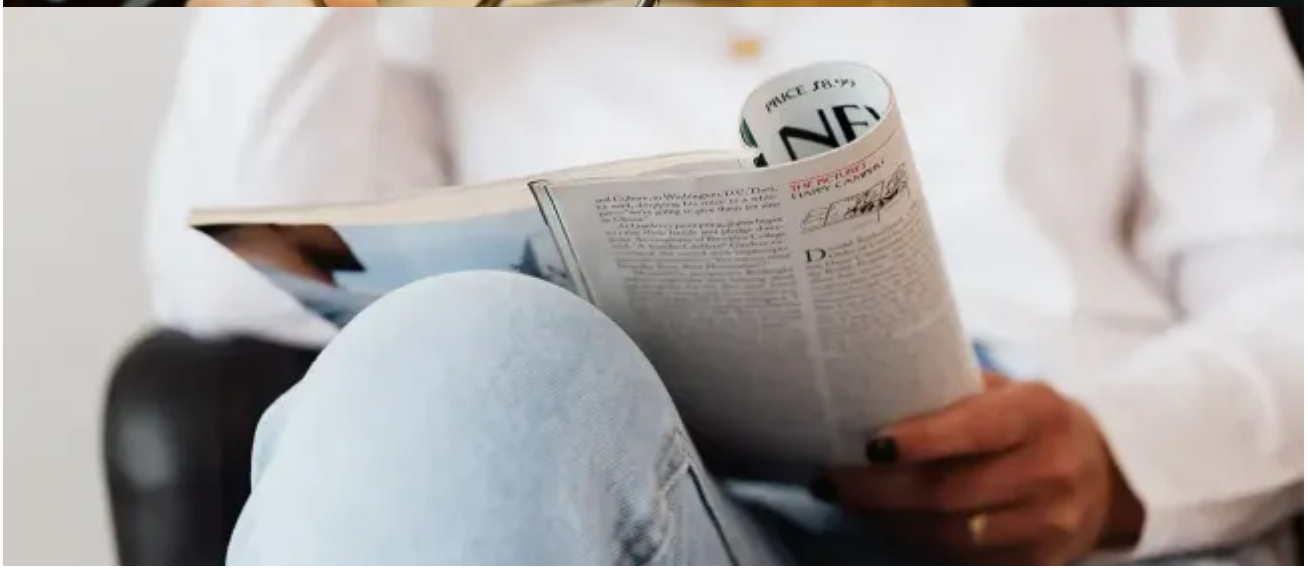
Pegasus: esto aprendimos tras un año de investigar al programa espía más potente del mundo





Tiempo de lectura: 4 min.

Michael Levenson

Dom, 30/01/2022 - 08:43

Se le reconoce ampliamente como el programa espía más potente del mundo, capaz de descifrar confiablemente las comunicaciones encriptadas de los iPhones y los teléfonos inteligentes Android.

Dicho software, Pegasus, fabricado por la empresa israelí NSO Group, ha logrado rastrear a terroristas y cárteles de narcotráfico. También se ha empleado en contra de activistas de derechos humanos, periodistas y disidentes.

Ahora, una investigación publicada el viernes en la revista The New York Times Magazine ha descubierto que Israel, que controla la exportación del programa espía del mismo modo que hace con las exportaciones de armas convencionales, ha hecho de Pegasus un elemento clave de su estrategia de seguridad nacional y lo usa para promover sus intereses en todo el mundo.

La investigación, realizada a lo largo de un año por Ronen Bergman y Mark Mazzetti, también informa que el FBI compró e hizo pruebas de software de NSO durante años con la intención de emplearlo para vigilancia doméstica hasta que el año pasado, al fin, la agencia decidió no utilizar las herramientas.

El Times encontró que las ventas de Pegasus tuvieron un papel clave para lograr el apoyo de los países árabes para la campaña de Israel en contra de Irán al negociar los Acuerdos de Abraham en 2020, que se firmaron en una ceremonia en la Casa Blanca de Donald Trump. Los acuerdos diplomáticos normalizaron las relaciones entre Israel y algunos de sus antiguos adversarios árabes.

EE. UU. buscó el arma cibernética para uso interno

Estados Unidos también había intentado adquirir Pegasus, según descubrió el Times. El FBI, en un trato que no se había dado a conocer hasta ahora, compró el software espía en 2019, a pesar de la existencia de distintos informes de que se había utilizado contra activistas y opositores políticos en otros países. La agencia pasó dos años discutiendo si implementaría un producto más nuevo, llamado Phantom, dentro de Estados Unidos.

Las discusiones en el Departamento de Justicia y el FBI prosiguieron hasta el verano pasado, cuando el FBI por fin decidió que no usaría armas de NSO.

Pero el equipo de Pegasus sigue en un edificio de Nueva Jersey que emplea el FBI y la empresa también le ofreció a la agencia una demostración de Phantom, que podría hackear las líneas telefónicas estadounidenses.

Un catálogo dirigido a clientes potenciales, que el Times obtuvo, dice que Phantom permite que agencias del orden y de espionaje estadounidenses “conviertan el

teléfono inteligente de su objetivo en una mina de oro de inteligencia”.

La investigación del Times estuvo basada en entrevistas con funcionarios del gobierno, líderes de agencias de inteligencia y del orden, expertos en cibernética, ejecutivos de empresas y activistas de la privacidad en más de una decena de países.

Es un relato del auge de NSO, que pasó de ser una empresa emergente que operaba en un gallinero de una cooperativa agrícola a entrar en una lista negra del gobierno de Joe Biden en noviembre debido a que gobiernos extranjeros la emplean para “atacar maliciosamente” a disidentes, periodistas y otros.

NSO empezó con dos amigos de escuela, Shalev Hulio y Omri Lavie que incubaban empresas emergentes en la cooperativa agrícola Bnai Zion, a las afueras de Tel Aviv a mediados de la primera década del siglo.

Una de estas empresas, CommuniTake, que ofrecía a los trabajadores de soporte tecnológico de celulares la capacidad de tomar el control de los dispositivos de los clientes —con permiso— llamó la atención de una agencia de inteligencia europea, dijo Hulio.

Así nació NSO, y la empresa eventualmente desarrolló un modo de adquirir acceso a los teléfonos sin el permiso del usuario y sin necesidad de pulsar algún vínculo o archivo malicioso adjunto. (Fue simple coincidencia que el nombre de la empresa sonara como NSA, la Agencia Nacional de Seguridad estadounidense).

Después de que NSO comenzó a vender Pegasus a nivel mundial en 2011, las autoridades mexicanas lo usaron para capturar a Joaquín Guzmán Loera, el narcotraficante conocido como el Chapo. Y los investigadores europeos lo emplearon para acabar con una red de abuso infantil con decenas de sospechosos en más de 40 países.

Pero también se dieron a conocer abusos en reportes a cargo de investigadores y medios de comunicación, entre ellos el Times.

México empleó el programa espía en contra de periodistas y disidentes. Arabia Saudita lo empleó en contra de activistas de derechos de las mujeres y contactos de Jamal Khashoggi, el columnista del Washington Post que fue asesinado y desmembrado por agentes saudíes en 2018.

Ese año, la CIA compró Pegasus para ayudarle a Yibuti, un aliado estadounidense, en la lucha contra el terrorismo, a pesar de que ya existían antiguas preocupaciones de abusos a los derechos humanos en ese país, incluida la persecución de periodistas y tortura de opositores.

En los Emiratos Árabes Unidos, se usó Pegasus para hackear el teléfono de Ahmed Mansoor, un franco crítico del régimen.

La cuenta de correo electrónico de Mansoor fue violada, su geolocalización fue monitoreada, le robaron 140.000 dólares de su cuenta bancaria, lo despidieron de su trabajo y extraños lo golpearon en la calle.

“Empiezas a pensar que todos tus movimientos son vigilados”, dijo. En 2018 fue sentenciado a diez años de prisión por publicaciones que había hecho en Facebook y Twitter.

A través de una serie de nuevos acuerdos comerciales licenciados por el Ministerio de Defensa israelí, Pegasus ha sido proporcionado a líderes de extrema derecha en Polonia, Hungría, India y otros países.

28 de enero 2022

NY Times

https://www.nytimes.com/es/2022/01/28/espanol/pegasus-israel-nso-espiona...