Technology | CyberSecurity

NSO Group: Hackers use Pegasus spyware to target and track supporters of Mexican soda tax

The Mexican government has previously reportedly confirmed being a client of Israel-based NSO Group's cyberweapons.

By India Ashok

February 13, 2017 05:06 GMT

Mexican researchers and public health activists supporting the Mexican soda tax were reportedly targeted by hackers using Israeli-based cyberweapons manufacturer, NSO Group's, spyware dubbed Pegasus. In an elaborate cyberespionage campaign , hackers targeted researchers and activists battling obesity in Mexico, in efforts to track their moves through their phones, according to reports.

The targets included Dr Simón Barquera, the director of nutrition policy at Mexico's National Institute of Public Health, Luis Manuel Encarnación, the-then director of Fundación Mídete, a foundation in Mexico City that combats obesity, Alejandro Calvillo, an activist and founder of El Poder del Consumidor, yet another organisation battling childhood obesity in the country, the New York Times reported.

The targets received messages containing malicious links, which when opened, would install the NSO Group's Pegasus spyware on their phones. The cyberespionage threat actors allegedly tailored the messages with emotional content, aimed at creating panic and eliciting a response.

All three of the targets have been vocal supporters of Mexico's 2014 soda tax, aimed at limiting the consumption of sugary drinks within the country by imposing higher prices on sodas. Despite the tax bill having been passed, primarily due to pressure from numerous Mexican organisations, raising awareness and battling obesity, the food and beverage industry has since resisted attempts to double the tax. In 2015, Mexican lawmakers, bowing to pressure, attempted to slash the tax in half. However, a massive public backlash put a stop to the tax cut.

Bitter Sweet bait

Security researchers at Citizen Lab said: "Spyware operators sometimes develop bait content that is both personalised and capable of stirring strong emotions. The Bitter Sweet NSO spyware operators personalised the messages to the interests and work of the targets and actively escalated the emotional content of the messages over time.

"There are many factors that could explain the heavy-handed targeting, including a lack of professionalism, intense pressure for results, a lack of concern for the consequences of being caught. Whatever the reason, recklessness by the Bitter Sweet operators led to the compromise of their operation."

According to Citizen Lab, circumstantial evidence indicates that the Mexican government, which has previously reportedly confirmed that it is a client of the NSO Group, may have allegedly participated in the cyberespionage campaign.

Researchers also noted that the same cyberespionage infrastructure used on the recent targets has also previously

Mexico is also allegedly one of the biggest clients of Italian surveillance firm Hacking Team. Since 2010, 14 Mexican states have reportedly purchased $6.3m worth of spy tools from Hacking Team.

"This is proof that surveillance in Mexico is out of control," said Luis Fernando García, the director of Mexican digital rights nonprofit - the Red en Defensa de los Derechos Digitales (R3D). "When we have proof that this surveillance is being used against nutritional activists, it's clear Mexico should not be given these technologies."

"This is one of the most brazen cases of abuse we have ever seen," said John Scott-Railton, a senior researcher at Citizen Lab. "It points to a total breakdown of government oversight in Mexico, and a complete failure of due diligence by the NSO Group."

The NSO Group reiterated that its products are sold to governments to help them track terrorists and criminals, adding that the firm had no knowledge of the use of its products to track activists and researchers in Mexico.

"Mexico's intelligence systems are subject to federal relevant legislation and have legal authorisation," Ricardo Alday, a spokesman for the Mexican Embassy in Washington, said in a statement. "They are not used against journalists or activists. All contracts with the federal government are done in accordance with the law."