EL ECONOMISTA

GOVERNMENT ESPIONAGE

Suspected greater espionage by the Mexican government

The cases of government espionage continue to come to light and confirm the abuse that the authorities do in the use of technology against civil society, at a cost of millions for the country's coffers.

Julio Sánchez Onofre
February 13, 2017, 05:45

First was FinFisher, the Gamma Group spyware detected in Mexico in 2013. Then, the DaVinci and Galileo malware from the Hacking Team discovered in 2014. And more recently there is Pegasus, from the NSO Group, found in 2016 and 2017. The cases of government espionage through malicious software continue to come to light and confirm the abuse that the authorities make in the use of technology against civil society, at a cost of millions for the country's coffers.

technology exclusively used by the government.

NEWS: PGR, Veracruz and PGJDF, the ones that monitor communications the most

We hope that our work helps highlight to journalists and other investigators that many attacks are taking place in Mexico. This may be the tip of the iceberg, said John Scott-Railton, a researcher at the Citizen Lab and one of the report's authors.

On February 11, the research institute published its most recent report called Bitter Sweet where it documented the use of the Pegasus solution by the Israeli firm NSO Group to spy on researcher Simón Barquera of the National Institute of Public Health (INSP); Alejandro Calvillo, general director of the organization Al Poder del Consumidor; and Luis Encarnación, coordinator of the ContraPESO Coalition, who promoted the tax on sugary drinks.

But Scott-Railton warns of a very high possibility that there are more victims of government espionage.

Timeline of NSO Exploit links sent to Mexican Soda-Tax supporters #bittersweetmx pic.twitter.com/RmKX34KTKZ
- citizen lab (@citizenlab) February 12, 2017

We firmly believe that there are other targets, assured the expert contacted by El Economista via email.

NEWS: The protection of personal data in the era of leaks

In previous investigations of espionage through malicious software used exclusively by the government, experts have determined that the motive has been political given that the targets have been human rights defenders and journalists. But the Bitter Sweet campaign hints at a possible corruption of officials or security agencies who intervened private communications to benefit commercial interests.

This case suggests that NSO Group's spy tools, used exclusively by the government, may be used by a government entity on behalf of business interests, and not for reasons of national security or the fight against crime, Citizen researchers consider. Lab.

The acquisition and abusive use of these technologies is also the responsibility of the treasury. Scott-Railton says the impact is in the millions, although given the lack of transparency and controls, it is difficult to know the exact cost.

NEWS: Reforms are lacking to curb espionage of governments in Latin America

the obvious use here even more alarming, he said.

The truth is that the country's authorities are avid buyers of spyware. Journalistic versions have mentioned that the Mexican government paid $ 20 million to acquire the NSO Group solutions in 2012; while the leaks of the Italian firm Hacking Team revealed that the Mexican authorities are the main clients of the company by paying more than 5.8 million euros.

A history of abuse

En diversas investigaciones realizadas por organizaciones como la Red en Defensa de los Derechos Digitales (R3D) así como por *El Economista*, se ha documentado que el gobierno mexicano abusa de la vigilancia, ya sea al solicitar datos y metadatos de las comunicaciones de los ciudadanos sin control, o al utilizar herramientas tecnológicas de hackeo e intervención de dispositivos con fines distintos al combate al crimen o protección de la seguridad nacional.

Y es que la adquisición y uso de malware ha sido una herramienta de las autoridades mexicanas para evadir tanto los controles judiciales como la colaboración de las empresas de telecomunicaciones para realizar campañas de espionaje a los usuarios del país.

NOTICIA: Rastreo de llamadas no culmina en averiguaciones

Estas prácticas permanecen en las sombras y exponen a los ciudadanos a potenciales abusos del gobierno.

En su reporte El estado de la vigilancia: fuera de control , presentado en diciembre pasado, R3D consignó que el excesivo gasto del gobierno de software malicioso, el alto nivel de invasión a la vida privada de los ciudadanos que representa un hackeo de este nivel por parte de las autoridades y la opacidad en la que operan estas herramientas están lejos de cumplir los principios de necesidad y proporcionalidad.

Así funciona el malware "Pegasus" de la empresa NSO Group:

pic.twitter.com/NIZUp39BO7

— R3D (@r3dmx) 12 de febrero de 2017

La utilización de esta técnica de vigilancia no requiere la colaboración de empresas de telecomunicaciones, y que resulta sumamente complicada la detección de dispositivos infectados, existen menos controles y puntos de detección de la utilización abusiva de

medidas , advirtió entonces.

NOTICIA: Usuarios de redes sociales, en la mira del gobierno de México

Scott-Railton, del Citizen Lab, es enfático en que la detección, investigación y divulgación de estas prácticas requiere la colaboración entre la sociedad civil, los expertos y las organizaciones defensoras de los derechos humanos. En la documentación de Bitter Sweet, participaron las organizaciones R3D y SocialTIC así como un investigador de Amnistía Internacional.

Esperamos que otras organizaciones mexicanas se sientan empoderadas para buscar mensajes sospechosos. Si creen que fueron testigos de esta campaña, pueden ponerse en contacto con nosotros directamente en bittersweet@citizenlab.ca. O, si tienen un problema de seguridad digital de manera más general, pueden ponerse en contacto con la línea de ayuda de Access Now: https://www.accessnow.org/help/ , escribió el experto.

julio.sanchez@eleconomista.mx

erp

Filed in:

ESPIONAGE SOCIETY DIGITAL ESPIONAGE

MORE POPULAR

one #AMLOTrackingPoll AMLO Approval, July 8

two Wouldn't it be time to change strategist in the pandemic?
6 hours ago

3 Austere baggage
6 hours ago

4 Amway 30 years here, pandemic pushes digital and marginal advance
6 hours ago

5 Pemex halted drop in crude reserves in 2019
6 hours ago

CONNECT WITH US

Receive our daily newsletter with the most important contents of the print and digital editions of El Economista

RECEIVE OUR NEWSLETTER

On social networks we publish breaking news, exclusive content and promotions. They are a way for you to be in direct contact with our newsroom.

1M 610K

188K 120K

LAST NEWS

32 minutes ago

Gold breaks the $ 1,800 per ounce barrier for the first time since 2011
By AFP

5 hours ago

Bank-store model is not failing: BanCoppel
By Edgar Juárez

6 hours ago

Ficrea Trustee announces seventh payment to defrauded
By Fernando Gutiérrez

6 hours ago

Banxico acknowledges attempted hacking of its site
By Yolanda Morales

6 hours ago

Without support, demand for new cars will recover until 2024
By Marisol Velázquez

KEEP READING

Marisol Velázquez

BEFORE THE MAJORITY OF MORENA, SPECIALISTS INDICATED THAT CONSENSUS IS NECESSARY

#AMLOTrackingPoll AMLO Approval, July 8

Election of INE directors without quotas, they insist

Maritza Pérez

AUTORIDAD COMICIAL HA CARECIDO

AMLO: han estado oportunistas, que avalaron fraudes

Jorge Monroy

POR SEIS MESES, ANUNCIÓ LA JUDICATURA

Suspenden a secretario por caso del Mochomo

Jorge Monroy

RESTOS FUERON ANALIZADOS EN LA UNIVERSIDAD DE INNSBRUCK

Reporta gobierno identificación de normalista de Ayotzinapa

Jorge Monroy

CRÓNICA. EN LAS CALLES DE LA CIUDAD DE MÉXICO

Avanza la "Nueva Normalidad" en la CDMX

Redacción

AMLO arriba a Washington en su primera gira internacional para reunirse con Donald Trump

Marisol Velázquez

CTE da a conocer lista de calificaciones de aspirantes a consejeros del INE