RECKLESS V

Director of Mexican Anti-Corruption Group Targeted with NSO Group's Spyware

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

AUGUST 30, 2017
RESEARCH REPORT #99

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 V: Director of Mexican Anti-Corruption Group Targeted with NSO Group's Spyware," Citizen Lab Research Report No. 99, University of Toronto, August 2017.

Acknowledgements

Citizen Lab would like to thank Claudio X. González who, along with the other targets that have participated in this investigation, make these investigations possible by consenting to share the targeting.

Special thanks to the teams at Article 19, R3D, SocialTic, for their careful and important investigative work. We would like to especially thank and highlight the exceptional contribution of Luis Fernando García at R3D in this investigation.

Thanks to the whole Citizen Lab team, especially Christine Schoellhorn, Miles Kenyon, and Adam Senft.

Thanks to 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 6 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

- **The director of a prominent anti-corruption organization Mexicanos Contra la Corrupción y la Impunidad (MCCI) was sent infection attempts with NSO Group's Pegasus spyware**
- **The targeting took place as his organization was working on issues related to offshore holdings and corruption among prominent Mexicans and Mexican government officials**
- **This report raises the number to 22 known cases of abusive and improper targeting with NSO Group's government-exclusive spyware**

Introduction

Since 2016, Citizen Lab and our partners R3D, SocialTic, and Article 19 have been conducting an investigation into the abuse of NSO Group's government-exclusive

spyware in Mexico. In six prior reports, published between August 2016 and August 2017, we identified abusive and potentially illegal infection attempts against multiple journalists, lawyers, international investigators, public health practitioners, senior politicians, and anti-corruption activists.

With this report, we are revealing the 22nd known individual abusively targeted with NSO's spyware in Mexico: Claudio X. González, the director of Mexicanos Contra la Corrupción y la Impunidad (MCCI: Mexicans Against Impunity and Corruption). In recent years, González's work, which includes founding MCCI, has focused on investigating and denouncing corruption in Mexico. González previously founded Mexicanos Primero (Mexicans First), an organization working on education issues.

MCCI has conducted a number of high profile investigations, including work with the Panama Papers to scrutinize offshore holdings of prominent Mexicans and investigative work on corruption in areas like procurement and nepotism. In addition, MCCI conducts policy engagement on high-profile issues, such as anti-corruption legislation.

In August and July 2016, while MCCI was engaged in advocacy around Mexico's anti-corruption legislation, its director, Claudio X. González, received two text messages purporting to alert him that he was being discussed in El Universal and Proceso, two prominent Mexican publications. The SMSes were deceptions designed to trick him into clicking on links to NSO's exploit framework. Clicking on the links would have resulted in the infection of his device with NSO's Pegasus malware.

Figure 1: MCCI director and staff targeted with NSO Group's spyware (note that two of the cases were previously reported in Citizen Lab's June 2017 report).

Claudio X. González is not the first individual affiliated with MCCI to be targeted with NSO Group's spyware. On June 19, 2016 Citizen Lab, in collaboration with R3D, SocialTic, and Article 19, published a report that revealed that Salvador Camarena and Daniel Lizárraga, two investigative journalists working with MCCI, were also targeted with infection attempts.

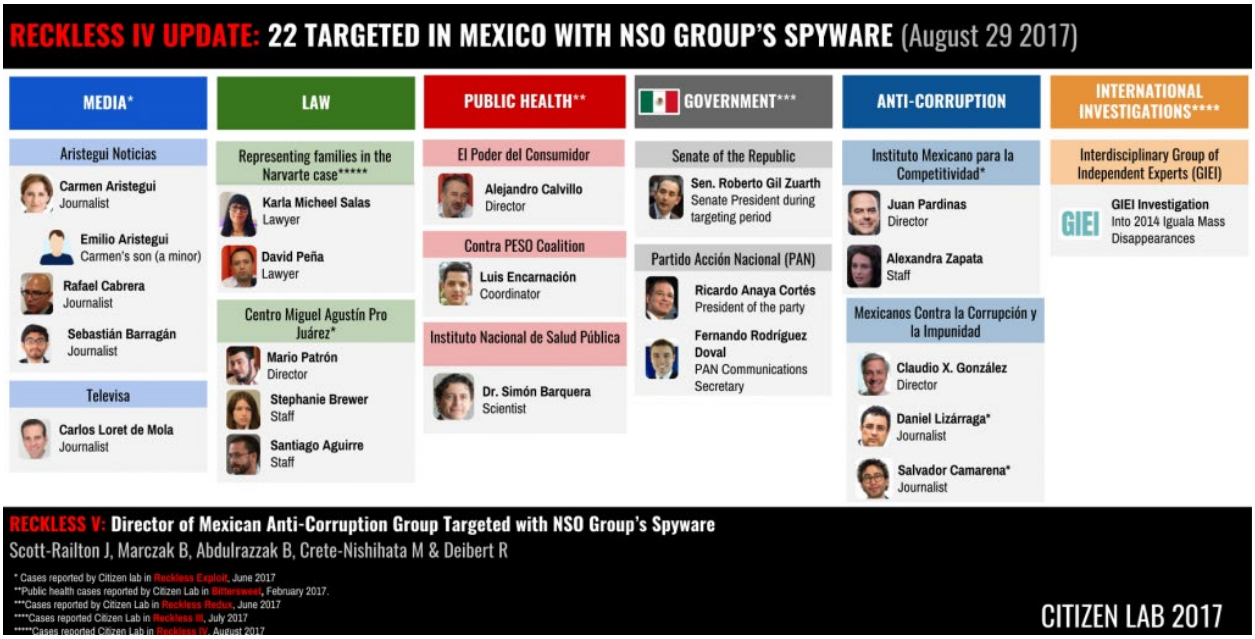

Figure 2: At least 22 individuals have been abusively targeted with NSO Group's spyware in Mexico as of August 29, 2017

Roadblocks and Harassment for Anti-Corruption Efforts

Mexico struggles with corruption across federal and state governments and all major sectors. Mexico has the highest level of perceived public sector corruption among OECD countries, which impacts all sectors of Mexican society. While Mexico's federal government has made some recent progress with anti-corruption legislation, the process is hampered by a lack of political will and harassment of organizations supporting the efforts.

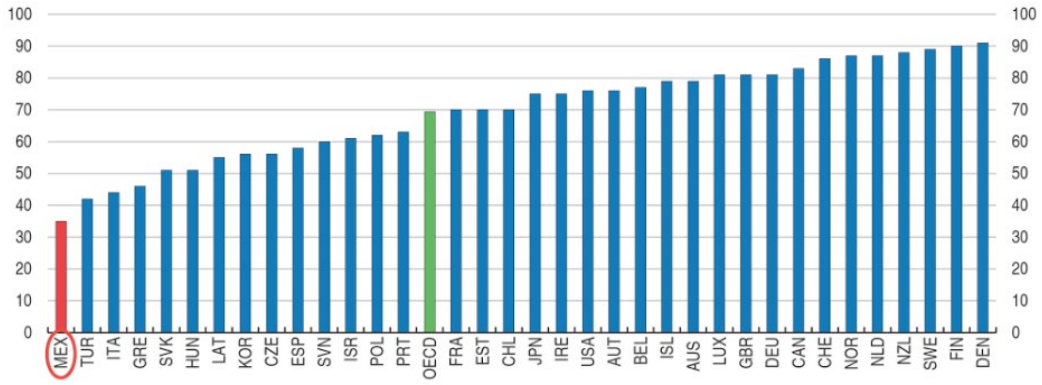

Figure 3: OECD analysis showing Mexico's in last among OECD countries in perceptions of public sector corruption. (Source: OECD)

The cases of Mexico's state governors highlight the twin problems of corruption and impunity in Mexican politics. According to MCCI, since 2000, of the 42 state governors suspected of corruption, only 17 were formally investigated, and four jailed. Four former governors, meanwhile, became fugitives. Concerns about the impunity of governors are high; most recently it was revealed that a fugitive former Mexican governor wanted on drug and money laundering charges continued to receive police protection.

In a climate in which many believe anti-corruption efforts are met with a lack of political will, efforts to promote comprehensive anti-corruption legislation are further hampered by scandals at the highest levels of Mexican government. Even as the Mexican congress recently moved to pass anti-corruption legislation, the process was tarnished by accusations of legislative delay tactics and the legislation was stripped of key provisions.

Meanwhile, organizations advocating against corruption have been the subject of a range of acts of harassment and intimidation. For example, several organizations, including MCCI, have been the targets of systematic audits, and others have been the victims of thefts, harassment, threats, and public denunciations.

Pattern: Anti-Corruption Advocates, Reporters Targeted with NSO Group's Spyware

The infection attempt against González highlights an emerging pattern: journalists and advocates working on corruption are being targeted with NSO Group's spyware. At least three organizations specifically working on corruption issues have had multiple staff members targeted with NSO Group's spyware and journalists who have covered stories related to high-level corruption have also been targeted. Targeted anti-corruption organizations and investigative reporters include:

- Aristegui Noticias
- Instituto Mexicano Para La Competitividad
- Mexicanos Contra la Corrupción y la Impunidad

During the period of targeting, each organization was working on issues related to high level corruption in Mexico.

Infection Attempts Against Claudio X. González

In collaboration with Mexican NGOs R3D, SocialTic, and Article 19, Citizen Lab examined messages sent to Claudio X. González, and confirmed that he was targeted with NSO's spyware.

On July 27 and August 2 2016, González received text messages as part of a ruse to trick him into clicking on malicious links. If clicked, the messages would have infected his device with NSO Group's Pegasus spyware. The first message, received on July 27th 2016, claimed that he was the subject of negative press coverage by major Mexican newsmagazine, Proceso. The second message, which arrived a few days later on August 2nd, used a similar ruse, but spoke of negative coverage in the newspaper El Universal. The full text of the messages, as well as additional metadata are in **Appendix A**.

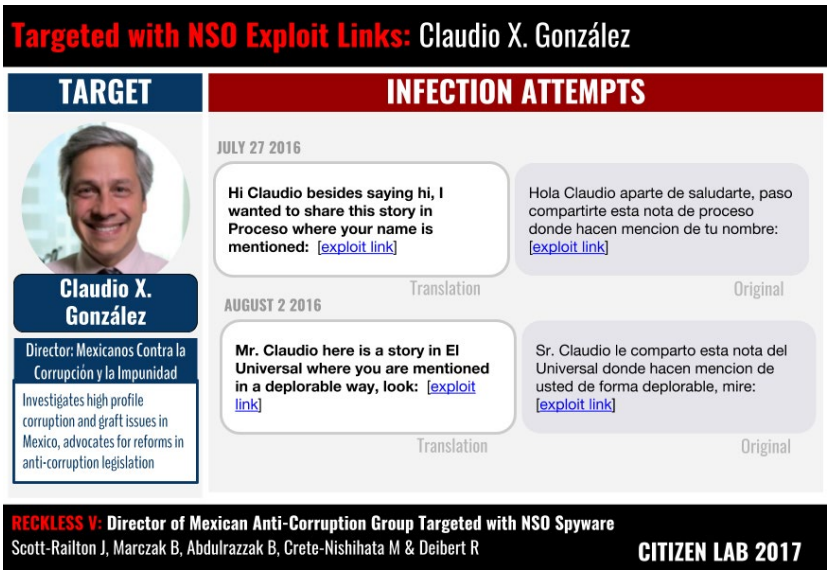

Figure 4: Text messages with infection attempts sent to Claudio X. González, director of anti-corruption organization MCCI.

Both links were shortened with bit.ly, and pointed to the domain smsmensaje[.]mx, a domain that is part of NSO's exploit framework, and has been present in many of our previous investigations of NSO abuse in Mexico.

Links to NSO Group's Exploit Infrastructure

Clicking on the shortened links in either messages would have resulted in a redirection to the NSO Group's exploit framework, and the silent infection of González's device with Pegasus spyware.

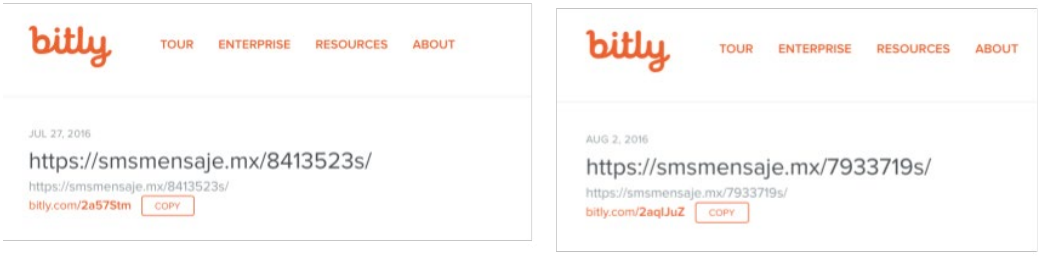

Figure 5: Publicly available data from the bit.ly shortener shows that the NSO exploit links were shortened by the operator on the same dates that the messages were received by González.

Publicly available data from the bit.ly shortener confirms that the NSO links were shortened on the same days that the messages were reported received (July 27 and August 2, 2016).

We first identified the smsmensaje[.]mx domain while performing internet scanning for unique fingerprints belonging to NSO's exploit infrastructure. Subsequent to the original find, we have consistently identified this domain in each of the cases established as part of our investigation into the Mexican case (reports: 1, 2, 3, 4, 5).

As shown in our prior investigations, a target clicking on the link would be infected using a chain of zero-day exploits against the operating system. Analyses have now been published on both NSO's iPhone and Android implants.

Conclusion: 22 Cases and Counting

The targeting of Claudio X. González, director of anti-corruption organization MCCI, marks the 22nd documented case in Mexico in which NSO Group's Pegasus spyware has been used in infection attempts. As with the previous cases, this incident was identified in cooperation with our partners R3D, SocialTic, and Article 19. At the time of writing, our investigations have revealed targets that include multiple journalists, lawyers, international investigators, public health practitioners, senior politicians, and anti-corruption activists.

Previous reports highlighted a pattern of targeted infection attempts against journalists and investigators who questioned government accounts of suspicious killings. This report highlights what appears to be a second, troubling pattern: systematic *targeting of organizations focused on issues of corruption* (Aristegui Noticias, MCCI, and IMCO). Just as was the case with those investigating the killings, the digital targeting of anti-corruption groups compounds the widely-reported patterns of harassment against civil society organizations.

Our technical methods do not permit us to conclusively attribute these operations to a particular customer. However, each finding, as well as extensive investigations by Mexican organizations, contribute to the mounting circumstantial evidence pointing to an entity or entities within Government of Mexico as the NSO Group customer(s) responsible for these abuses. Moreover, leaks show that the Mexican office of the prosecutor is an NSO Group customer, and, although he denied that the spyware was being abused, the Mexican President has also publicly admitted that the Mexican government has also purchased the technology.

NSO's Oversight and Abuse Problems are a Matter of Public Record

As case after case emerges, it has become a matter of public record that NSO Group has serious problems with oversight and control of its offensive technology, and has been unable to prevent customers from committing abuses and possibly illegal activities.

To date, there is evidence of systematic abuse of NSO's spyware in two countries, Mexico and Panama, and further evidence of abuse in the United Arab Emirates showing that at least three of NSO Group's governmental customers have seriously abused their product. These cases have led to ongoing governmental investigations (in Mexico and Panama), and numerous calls for further investigation by international bodies. In addition, there is evidence of likely-illegal cross-border targeting into the United States, and the targeting of United States Embassy personnel and American citizens.

Nevertheless, NSO Group has reportedly attracted investment interest from US firms, even as more cases of the targeting of Americans come to light. Recently, NSO Group and its majority owner, Francisco Partners, were reportedly negotiating the sale of a 40% stake to investors led by Blackstone Group L.P (NYSE: BX). That negotiation has reportedly fallen through amid questions about human rights and

due diligence from Citizen Lab and civil society groups R3D, SocialTic, Article 19, Consumer Power, Centro PRODH, Access Now, and Business and Human Rights Group.

This report, and our six previous reports on abuses of NSO Group's spyware that have come before it, a growing body of research from many other groups, and other ongoing investigations, make it clear that the market for "lawful intercept" and "government exclusive" surveillance technologies has a fundamental problem of oversight. None of the widely-known sellers of this technology (Hacking Team, Gamma Group, and NSO Group) have shown the will, or the capability, to prevent abuses.

Any investor exploring the possibility of acquiring a stake in developers of government-exclusive spyware like NSO Group must reckon with this reality, and the substantial business, due diligence, and human rights risks that come with it.

Appendix A: Full Message List

Target	Original Message	English	Date	Link in SMS	Unshortened	Telephone Number
Claudio X. González	Sr. Claudio le comparto esta nota del Universal donde hacen mencion de usted de forma deplorable, mire: [enlace malicioso]	Mr. Claudio here is a story in El Universal where you are mentioned in a deplorable way, look: [malicious link]	August 2, 2016	hxxp://bit[.]ly/2aqIJuZ	hxxps://smsmensaje[.]mx/7933719s/	(33) 1926 0317
Claudio X. González	Hola Claudio aparte de saludarte, paso compartirte esta nota de proceso donde hacen mencion de tu nombre: [enlace malicioso]	Hi Claudio besides saying hi, I wanted to share this story in Proceso where your name is mentioned: [malicious link]	July 27, 2016	hxxp://bit[.]ly/2a57Stm	hxxps://smsmensaje[.]mx/8413523s/	(55) 6108 9094