PERIÓDICO	PAGINA	FECHA	SECCIÓN
REFORMA	7	21/10/2022	LEGISLATIVO

Preocupa a expertos uso de software Pegasus

Alertan por hackeo de grupos del narco

Advierten riesgos de seguridad tras la filtración de grupo Guacamaya

VICTORIA FÉLIX

El contexto histórico de corrupción y narcotráfico del País plantea la pregunta sobre si el Gobierno mexicano puede garantizar a los ciudadanos que el software espía Pegasus no está siendo utilizado por cárteles, alertaron especialistas.

Además del riesgo de espionaje político, John Scott-Railton, investigador senior de Citizen Lab, advirtió en entrevista con Grupo REFORMA que desde el Gobierno podría facilitarse el programa a delincuentes.

"La preocupación con Pegasus es, en el contexto de la corrupción oficial, ¿el Estado (mexicano) es capaz de proporcionar garantías de que las personas que trabajan en nombre de los intereses de los cárteles no tengan acceso a Pegasus", cuestionó.

El especialista señaló que casos como los del periodista sinaloense Javier Valdez, asesinado en 2017, y su viuda, Griselda Triana, han puesto en evidencia que Pegasus podría ser usado a favor del crimen organizado.

Pegasus es un software espía que infecta celulares y fue creado por la empresa israelí NSO Group, que asegura que sólo lo vende a Gobiernos nacionales para actividades legales.

Desde el sexenio priista de Enrique Peña, periodistas, activistas y opositores han denunciado ser espiados por Pegasus, lo que ha sido corroborado por el Citizen Lab, especializado en ciberseguridad y con sede en la Escuela Munk de Asuntos Globales y Políticas Públicas de la Universidad de Toronto.

Aunque el Presidente Andrés Manuel López Obrador ha negado que espíe, la Fiscalía General de la República (FGR) investiga casos en el actual sexenio.

La denuncia más reciente comprobada por el Citizen Lab es la del diputado federal emecista por Nuevo León, Agustín Basave.

Scott-Railton cuestionó además que el Gobierno mexicano haya sido víctima de una filtración por el llamado "Guacamaya Leaks", y señaló que esto puede generar serias amenazas a la seguridad nacional.

Consideró que es contradictorio que, por una parte, los Gobiernos usan herramientas como Pegasus para espiar, pero no pueden defenderse de ciberataques.

"Los Gobiernos han comenzado a reconocer que esta tecnología", dijo Scott-Railton, "incluso si es algo que desean por sus propios motivos, presenta una verdadera amenaza para su propia privacidad y confidencialidad. Hay una desafortunada tendencia de los Gobiernos a buscar herramientas para entrometerse y monitorear, incluso si ellos mismos no son capaces de proteger su información".

John Scott-Railton *Investigador senior de Citizen Lab*

"La preocupación con Pegasus es, en el contexto de la corrupción oficial, ¿el Estado (mexicano) es capaz de proporcionar garantías de que las personas que trabajan en nombre de los intereses de los cárteles no tengan acceso a 'Pegasus'".

Nueva modalidad

John Scott-Railton, investigador senior de Citizen Lab, alertó de una nueva tendencia de hackeo llamada "clic cero".

- El celular es interceptado sin necesidad de abrir una liga.
- No habrá alerta del virus.
- Facilita el espionaje.
- Entre 2017 y 2018, este tipo de filtración requería hacer clic en una liga que le llegaba al usuario.
- Así, el teléfono era intervenido por el software espía.
- Ahora son hackeados sin liga.