RECKLESS III

Investigation Into Mexican Mass Disappearance Targeted with NSO Spyware

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

JULY 10, 2017
RESEARCH REPORT #96

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 III: Investigation Into Mexican Mass Disappearance Targeted with NSO Spyware," Citizen Lab Research Report No. 96, University of Toronto, July 2017.

Acknowledgements

Citizen lab would like to thank to the GIEI for consenting to share this case with the collaborating organizations, and with the public.

Special thanks to the teams at R3D, SocialTic and Article19, for their careful and important investigative work. We would like to especially thank and highlight the contribution of Luis Fernando García and his colleagues at R3D.

Thanks to the whole Citizen lab team, especially Miles Kenyon, Adam Senft, 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.

This report is Part 4 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 international investigation into the 2014 Iguala Mass Disappearance was targeted with infection attempts using spyware developed by the NSO group, an Israeli "cyber warfare" company**
- **A phone belonging to the Interdisciplinary Group of Independent Experts (GIEI), a group of investigators from several countries, was sent text messages with links to NSO's exploit infrastructure**
- **The infection attempts took place in early March of 2016, shortly after the GIEI had criticized the Mexican government for interference in their investigation, and as they were preparing their final report**
- **Our published investigations have now confirmed at least 19 individuals targeted with NSO in Mexico, including lawyers, politicians, journalists, anti-corruption activists, scientists, public health campaigners, government officials, and their family members.**

Introduction

This research note reveals that an international group of experts investigating the 2014 Iguala Mass Disappearance of 43 Mexican students were targeted with Pegasus, the government-exclusive commercial spyware made by NSO Group.

NSO Group, the creator of the Pegasus spyware, is an Israeli company that describes their spyware product as designed for tracking criminals and terrorists. Notably, some have reported that it is re-branding as Q Cyber Technologies. Prior Citizen Lab reporting has identified abuses of Pegasus, including its use by the UAE government, to target prominent human rights defender Ahmed Mansoor.

While NSO Group is an Israeli company, its majority owner is the United States based private equity firm Francisco Partners. Recent reports suggest that Francisco Partners is considering selling NSO Group, with a reported valuation of $1 billion. Francisco Partners also owns a number of other companies that develop and sell mass surveillance technology.

Figure 1: Journalists, lawyers, scientists, public health campaigners, senators, politicians, and international investigations have all been identified as targeted with NSO's spyware

Citizen Lab researchers, along with Mexican collaborators R3D, SocialTic and Article 19, are conducting an investigation into the misuse of NSO Group's government-exclusive Pegasus spyware in Mexico.

The first report from the investigation, published on February 11 2017, revealed that three Mexican food scientists and anti-obesity campaigners were targeted with NSO's Pegasus spyware. These three individuals were linked by their support for Mexico's Soda Tax, which was opposed by commercial interests.

The second report, published on June 19 2017, revealed that 12 journalists, lawyers, and family members were targeted with over 76 infection attempts with Pegasus. The targeted journalists included some of Mexico's most prominent journalists, like Carmen Aristegui and Carlos Loret de Mola. Targeted lawyers included individuals working for organizations representing family members of those lost in the 2014 Iguala Mass Disappearance. Other targets included anti-corruption organizations. Notably, Carmen Aristegui's minor child was also targeted while in the United States, with techniques that included impersonating the United States government.

The third report, published on June 29 2017, demonstrated that three prominent Mexican politicians from the opposition National Action Party (PAN) were similarly targeted with NSO spyware. The targets included the then-president of Mexico's Senate, the president of the PAN party, and its communications director.

Following the initial publication, numerous individuals who suspected that they were targeted with NSO's Pegasus have contacted Citizen Lab, R3D, SocialTic and Article19. Among those contacts is the Group of Independent Experts (GIEI), an international group of expert investigators working on the 2014 Iguala Mass Disappearance. Working closely with R3D, which collected the original messages, Citizen Lab has analyzed messages sent to a phone belonging to the GIEI, and confirmed that they were infection attempts using NSO's technology.

This report adds to our prior analysis a new category of targets in addition to lawyers, politicians, journalists, anti-corruption activists, scientists, public health campaigners, government officials, and their family members: **international expert investigators working on the 2014 Iguala Mass Disappearance.**

The GIEI Investigation

On September 26, 2014, 43 students from the Ayotzinapa Rural Teachers' College were disappeared while travelling to Mexico City to participate in an event commemorating the Tlatelolco Massacre. The event, referred to as the 2014 Iguala Mass Disappearance, and the government's response, prompted calls for an independent investigation.

In November 2014 the Interdisciplinary Group of Independent Experts (GIEI) was formed to conduct an independent investigation into the case. The group, convened by the Inter-American Commission on Human Rights (IACHR) was the result of an agreement between the Organization of American States (OAS), representatives of the disappeared students, and representatives from the Mexican government, including the Office of the Prosecutor (PGR).

GIEI investigators were drawn from Colombia, Chile, Guatemala and Spain. The experts made several visits to Mexico, beginning in March 2015 to conduct their investigation.

The GIEI's findings have cast doubt on important elements of the Mexican Government's accounts of the events surrounding the disappearances, such as whether there was government involvement, and the purported location of the students' bodies. Following the publication of their initial report, the GIEI was the target of harassment and criticism, attributed to allies of the Mexican government. The PGR also briefly opened an investigation into the executive secretary of the IACHR for "fraud." United Nations Special Rapporteurs have referred to this harassment as a defamation campaign to discredit the results of the GIEI investigations.

We have found that the GIEI was targeted shortly after publicly protesting interference in their investigation by the Mexican government and the PGR, and in the period prior to the publication of their final report investigating the disappearances.

Reporting has identified the Office of the Prosecutor as an NSO client, and suggested that the transaction may have been run through an intermediary company.The president of Mexico has also confirmed that the Mexican Government is a customer of NSO Group.

Infection Attempts Against GIEI Investigators

In March of 2016, while their final report was being prepared, a phone belonging to GIEI investigators was targeted with at least two infection attempts using NSO Exploit links.

In March 2016 a phone belonging to the GIEI group received two messages designed to trick the recipient into clicking. The two messages related to the purported death of a relative.

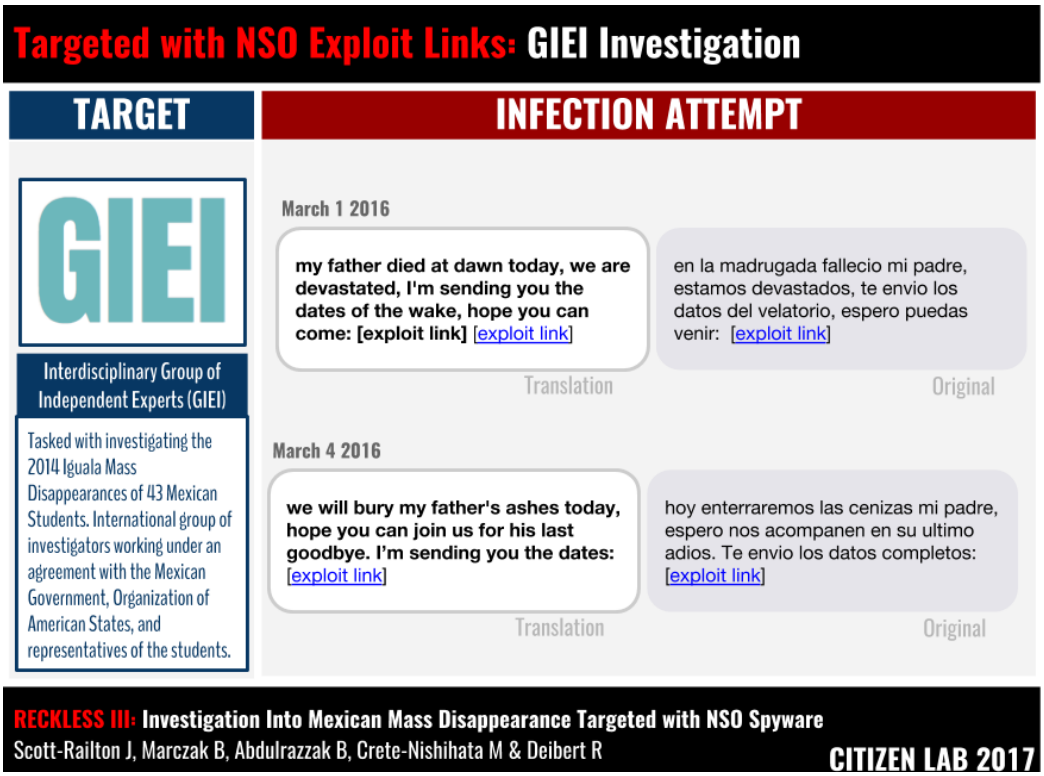

Figure 2: Infection attempts sent to a phone belonging to the GIEI investigation as the investigators were preparing their final report.

The messages contained a link to a URL on the domain smsmensaje[.]mx. Clicking on the link would have resulted in the infection of the phone with NSO's Pegasus malware (see: **Links to NSO Exploit Infrastructure**). The domain `smsmensaje[.]mx` has been identified in previous Citizen Lab reporting as used to target senior Mexican politicians, as well as journalists and lawyers.

Several additional elements of this case suggest that the same NSO operator may be responsible. The text message lures are highly similar to those described in the past three Citizen Lab reports uncovering NSO targeting in Mexico, each of which included messages concerning death of a relative or details of a funeral service.

In addition, one of the messages appeared to have been sent from 55 52 89 94 27. The same number was observed displayed on infection attempts sent to Carmen Aristegui on at least three occasions in February 2016. While we cannot confirm whether or not the number was spoofed, the use of the same number (spoofed or legitimate) suggests further overlap between the NSO Pegasus operator involved in these infection attempts.

Timing of the Infection Attempts

The infection attempts occurred during a period in which the GIEI had faced harassment, and had just publicly criticized the Mexican government for hampering

the progress of the investigation. During the same period, the GIEI was preparing a final report, which rejected claims central to the Government's account of what had happened. The report also included findings indicating investigative irregularities, and torture of suspects, during the PGR's investigation.

On February 21, 2016 the GIEI publicly asserted that their investigation had been obstructed and deliberately hampered by the Mexican Government and the PGR.

On March 1, just over a week later, a phone belonging to the investigation received an infection attempt. A second attempt followed on March 4. The GIEI published its final report on April 24, 2016.

Links to NSO Exploit Infrastructure

The links in the text messages, when clicked, would silently infect the visitor's phone with NSO's Pegasus spyware.

Once infected, the Pegasus implant on the phones phones would connect with Pegasus' Command and Control (C2) servers, enabling the NSO customer to invisibly control the phone's microphone and camera, as well as collect all of the contacts, e-mails, messages, geolocation, and other personal information on the phone.

The links were shortened with bit.ly, and created on the same dates of the messages (see: Appendix). They un-shortened to a domain that we previously identified using scanning for signatures of NSO servers as part of NSO exploit infrastructure:

```
smsmensaje[.]mx
```

Notably, the domain has been identified in all of Citizen Lab's prior reporting of NSO targeting in Mexico.

Conclusion

The GIEI investigation into the 2014 Iguala Mass Disappearance was targeted with infection attempts using NSO Group's Pegasus spyware. The attempts came while the GIEI was preparing their final report, and just over a week after they had publicly criticized the Mexican government for interference in their investigation.

The GIEI was created with the agreement of the Mexican government and the Organization of American States to serve as an independent, impartial body to conduct an investigation into a serious event: the disappearances of 43 students.

The infection attempts were clearly intended to compromise the privacy and integrity of the GIEI investigative process. We speculate that the operators behind these attempts may have sought to learn the theories, sources, and substance of the investigation as the final report was being prepared.

Notably, GIEI report strongly contradicted key statements and theories by the Mexican government. The report also highlighted irregularities in the investigation led by Mexico's Office of the Prosecutor (PGR), a known NSO client.

It is self evident that elements of the Mexican government would be interested in the activities of the GIEI during the time-frame in which the targeting with NSO took place.

We previously reported that lawyers representing families of the victims were targeted with NSO spyware. Taken together with the GIEI targeting, this suggests the NSO operators were heavily involved in attempting to monitor various parties to the case that had been critical of the Government's handling of the investigation.

19 Cases and Counting

The infection attempts against the GIEI are the latest case in which NSO Group's technology has been found to be involved in surveillance targeting in Mexico outside of the scope of what could reasonably be defined as anti-terror, criminal, or national security operations. Our published investigations, and the work of our collaborators at R3D, SocialTic and Article 19, have now confirmed at least 19 individuals targeted with NSO in Mexico, including lawyers, politicians, journalists, anti-corruption activists, scientists, public health campaigners, government officials, international investigators and family members.

As with prior reports, we do not conclusively attribute these infection attempts the Mexican government. However, each new case contributes to the already-strong circumstantial evidence that entities within the Mexican government are the responsible party.

We hope that this latest case will contribute to the efforts underway to more fully uncover the scope and scale of how NSO Group's government-exclusive spyware has been aggressively abused to target Mexican civil society.

Appendix

This appendix contains the list of messages sent to GIEI phones that have a confirmed link to NSO's exploit framework.

Original Message	English	Date	Link in SMS	Unshortened link in SMS	Telephone Number
en la madrugada fallecio mi padre, estamos devastados, te envio los datos del velatorio, espero puedas venir: [exploit link]	my father died at dawn today, we are devastated, I'm sending you the dates of the wake, hope you can come: [exploit link]	March 1 2016	hxxp://bit[.]ly/1OLQXs0 (Created March 1 2016)	hxxps://smsmensaje[.]mx/2678883s/	555 9063534
hoy enterraremos las cenizas mi padre, espero nos acompanen en su ultimo adios. Te envio los datos completos: [exploit link]	we will bury my father's ashes today, hope you can join us for his last goodbye. I'm sending you the dates: [exploit link]	March 4 2016	hxxp://bit[.]ly/1pqkKC4 (Created March 4 2016)	hxxps://smsmensaje[.]mx/4435381s/	555289 9427Leer el post de R3D