RECKLESS REDUX

Senior Mexican Legislators and Politicians Targeted with NSO Spyware

By John Scott-Railton, Bill Marczak, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert

JUNE 29, 2017
RESEARCH REPORT #94

munk school
OF GLOBAL AFFAIRS & PUBLIC POLICY

UNIVERSITY OF TORONTO

THECITIZENLAB

Copyright

Document Version: 1.0

Suggested Citation

John Scott-Railton, Bill Marczak, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert. "Reckless Redux: Senior Mexican Legislators and Politicians Targeted with NSO Spyware," Citizen Lab Research Report No. 94, University of Toronto, June 2017.

Acknowledgements

We thank the targets of these infection attempts who have come forward to provide us with the messages, and given permission to publicly describe their cases.

Citizen Lab would like to thank our collaborating organizations, including R3D, SocialTic and Article19, for their careful and important investigative work as Citizen Lab continues to investigate the use of NSO technology in Mexico. Without their assistance, the investigative project would not be possible.

We also thank Azam Ahmed of the New York Times, as well as additional researchers, including TNG.

Special thanks to Citizen Lab's team.

We also thank Amnesty International and Access Now for assistance in earlier phases of the investigation.

About the Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto

The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs and Public Policy, University of Toronto, focusing on research, development, and high-level strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security.

We use a "mixed methods" approach to research that combines methods from political science, law, computer science, and area studies. Our research includes investigating digital espionage against civil society, documenting Internet filtering and other technologies and practices that impact freedom of expression online, analyzing privacy, security, and information controls of popular applications, and examining transparency and accountability mechanisms relevant to the relationship between corporations and state agencies regarding personal data and other surveillance activities.

This report is Part 3 of a series on the abuse of NSO Group's spyware in Mexico

Part 1: Bittersweet: Supporters of Mexico's Soda Tax Targeted With NSO Exploit Links

Part 2: Reckless Exploit: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware

Part 3: Reckless Redux: Senior Mexican Legislators and Politicians Targeted with NSO Spyware

Part 4: Reckless III: Investigation Into Mexican Mass Disappearance Targeted with NSO Spyware

Part 5: Reckless IV: Lawyers For Murdered Mexican Women's Families Targeted with NSO Spyware

Part 6: Reckless V: Director of Mexican Anti-Corruption Group Targeted with NSO Group's Spyware

Part 7: Reckless VI: Mexican Journalists Investigating Cartels Targeted with NSO Spyware Following Assassination of Colleague

Part 8: Reckless VII: Wife of Journalist Slain in Cartel-Linked Killing Targeted with NSO Group's Spyware

Key Findings

Three senior Mexican politicians were targeted with infection attempts using spyware developed by the NSO group, an Israeli "cyber warfare" company.

The targets:

- **Ricardo Anaya Cortés**, President of Mexico's National Action Party (PAN)
- **Senator Roberto Gil Zuarth**, President of Mexico's Senate (during the targeting)
- **Fernando Rodríguez Doval**, Communications Secretary for PAN

All three targets are members of the socially conservative National Action Party (PAN). Between June and July 2016 they were sent text messages containing links to NSO's exploit framework.

The findings build on our prior collaborative investigations published on June 19 2017, and February 11 2017 uncovering targeting of Mexican journalists, lawyers, scientists, and public health campaigners using NSO's exploit framework.

Introduction

On Monday June 19, 2017 Citizen Lab published results of an investigation that revealed that 12 individuals in Mexico and the United States were sent at least 76 text messages in an attempt to infect them with government-exclusive spyware called Pegasus. The targets included prominent journalists, lawyers, and a minor child. The investigation was undertaken collaboratively with Mexican non-governmental organizations R3D, SocialTic and Article 19, which also published a report in Spanish.

Pegasus is made by NSO Group, an Israeli company that some have reported is re-branding as Q Cyber Technologies. The majority owner of NSO Group is the United States-based firm Francisco Partners, which is reportedly considering selling the company with a valuation of $1 billion.

Prior to our June 2017 report, in February 2017, Citizen Lab along with our collaborators, published a report demonstrating that Mexican food scientists and anti-obesity campaigners who supported Mexico's Soda Tax were targeted with Pegasus.

Since the initial announcement, a number of individuals have contacted Citizen Lab and our collaborators with suspicious text messages. After analyzing the messages shared with us, we have been able to confirm that some of these messages contain links pointing to NSO Group's exploit infrastructure. This report adds to our prior analysis a new category of targets in addition to lawyers, journalists, health scientists, and human rights advocates (and their families): **Mexican politicians**.

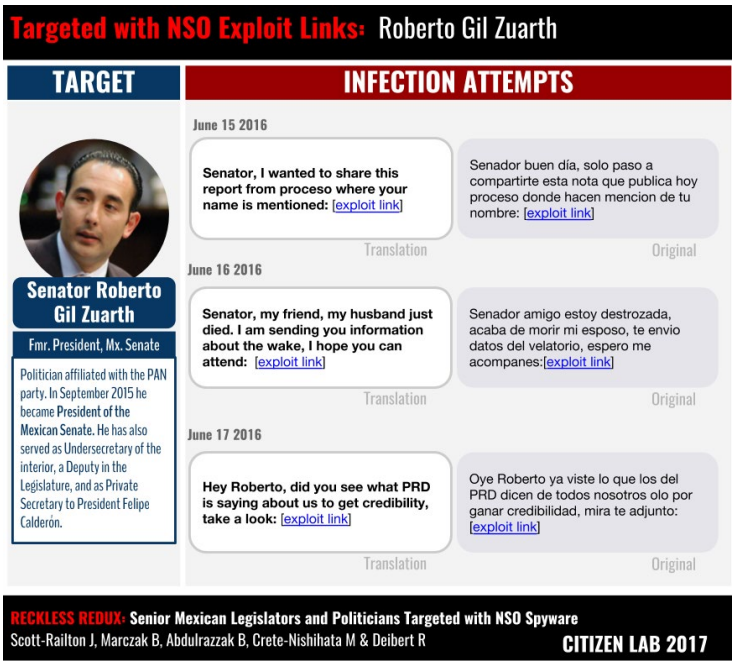
Newly Discovered Targets

This research note outlines three new targets: Senator Roberto Gil Zuarth, President of Mexico's Senate during the targeting period and member of Mexico's National Action Party (PAN), Ricardo Anaya Cortés, President of PAN, and Fernando Rodríguez Doval, Communications Secretary for PAN. PAN, a major opposition party, is traditionally viewed as socially conservative, and has provided Mexico with two of its most recent presidents: Vicente Fox and Felipe Calderón.

Figure 1: Widespread targeting in Mexico using NSO's Pegasus.

Target: Senator Roberto Gil Zuarth

Senator Roberto Gil Zuarth is currently the President of Mexico's Senate and a member of PAN. Between June 15 and 17 2016 he was sent three infection attempts in the form of text messages with links to NSO exploit infrastructure.



The messages echoed themes uncovered in prior Citizen Lab reports of targeting in Mexico, such as the death of a father, and a news story in the Mexican news magazine *Proceso* mentioning the target. A third message suggests that another political party (Party of the Democratic Revolution: PRD) has been critical of him and his colleagues.

Figure 2: Senator Roberto Gil Zuarth was targeted with at least three infection attempts during June 2016, while he was President of Mexico's Senate (Photo: Wikipedia)

The messages pointed to links on the domain **smsmensaje[.]mx**. Citizen Lab has previously identified this domain as a part of the NSO exploit infrastructure. Clicking on the link would have infected Roberto Gil Zuarth's iPhone with Pegasus spyware.

The **Appendix** provides further detail on the messages.

Target: Ricardo Anaya Cortés

Ricardo Anaya Cortés is a lawyer, politician, and current president of PAN. On June 15, 2016 he was sent a text message claiming that he was mentioned in an article in *Proceso*. Notably, his colleague at PAN, Senator Roberto Gil Zuarth received a nearly identical message on the same day.

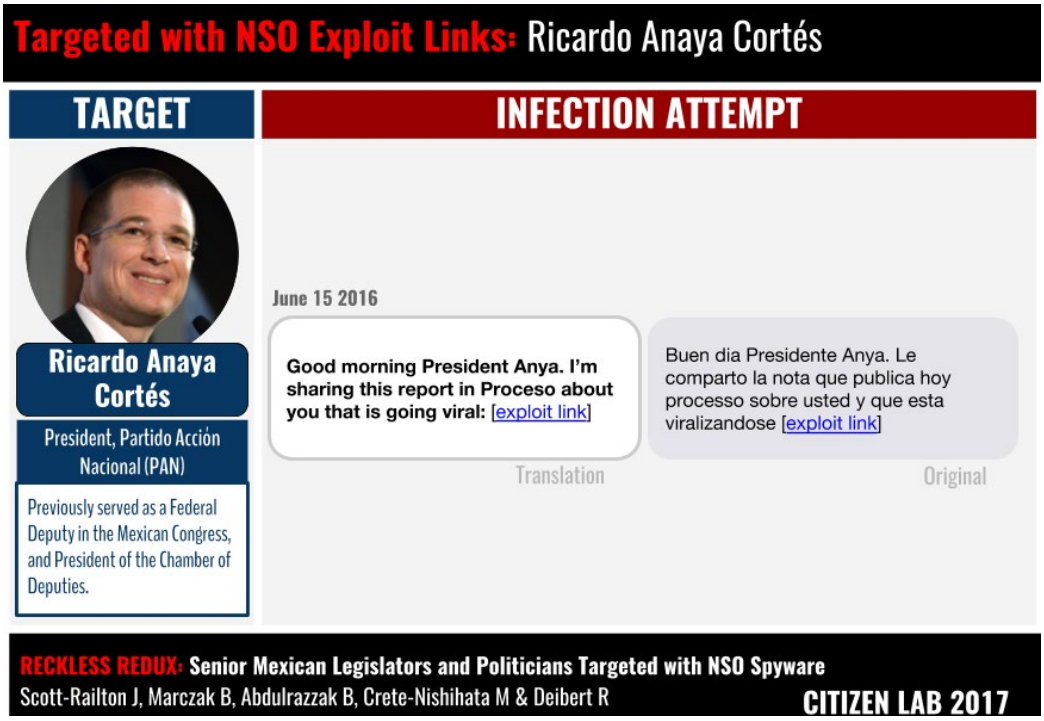


Figure 3: Ricardo Anaya Cortés was targeted with an infection attempt on June 15 2016 while serving as President of PAN, a major Mexican political party (Photo: Wikipedia)

The link in the SMS also pointed to the NSO exploit domain smsmensaje[.]mx.

Target: Fernando Doval

Fernando Doval is the communications secretary for PAN, having previously served as a legislator representing the Federal District (Mexico City) in the Mexican

Congress. On July 14, 2016 he was targeted with an infection attempt via text message.

The message was similar to messages sent to his PAN colleagues, and claimed that he had been mentioned in an article on *Proceso* (Figure 4).

Figure 4: Fernando Rodríguez Doval, the communications secretary of PAN, was targeted with an infection attempt on July 14 2016 (Photo: Wikipedia)

The link in the SMS also pointed to the NSO exploit domain smsmensaje[.]mx.

Conclusion

These cases indicate that during June and July 2016 senior Mexican politicians who are members of PAN were targeted with multiple infection attempts using NSO's technology. While we are not privy to the reasons behind the timing of the targeting, it may be relevant that during this particular timeframe, anti-corruption legislation was being discussed in Congress.

This latest discovery is the result of close collaboration between Citizen Lab and Mexican partner organizations, and provides further evidence of the widespread and highly political targeting using NSO's Pegasus infrastructure. It also reflects the willingness of individuals targeted with infection attempts to come forward and share their cases.

Our investigations have now found NSO used against scientists, health advocates, lawyers, journalists, senators, and politicians in Mexico.

We hope this finding will contribute to further scrutiny and investigation of the way that NSO's Pegasus was used in the Mexico, and across its borders.

Appendix

Full list of messages from the cases discussed in this note.

Target	Text Message Date	Text message Original	Text Message English	Sender Phone Number	Link in SMS	Unshortens to
Ricardo Anaya	6/15/2016	Buen dia Presidente Anya. Le comparto la nota que publica hoy processo sobre usted y que esta viralizandose:	Good morning President Anya. I'm sending you a report in Processo about you that is going viral: [malicious link]	(81) 2210 4015	hxxp://bit[.] ly/29F2psM	hxxps:// smsmensaje[.] mx/8306090s/
Fernando Doval	7/14/2016	Fernando buen dia, te envio esta nota de proceso donde hacen mencion de tu nombre, se esta viralizando mira: [malicious link]	Good day Fernando, I'm sending you this piece from Processo that mentions your name, it is going viral [malicious link]	(81) 2219 4015	hxxp://bit[.] ly/29F2psM	hxxps:// smsmensaje[.] mx/8306090s/
Roberto Gil Zuarth	6/16/2016	Senador amigo estoy destrozada, acaba de morir mi esposo, te envio datos del velatorio, espero me acompanes: [malicious link]	Senator, my friend, my husband just died. I am sending you information about the wake, I hope you can attend: [malicious link]	(81) 2125 3396	hxxp://bit[.] ly/1WONumj	hxxps:// smsmensaje[.] mx/4995075s/
Roberto Gil Zuarth	6/17/2016	Oye Roberto ya viste lo que los del PRD dicen de todos nosotros olo por ganar credibilidad, mira te adjunto: [malicious link]	Hey Roberto, did you see what PRD is saying about us to get credibility, take a look: [malicious link]	(33) 3207 9059	hxxp://bit[.] ly/1WRYHm8	hxxps:// smsmensaje[.] mx/1351276s/
Roberto Gil Zuarth	6/15/2016	Senador buen día, solo paso a compartirte esta nota que publica hoy proceso donde hacen mencion de tu nombre: [malicious link]	Senator, I wanted to share this report from processo where your name is mentioned: [malicious link]	(33) 1923 1306	hxxp://bit[.] ly/1UUsVi6	hxxps:// smsmensaje[.] mx/9993247s/