



## Investigación revela uso global del spyware Pegasus. México es de los principales países que espía a activistas

Pegasus, un software espía utilizado por gobiernos en todo el mundo, ha sido tendencia en las últimas horas debido a una nueva investigación que detalla los objetivos de diferentes organizaciones gubernamentales, específicamente contra activistas de derechos humanos, periodistas y abogados de todo el mundo.

La investigación realizada por [The Guardian](#) y otras 16 organizaciones de medios, especifica que existe un abuso generalizado y continuo del software espía de NSO Group, [Pegasus](#), mismo que la compañía desarrolladora insiste que sólo está destinado a un uso contra delincuentes y terroristas.

Pegasus es un malware que infecta iPhones y dispositivos Android para permitir que los operadores del spyware puedan extraer mensajes, fotos y correos electrónicos, además de poder grabar llamadas y activar los micrófonos en secreto.

La filtración de datos que se detalla en la investigación, contiene una lista con más de 50 mil números de teléfono, que se cree, han sido identificados referentes a personas de interés por clientes de NSO desde al menos 2016.

Forbidden Stories, una organización de medios sin fines de lucro, con sede en París, y Amnistía Internacional, inicialmente tuvieron acceso a la lista filtrada y acceso compartido con socios de medios como parte del Proyecto Pegasus, un consorcio de reportajes.

La presencia de un número de teléfono en los datos no revela si un dispositivo ha sido infectado con Pegasus o fue objeto de un intento de hackeo. Sin embargo, el consorcio cree que los datos son indicativos de los posibles objetivos que los clientes gubernamentales de NSO identificaron antes de posibles intentos de vigilancia.

El análisis forense de una pequeña cantidad de teléfonos cuyos números aparecieron en la lista filtrada también mostró que más de la mitad contenían rastros del software espía Pegasus.

Entre las personas cuyos números telefónicos aparecieron en la lista, se incluyen cientos de



## Investigación revela uso global del spyware Pegasus. México es de los principales países que espía a activistas

ejecutivos empresariales, figuras religiosas, académicos, empleados de ONG, dirigentes sindicales y funcionarios gubernamentales, incluidos ministros, presidentes y primeros ministros del gabinete.

La lista también cuenta con números de familiares cercanos de gobernantes de países, lo que sugiere que el gobernante también puede haber dado instrucciones a sus agencias de inteligencia para que exploren la posibilidad de monitorear a sus propios parientes.

Las divulgaciones comenzaron este domingo, con la revelación de que en los datos figuran las cifras de más de 180 periodistas, incluyendo reporteros, editores y ejecutivos de Financial Times, CNN, The New York Times, France 24, The Economist, Associated Press y Reuters.

En el caso de México, aparece el número telefónico de un reportero mexicano independiente, Cecilio Pineda Birto, aparentemente de interés para un cliente mexicano en las semanas previas a su asesinato en un lavado de autos. Su teléfono nunca fue encontrado, por lo que ningún análisis forense fue posible para establecer si fue infectado con el spyware.

NSO Group dijo que incluso si el teléfono de Pineda fue atacado, no significaba que los datos recopilados de su teléfono contribuyeron de alguna forma con su muerte, y enfatizó que los gobiernos podrían haber descubierto su ubicación por otros medios. Estaba entre al menos 25 periodistas mexicanos aparentemente seleccionados como candidatos para vigilancia por un período de dos años.

*«El análisis del consorcio de datos filtrados identificó al menos 10 gobiernos que se cree que eran clientes de NSO que estaban ingresando números en un sistema: Azerbaiyán, Bahrein, Kazajstán, México, Marruecos, Ruanda, Arabia Saudita, Hungría, India y los Emiratos Árabes Unidos», dice la investigación.*

*«El análisis de los datos sugiere que el país cliente de NSO que seleccionó la mayor cantidad de números, más de 15,000, fue México, donde se sabe que varias agencias gubernamentales diferentes compraron Pegasus. Tatu Marruecos como los*



Investigación revela uso global del spyware Pegasus. México es de los principales países que espía a activistas

*Emiratos Árabes Unidos seleccionaron más de 10,000 números, según el análisis sugerido».*

Sin embargo, sin un examen forense de los dispositivos móviles, es imposible decir si los teléfonos fueron sometidos a un intento de hackeo con Pegasus exitosamente.

NSO siempre ha dicho que *«no opera los sistemas que vende a clientes gubernamentales examinados y no tiene acceso a los datos de los objetivos de sus clientes».*

En declaraciones emitidas por sus abogados, NSO negó las *«afirmaciones falsas»* hechas sobre las actividades de sus clientes, pero dijo que *«seguirán investigando todas las denuncias creíbles de uso indebido y tomaría las medidas apropiadas».* También mencionó que la lista no podría ser una lista de número *«apuntados por los gobiernos para usar Pegasus»*, y describió la cifra de 50,000 como *«exagerada».*

Según la compañía, solo vende su software a agencias militares, policiales y de inteligencia en 40 países sin nombre, y dice que examina rigurosamente los registros de derechos humanos de sus clientes antes de permitirles usar sus herramientas de espionaje.

El ministro de defensa israelí regula de cerca a NSO, otorgando licencias de exportación individuales antes de que su tecnología de vigilancia pueda venderse a un nuevo país.

En junio, NSO publicó un informe de transparencia en el que asegura tener un enfoque de derechos humanos líder en la industria y publicó extractos de contratos con clientes que estipulaban que solo deben usar sus productos para investigaciones penales y de seguridad nacional.

No hay evidencia que sugiera que los clientes de NSO también utilizaron Pegasus en investigaciones de terrorismo y delitos, y el consorcio también encontró cifras en los datos que pertenecen a presuntos delincuentes.



## Investigación revela uso global del spyware Pegasus. México es de los principales países que espía a activistas

Sin embargo, la amplia gama de números en la lista que pertenecen a personas que aparentemente no cuentan con conexión con la delincuencia sugiere que algunos clientes de NSO están incumpliendo sus contratos con la empresa, [espiando a activistas](#) prodemocráticos y periodistas que investigan la corrupción, así como a opositores políticos y a críticos del gobierno.

La investigación, realizada por Amnesty's Security Lab, un socio técnico del Proyecto Pegasus, encontró rastros de actividad de Pegasus en 37 de los 67 teléfonos examinados.

El análisis también descubrió algunas correlaciones secuenciales entre la hora y la fecha en que se ingresó un número en la lista y el inicio de la actividad de Pegasus en el dispositivo, que en algunos casos ocurrió solo unos segundos después.

Amnistía compartió su trabajo forense en cuatro iPhones con Citizen Lab, un grupo de investigación de la Universidad de Toronto que se especializa en el estudio de Pegasus, que confirmó que mostraban signos de infección por Pegasus. Citizen Lab también llevó a cabo una revisión por pares de los métodos forenses de Amnistía y descubrió que eran sólidos.

Ruanda, Marruecos, India y Hungría negaron haber utilizado Pegasus para piratear los teléfonos de las personas mencionadas en la lista.

Los gobiernos de Azerbaiyán, Bahrein, Kazajstán, Arabia Saudita, México, Emiratos Árabes Unidos y Dubai no respondieron a las invitaciones para comentar al respecto.

Claudio Guarnieri, quien dirige el Laboratorio de Seguridad de Amnistía Internacional, dijo que una vez que el teléfono se infecta con Pegasus, un cliente de NSO podría tomar el control del dispositivo, lo que le permite extraer mensajes, llamadas, fotos, correos electrónicos, entre otra información, además de activar cámaras en secreto y micrófonos.

Al acceder al GPS y a los sensores de hardware en el teléfono, los clientes de NSO también pueden obtener un registro de los movimientos pasados de una persona y rastrear su ubicación en tiempo real con una precisión milimétrica, por ejemplo, estableciendo la



Investigación revela uso global del spyware Pegasus. México es de los principales países que espía a activistas

dirección y velocidad en la que viajaba un automóvil.

Los últimos avances en la tecnología de NSO le permiten acceder a teléfonos con ataques de cero clic, lo que significa que un usuario ni siquiera necesita hacer clic en un enlace malicioso para que su teléfono se infecte.

Guarnieri ha identificado evidencia de que NSO ha estado explotando las vulnerabilidades asociadas con iMessage, que viene instalado en todos los iPhones, y ha podido penetrar incluso el iPhone más actualizado con la última versión de iOS. El análisis forense de su equipo descubrió infecciones exitosas e intentadas por Pegasus en teléfonos tan recientes como este mes.

«Los investigadores de seguridad están de acuerdo en que el iPhone es el dispositivo móvil de consumo más seguro y protegido del mercado», dijo Apple.

NSO negó dar detalles específicos sobre sus clientes y las personas a las que se dirigen.

Sin embargo, una fuente familiarizada con el asunto dijo que el número promedio de objetivos anuales por cliente era 112. La fuente dijo que la compañía tenía 45 clientes para su software espía Pegasus.