RECKLESS IV

Lawyers for Murdered Mexican Women's Families Targeted with NSO Spyware

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

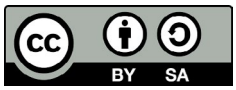
AUGUST 2, 2017
RESEARCH REPORT #98

munk school
OF GLOBAL AFFAIRS & PUBLIC POLICY

UNIVERSITY OF TORONTO

THECITIZENLAB

Copyright



Suggested Citation

John Scott-Railton, Bill Marczak, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert. "Reckless IV: Lawyers for Murdered Mexican Women's Families Targeted with NSO Spyware," Citizen Lab Research Report No. 98, University of Toronto, August 2017.

Acknowledgements

Special thanks to Karla Micheel Salas and David Peña who consented to share this case with the collaborating organizations and with the public.

Special thanks to the teams at Article19, R3D, SocialTic, for their careful and important investigative work. We would like to especially thank and highlight the contribution from Sandra Patargo at Article 19 and her colleagues as well as Luis Fernando García at R3D.

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

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.

Contents

This report is Part 5 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

- **Two prominent lawyers representing the families of three slain Mexican women were sent infection attempts with NSO Group's Pegasus spyware**
- **The infection attempts occurred in September and October of 2015 as public frustration grew at the Mexican government's seemingly contradictory statements about the "Narvarte" case**
- **With this latest report, we have now identified at least 21 cases in Mexico of abusive, improper targeting with NSO Group's Pegasus spyware**

Introduction

This research note reveals newly-discovered infection attempts using NSO Group's government-exclusive Pegasus spyware. The targets were Karla Micheel Salas and David Peña, Mexican lawyers and human rights defenders representing the families of Nadia Vera, Yesenia Quiroz Alfaro, and Mile Virginia Martin. Vera was a government critic and women's rights advocate who was slain in July 2015 along with journalist Rubén Espinosa, Alejandra Negrete, Alfaro, and Martín in the Narvarte neighborhood of Mexico City.

Salas and Peña were targeted with NSO Group's Pegasus spyware in September and October 2015 as questions grew about official accounts of the Narvarte killings, and the reported torture, and sexual assault of the victims.

The Narvarte killings illustrate the exceptionally serious threats to journalists and government critics in Mexico, and contribute to what has been called "climate of impunity" surrounding such killings. Many of these cases are linked to the government, with a recent report linking officials to over half of the reported cases of violence against journalists. Evidence is also growing that digital surveillance of journalists with spyware is yet another aspect of this climate of extreme threat.

In four prior reports, Citizen Lab and our partners R3D, SocialTic, and Article19 have documented extensive abuses of NSO Group's spyware in Mexico. Targets have included journalists, anti-corruption groups, health scientists, political figures, opposition party officials, and international investigators. In total, we have now publicly reported 21 cases in Mexico of abusive targeting with NSO's spyware.

A Pattern of Targeting Lawyers and Investigators with NSO Group's Spyware

A pattern has emerged in a subset of these cases: lawyers and investigators working on targeted killings in Mexico have been targeted with NSO Group's spyware when their investigations questioned official accounts provided by the authorities.

Prior to this discovery, Citizen Lab reported that, in March of 2016, a team of international experts investigating the 2014 Iguala mass disappearance of 43 students in Veracruz were targeted with NSO's Group's Pegasus spyware as they prepared their final reports. Then, from April to June of 2016, lawyers working with Centro PRODH, an organization representing the families of the disappeared students, were also targeted with NSO Group's Pegasus spyware.

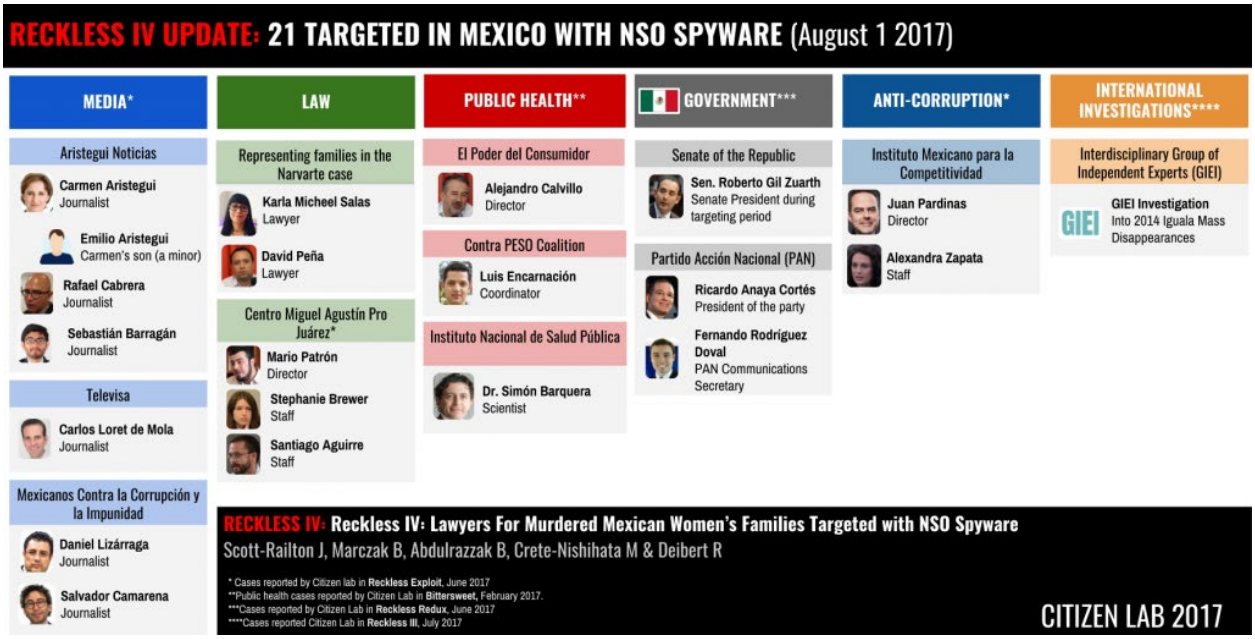


Figure 1: To-date our research has identified over 21 cases of misuse of NSO Group's spyware in Mexico

NSO Group: A Majority American-Owned Spyware Company

NSO Group is an Israel-based company that sells digital surveillance technology, known colloquially as "spyware," that enables the operator to remotely infect and spy on mobile phones. The spyware infects phones once a target is tricked into clicking on a link, triggering a chain of sophisticated zero-day exploits that allow the surveillance technology to be implanted on the phone.

Although based in Israel, NSO Group's majority owner is Francisco Partners, a private equity firm based in San Francisco. At the time of writing, American investment firms Blackstone Group Ltd. and ClearSky are reportedly in talks to purchase a 40 percent stake in NSO Group Technologies for $400 million from Francisco Partners.

Given NSO Group's demonstrated difficulties preventing abuse of their export-controlled spyware, Citizen Lab has written an open letter to Blackstone. The letter informs Blackstone of our findings and requests clarification on the due diligence process surrounding the reported acquisition. A number of advocacy organizations, including Access Now, have also publicly stated concerns over the process.

Karla Micheel Salas and David Peña

Karla Micheel Salas and David Peña are Mexican lawyers and human rights defenders who have worked on a series of high profile cases. Notably, they represent the families of Nadia Vera, Yesenia Quiroz Alfaro, and Mile Virginia Martin who were

slain alongside journalist Rubén Espinosa and Alejandra Negrete in the so-called Narvarte killings. In addition to this case, Salas and Peña are well known for their work on women's rights.

Figure 2: Karla Micheel Salas and David Peña, prominent lawyers representing the family of Nadia Vera (Image: Cima Noticias)

The "Narvarte" Killings

On July 31, 2015, journalist Rubén Espinosa and activist Nadia Vera were killed, execution style, by shots to the head along with Vera's flat mates and cleaner in Mexico City. Espinosa and Vera had both been critical of Javier Duarte, the then-governor of Veracruz, and in the months leading up to the killing had traveled to Mexico City seeking safety from a series of increasingly troubling incidents and threats. Reportedly, there was evidence that Espinosa had been tortured and that Vera and the others had been subjected to torture and sexual assault before being killed.

Figure 3: Nadia Vera and Rubén Espinosa were killed on July 31, 2015, along with three other women. The crime scene reportedly included evidence of torture and sexual assault. (Images: Rompeviento, W Radio)

In the wake of the executions, numerous questions were raised about the official investigation into the case, which promoted the theory of a robbery as the likely

motive and identified a serial rapist and two never-found petty criminals as accomplices. This theory was rejected by many who pointed out that valuables were not taken and led to a public outcry and protests over violence against journalists.

A number of reports pointed to an another possible motive: governor Duarte was particularly irked by an unflattering photo taken by Espinosa. Reportedly, the governor attempted to buy out every copy of the magazine, *Proceso*, with the photo on the cover. In the month prior to the killing, Duarte had made statements that many viewed as thinly veiled threats against journalists whom he accused of being close with "criminals," including stating that "...we will shake the tree and many rotten apples will fall…" When asked after the murders to clarify his earlier statements, he denied that he was referring to journalists.

Duarte's time in power was plagued with reports of corruption, and he later fled the country in the face of accusations of having stolen tens of millions of dollars in public money. He was later found in Guatemala and extradited back to Mexico to face corruption and graft charges.

The Narvarte killings have triggered local and international condemnation, including by the head of UNESCO.

Infection Attempts

This section outlines the infection attempts against Peña and Salas using NSO's exploit infrastructure. The targeting was collected by R3D and Article 19 and shared with Citizen Lab researchers.

Target: Lawyer David Peña

On September 25 and October 15, 2015, Peña received text messages containing infection attempts with NSO's Pegasus spyware. The messages were designed to trick him into clicking on the links. Once clicked, the links would infect Peña's phone. The first message referenced an organization Peña belongs to, the second masqueraded as a "service message" (See **Figure 4**).

Figure 4: Infection attempt sent to Lawyer David Peña in September and October 2015 (Picture: Cima Noticias)

On September 25, 2015, Peña received a "service message" containing a link.

Then, on October 15, 2015 he received a message purporting to be a news story revealing audio of a conspiracy to commit extortion by a member of Mexico's Association of Democratic Lawyers (ANAD: Asociación Nacional de Abogados Democráticos, A.C.) and Perla Gomez, the Director of the Human Rights Commission for Mexico City (Comisión de Derechos Humanos del Distrito Federal).

Both messages contained links to `smsmensaje[.]mx`, a domain previously identified in our reporting as part of NSO's exploit framework.

Target: Lawyer Karla Micheel Salas

On October 1, 2015, Salas received a message purporting to inform her of a death and inviting her to a wake (See **Figure 5**). Clicking on the link would have resulted in the infection of her device with NSO's Pegasus exploit infrastructure and spyware.

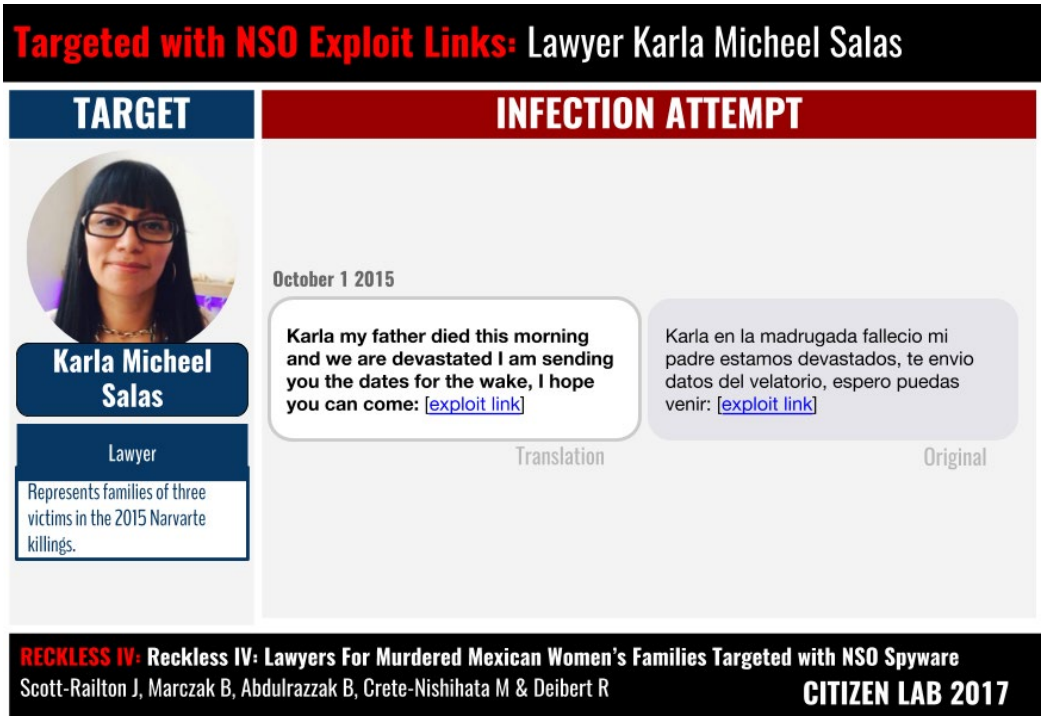


Figure 5: Infection attempt sent to lawyer Karla Micheel Salas (Picture: Publico)

The message contained a link to to smsmensaje[.]mx, the same domain used to target Peña.

Links to NSO Exploit Infrastructure

The messages sent to lawyers Peña and Salas were ruses designed to trick them into clicking on a link. Clicking on the link would have resulted in the silent infection of their devices.

The messages sent to both Peña and Salas included links to the following domain:

```
smsmensaje[.]mx
```

Prior Citizen Lab research included Internet scanning using fingerprints matching command and control servers belonging to NSO Group's exploit infrastructure. The smsmensaje[.]mx server was first identified during this scanning. The domain has been subsequently identified in all of Citizen Lab's prior reports on the Mexican NSO case (reports: 1, 2, 3, 4).

Previous Citizen Lab investigations have shown that in 2016, for example, the system used a chain of three zero-day exploits against Apple's iOS to deliver NSO's spyware payload, called "Pegasus." Once the link has been clicked, the exploit

infrastructure exploits vulnerabilities in the device's browser and operating system to deliver NSO's Pegasus spyware for Apple devices.

Based on research by Google Inc. and Lookout Security, we know that NSO has developed a similar spyware product for the Android operating system.

Conclusion: 21 Cases and Counting

This investigation raises the number of confirmed abuses of NSO's spyware in Mexico to 21. The murders and evidence of torture of Nadia Vera, Rubén Espinosa, Alejandra Negrete, Yesenia Quiróz, and Mile Virginia Martín are exceptionally disturbing, as are the reports that evidence of sexual assault and torture were found at the scene.

The Narvarte case served as a touchstone for popular anger over the mortal danger faced by journalists and advocates who earn the ire of Mexican government officials. Along with numerous other similar high profile cases, such as the 2014 Iguala Mass Disappearances of 43 students, and countless other murders less reported on, the case has crystallized popular frustration with official investigations.

Even as lawyers for the family of Nadia Vera were questioning how Mexico City's Attorney General was investigating the case, their phones were targeted with NSO Group's government-exclusive Pegasus spyware.

This is not the only case in which lawyers and investigators defending the families of victims of government-linked atrocities have been targeted with NSO Group spyware. This disturbing pattern also highlights the challenge that the Mexican Attorney General faces as they investigate these reported abuses. While we cannot technically attribute the NSO deployment to a particular customer, or an entity within the Mexican government, it is noteworthy that, as leaked documents show, the Mexican Attorney General's office has been one of NSO's clients. The Mexican president has also confirmed Mexican government agencies have purchased NSO Group technology, but denied the abuses.

NSO Group: Patterns of Abuse and Due Diligence Issues

There is now abundant evidence that NSO Group has a problem preventing misuse of its export-controlled spyware.

Mexico is not the only case in which there is evidence of misuse of NSO's spyware. In the United Arab Emirates, Citizen Lab has shown how human rights defender Ahmed Mansoor was targeted with NSO's spyware in August 2016. Citizen Lab reports previously found that in 2011 and 2012 Mansoor was targeted by the UAE government using two other government-exclusive pieces of spyware. Mansoor is currently detained in the UAE as a prisoner of conscience according to Amnesty International. Clearly, NSO's due diligence process for selling to the UAE is highly questionable given the UAE's notorious spyware abuse in prior cases.

Panama: Reports of an NSO Customer Targeting Panamanians and Americans

Former president of Panama Ricardo Martinelli is currently detained without bail in the United States and facing extradition to Panama. He is accused of diverting $13.4 million dollars intended for social programs to purchase NSO's spyware. The accusations stem from criminal charges prepared by the Panamanian government that he used public money to set up an NSO deployment targeting Android and Blackberry phones to monitor up to 150 of his political rivals.

According to a recent investigative report by Univision citing affidavits in the case, NSO Group's spyware was used to record communications, including spousal disputes, of Martinelli's opponents. Recent reports provide a window into these cases and how the technology was used to spy on and discredit opponents.
Pitti acknowledged that he was in charge of eavesdropping on 25 people among whom was the opposition deputy Zulay Rodriguez...

> *"When I got a recording of a call in which Mrs. Rodriguez was arguing with her husband who accused her of infidelity, I immediately reported it to Ronny Rodriguez who informed Martinelli of the contents, '' Pitti explained.*
>
> *According to Pitti, Martinelli ordered the audio edited and uploaded to YouTube from an internet cafe.*

Source: Univision, citing an affidavit by Pitti

The criminal case prepared by the Panamanian government is built on the forensic analysis of materials (computers, hard drives, and digital media) generated as part of the program to store and review surveillance data. The complaint outlines in detail a wide range of targets, including businessmen, journalists, civil society members, politicians, and their family members and relatives. The complaint alleges that NSO Group's spyware was used to monitor political discussions and strategy meetings of the president's rivals, as well as their family and personal affairs.As with the

Mexican case, the Panamanian case includes reports that NSO Group's technology was used to monitor Americans, including staff at the United States Embassy in Panama. American targets also included political consultants working for two of the former president's opponents in the 2015 presidential election: Christian Ferry and U.S. Army Colonel (Ret.) Richard Downie.

According to the investigation, the president received a sealed envelope each morning with the results of the previous day's monitoring of his rivals. The president would also sometimes publicly intimate the possession of certain information or present it to the targets of monitoring.

Together, these cases, involving alleged gross abuse of NSO Group's spyware, paint a troubling picture of the international market for spyware—and NSO's Group's role in supplying this technology in several highly questionable cases.

Citizen Lab has recently written a letter to Blackstone Group, which is contemplating a $400 million investment in NSO Group, to make them aware of these concerns and asking specific questions about due diligence. To date, the letter has received no response.

Appendix: Full Message Details

Target	Original Message	English	Date	Link in SMS	Telephone Number
David Peña	UNOTV.COM/ REVELAN AUDIOS TELEFONICOS ENTRE DE INTEGRANTE DE LA ANAD Y PERLA GOMEZ. PLANEARON EXTORSION. AUDIOS EN: [exploit link]	UNOTV.COM/ PHONE CALL AUDIO BETWEEN MEMBER OF ANAD AND PERLA GOMEZ. THEY PLANNED EXTORTION. AUDIO: [malicious link]	October 15, 2015	hxxps:// smsmensaje[.] mx/6070525s/	(55)61676879
David Peña	Mensaje de servicio [enlace malicioso]	Service message [malicious link]	September 25, 2015	hxxp:// smsmensaje[.] mx/9142658s/	(55)49576224
Karla Micheel Salas	Karla en la madrugada fallecio mi padre estamos devastados, te envio datos del velatorio, espero puedas venir: [enlace malicioso]	Karla my father died this morning and we are devastated I am sending you the dates for the wake, I hope you can come: [malicious link]	October 1, 2015	hxxp:// smsmensaje[.] mx/2265561s/	(55)35044351