BITTER SWEET

Supporters of Mexico's Soda Tax Targeted With NSO Exploit Links

By John Scott-Railton, Bill Marczak, Claudio Guarnieri, and Masashi Crete-Nishihata

FEBRUARY 11, 2017
RESEARCH REPORT #89

munk school
OF GLOBAL AFFAIRS & PUBLIC POLICY

UNIVERSITY OF TORONTO

THECITIZENLAB

Copyright

Suggested Citation

John Scott-Railton, Bill Marczak, Claudio Guarnieri, and Masashi Crete-Nishihata. "Bitter Sweet: Supporters of Mexico's Soda Tax Targeted With NSO Exploit Links," Citizen Lab Research Report No. 89, University of Toronto, February 2017.

Acknowledgements

We would like to thank our Citizen Lab colleagues Ron Deibert, Irene Poetranto, Adam Senft, Sarah McKune, and Adam Hulcoop.

Additional thanks to other researchers, Jen Weedon, and TNG.

Special thanks to R3D and SocialTIC for their assistance with this project. Without their extensive work assembling this case, our report would not have been possible.

We thank Access Now, especially their Help Line team, and Amnesty International for assistance compiling evidence, and ensuring that this case came to our attention.

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 1 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

- **A prominent scientist at the Mexican National Institute for Public Health (INSP) and two directors of Mexican NGOs working on obesity and soda consumption were targeted with government-exclusive spyware.**
- **All of the targets have been active supporters of Mexico's soda tax, a public health measure to reduce the consumption of sugary drinks.**
- **The targets received messages with malicious links that would have installed NSO Group's Pegasus spyware on their phones. NSO Group is an Israeli "cyber warfare" company.**
- **NSO's government surveillance tool may have been misused on behalf of special commercial interests, not for fighting crime or terrorism.**

Summary

This report describes an espionage operation using government-exclusive spyware to target a Mexican government food scientists and two public health advocates. The operation used spyware made by the NSO Group, an Israeli company that sells intrusion tools to remotely compromise mobile phones. On August 25, 2016, the Citizen Lab published a report showing that NSO's technology was used to target Ahmed Mansoor, a UAE-based human rights defender, as well as identifying targeting in Mexico. Mexico has previously confirmed that it is a purchaser of NSO Group's spyware.

Mansoor was targeted with links sent via SMS. Had he clicked on the links, his iPhone would have been silently exploited with the *Trident*, a series of three zero-day exploits designed to install NSO's Pegasus spyware on his phone.

This research presents evidence that NSO's exploit infrastructure and spyware were used to target additional individuals in Mexico in July and August 2016, including Dr. Simon Barquera, a well-respected Mexican government health scientist, Alejandro Calvillo, the director of a consumer and health advocacy organization, and Luis Encarnación, the director of a coalition working on obesity prevention.

These individuals are neither criminals nor terrorists, but a prominent government scientist and two health campaigners who support a public health measure: Mexico's soda tax on sugary drinks. They received the malicious links via SMS while campaigning to increase the soda tax rate, improve drink labelling, and raise awareness of health risks associated with sugary drinks.

This case suggests that NSO's government-exclusive espionage tools may be being used by a government entity on behalf of commercial interests, and not for national security reasons or fighting crime.

Citizen Lab's investigation was conducted with the assistance of Mexican non-governmental organizations (NGOs) R3D and SocialTIC.

Mexican Soda Tax Supporters Targeted with NSO Exploit Links

Following publication of the August 2016 report, researchers with Citizen Lab and Amnesty International were contacted by Access Now, which had received a request for assistance on its helpline from R3D and SocialTIC, two Mexican NGOs working on digital rights and security. These NGOs assisted Citizen Lab researchers in collecting suspicious messages from a range of Mexican targets.

Image 1. Alejandro Calvillo, who was targeted with NSO, has strongly advocated for the soda tax as a means to combat obesity. Image by Cartoscuro.

Analysis of the text messages collected by R3D and SocialTIC revealed a campaign involving NSO exploit links active between at least April 20 and August 17, 2016.

This report describes a subset of these discoveries: SMS messages sent to three individuals—Dr. Simon Barquera, Alejandro Calvillo, and Luis Encarnación—in July and August 2016 (See: **Confirmed Targets of NSO Exploit Links**). We are naming these individuals with their explicit consent.

- Dr. Simon Barquera is a well-respected researcher at the Mexican Government's Instituto Nacional de Salud Pública (National Institute of Public Health).
- Alejandro Calvillo is the Director of El Poder del Consumidor, a consumer rights and health advocacy organization.
- Luis Encarnación is the Director of the Coalición ContraPESO, a coalition of more than 40 organizations that work on obesity prevention and reduction strategies. All three individuals work to support Mexico's soda tax.

Target	Description	Common Theme
 Dr. Simón Barquera	Researcher at Mexico's National Institute for Public Health, Fellow of the National Academy of Medicine, and the Mexican Academy of Science. [Bio]	Advocates for lowering consumption of sugary drinks and sodas
 Alejandro Calvillo	Director of El Poder del Consumidor (Power of the Consumer) NGO. Focusing on consumer rights, public health, the soda tax.	
 Luis Encarnación	Coordinator of the Coalición ContraPESO (CounterWEIGHT Coalition), a group of more than 40 organizations that work on obesity prevention and reduction strategies.	

Table 1. Confirmed Targets of NSO Exploit Links

Images adapted from from: emsavalles, eatforum, Fundacion Midete

Obesity is Political: Mexico's Soda Tax & Beyond

Facing an obesity epidemic, many Mexican organizations have campaigned to reduce the consumption of sugary drinks, especially sodas. The effort resulted in a tax on sugary drinks, passed in 2014. The tax slightly raises prices to encourage consumers—especially children—to seek healthier alternatives. The so-called "soda tax" has led to decreases in soda consumption and is projected to save over 18,000 lives from illnesses related to excess sugar consumption over 10 years.

Despite the positive effects on public health, efforts to promote healthier consumer habits have been met with resistance from the food and beverage industry. For example, the CEO of Coca Cola personally called Mexico's president in 2013 to encourage him to oppose the soda tax, and some Mexican media companies refused to air advertising supporting the tax. After the tax bill was passed, the pressure continued.

In October 2015, legislators attempted to cut the tax in half, although a swift public backlash and accusations of influence by soft drink companies forced cancellation

of the tax cut. Nevertheless, there is evidence that the industry continues to exert political pressure to block Mexico's efforts efforts to curb soda consumption.

Context of the Bitter Sweet Targeting Period

In response to the political pressure against the soda tax, in mid-2016 public health groups and food scientists prepared a mass media campaign to build support for the tax, increase the tax rate, and call for accountability in how the tax revenue was being spent. Campaigners held a press conference on June 29, 2016, highlighting misleading and confusing product labelling standards promoted by the food and beverage industry and planned a full launch of their campaign in August 2016. Campaigners began receiving the spyware links one week after the press conference, and throughout the period that the campaign was being prepared (See **Figure 1**).

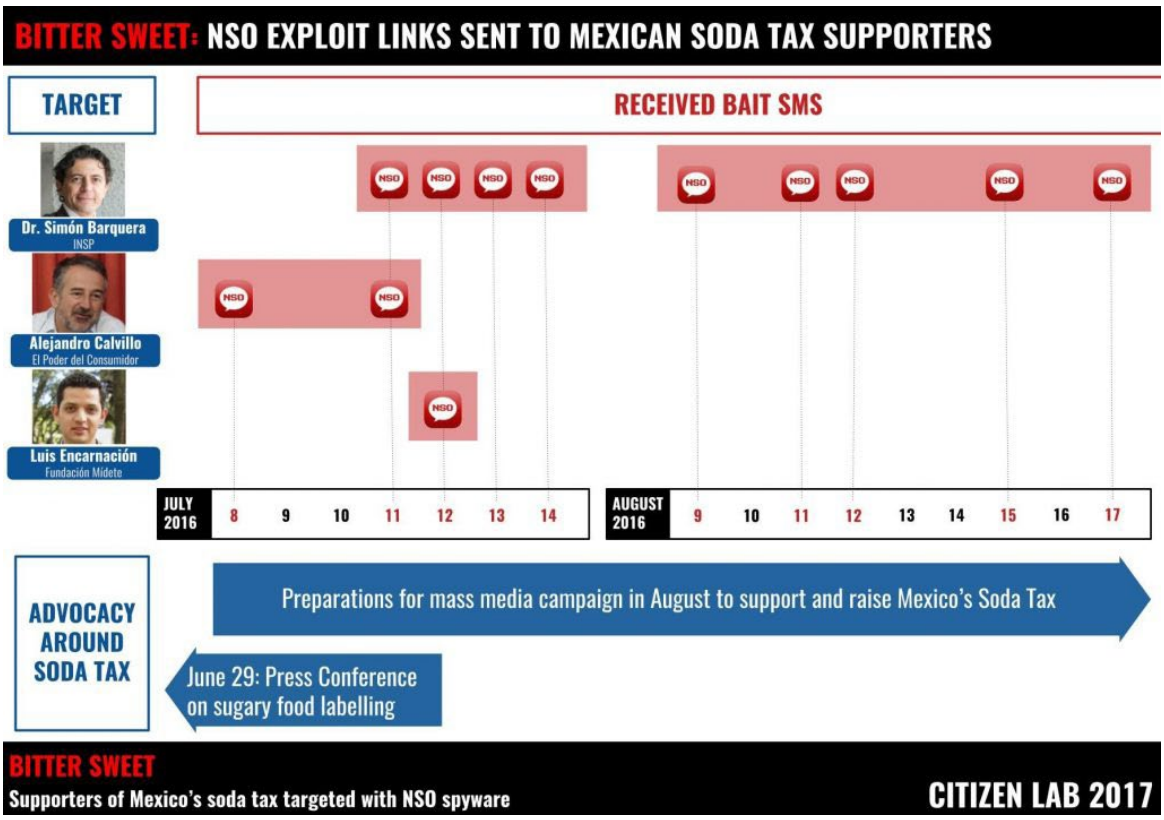

Figure 1. Dates in July 2016 when the three targets are known to have received malicious messages containing links to NSO's exploit framework. We may not have all of the messages sent to them.

Bitter Sweet Bait Texts: Personalized, Profane

Social engineering is a common strategy for delivering even very sophisticated spyware. Operators rely on social engineering because it "just works." Many instances of social engineering involve an operator sending a malicious attachment or link

in a message specially crafted to appeal to a target. Messages may be designed to appear urgent, important, upsetting, or intriguing to targets, to convince the target to open the link or attachment.

Spyware operators sometimes develop bait content that is both personalized and capable of stirring strong emotions. The Bitter Sweet NSO spyware operators personalized the messages to the interests and work of the targets (See **Figure 2**), and actively escalated the emotional content of the messages over time (See **Figure 3**).

Figure 2. SMS message sent to Dr. Simon Barquera, telling him that his daughter was in a serious car accident, and to click the link to learn about the hospital.

The messages used several deceptions to encourage targets to click on malicious links. For example:

- Upsetting fake news updates suggesting personal scandals
- Upsetting personal messages, like the news of the death of a relative, or injury of a child
- Personal sexual taunts and allegations

Bitter Sweet Escalation: From "I saw you mentioned" to "I f*cked your old lady" to "your daughter was in a car accident"

In several cases, a single target received several kinds of messages, ranging from mundane to highly emotional and upsetting.

For example, the targeting of Dr. Simón Barquera (that we know of) began with the operators sending him a message on July 11, 2016 with a fake news story relevant to his work. The Bitter Sweet operators subsequently escalated the personal content and aggressiveness of the messages in two waves, ending on August 17 (See **Figure 3**).

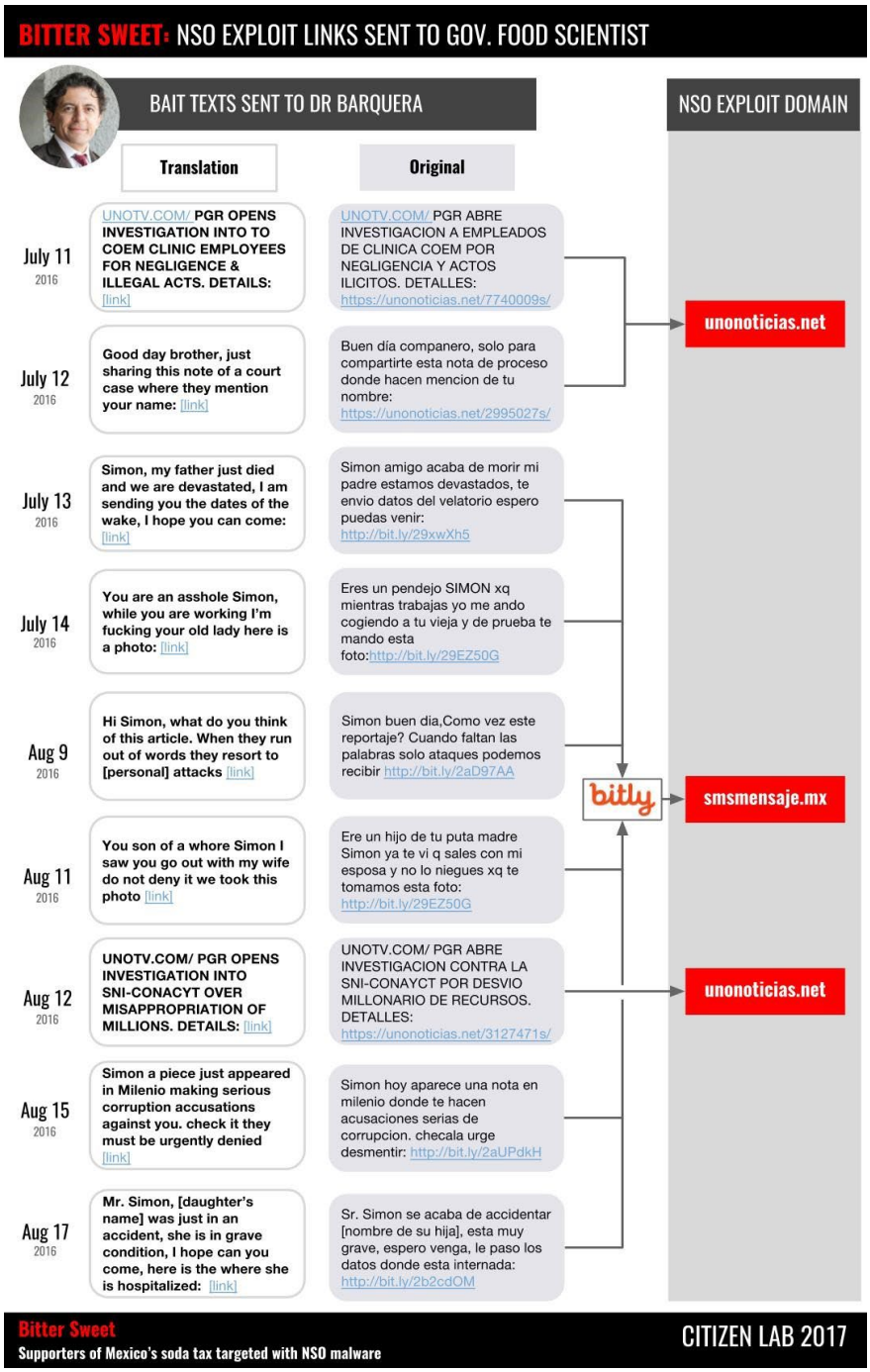

Figure 3. Beginning with a fake news story, the texts sent to Dr. Barquera escalated into the personal, and then the obscene. By July 14, the messages taunted that someone had slept with his wife, and by August the operators were trying to trick him into believing that his daughter was injured.

On July 12, Dr. Barquera received a message saying that he was mentioned in a court case. The following day, he received a more emotionally charged message: someone's father has died, the sender is devastated, and would Dr. Barquera check the dates of the funeral to see if he could attend?

On July 14, perhaps frustrated at a lack of success, the operators tried an even more upsetting theme: "While you are working I am fucking your old lady here is a photo."

On August 9 he got a message hinting that a news article contained personal attacks against him. Then, a message on August 11 accused him of sleeping with the sender's wife, continuing the theme. On August 12 a fake news update suggested that a place where he was affiliated was being investigated for corruption, and on August 15 he received an alarming message saying he was being accused of corruption in a national publication.

Finally, on August 17 he received an extremely upsetting message stating that his daughter had just been in an accident and was in "very serious condition." The message included a link with information about the place where she was purportedly hospitalized.

Why So Many Messages?

The repeated messages and escalation of emotional content suggest a strong desire on the part of the operators to compromise Dr. Barquera's device. The Bitter Sweet operators may have either failed to infect Dr. Barquera's devices with NSO's Pegasus or had trouble maintaining a stable infection on the target device (see: **Figure 3**).

The Other Targets

Alejandro Calvillo also received a message about a father's funeral on July 8 and a message on July 11 stating that his name was mentioned in a news article that was "going viral."

Luis Encarnación, meanwhile, received a message on July 12 suggesting that he was mentioned in a news article (See **Figure 1**). A full list of the texts and malicious links is included in Appendix A.

The Redirects

According to the targets, in several cases there were links that redirected to the website of a funeral home. These included messages about a funeral, but also bait messages that were on unrelated subjects. It is unclear whether this was a veiled threat, or a sloppiness by the operators. The more explicit taunts, meanwhile,

reportedly redirected to pornography websites. Citizen Lab was not able to examine these redirects, as NSO's entire exploit infrastructure was shut down around the time of our August 2016 report.

All three targets have taken steps to ensure the security of their devices following this incident.

Heavy Handed Targeting: Why such obvious lies?

Dr. Barquera could easily figure out that his daughter was not injured, just as Alejandro Calvillo could determine that there was no "viral" news article about him. This is telling about the style of the Bitter Sweet operators: they did not try very hard to avoid detection. They seem to have prioritized getting a target to click, rather than carefully concealing their targeting.

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.

Bitter Sweet's 'noisy' targeting also speaks to the issue of risk to other customers: if the NSO Group cannot stop its customers from recklessly using its tools, then it cannot guarantee other customers full secrecy. The NSO Group sells the same software and exploits to multiple government customers, and if one customer exposes their tools, all customers' are impacted. This scenario came to pass when a different NSO client targeted Ahmed Mansoor, triggering to our original investigation, which led to the patching of hundreds of millions of Apple devices, and exposed NSO's Pegasus software and Exploit infrastructure.

Connecting the Bitter Sweet SMSes to the NSO Exploit Infrastructure

The messages sent to Dr. Simon Barquera, Alejandro Calvillo, and Luis Encarnación all contained links pointing to domains previously identified as part of our investigation into NSO's infrastructure. The URLs in several text messages directly linked to the exploit infrastructure, while in others targets received exploit links that were shortened using the bit.ly link shortening service (See **Appendix A** for a full list, including all redirects).

NSO Group Trident Exploit & Spyware Domain	Target(s)
smsmensaje[.]mx	Dr. Simon Barquera, Alejandro Calvillo, and Luis Encarnación
unonoticias[.]net	Dr. Simon Barquera

Table 2. NSO Exploit Infrastructure Observed in This Operation

Based on the behavior of links received by human rights defender Ahmed Mansoor, clicking on the link would have caused the phone to be silently and remotely jailbroken, and infected with NSO's Pegasus spyware.

Our previous report mentioned a subset of the NSO exploit infrastructure domains that we discovered, including unonoticias[.]net. We also identified smsmensaje[.]mx as an NSO exploit infrastructure domain during the scanning period, although it was not listed in our report to protect ongoing investigations.

Bitter Sweet Attribution: The Mexican Nexus

While we do not conclusively demonstrate that elements of the Mexican government participated in the Bitter Sweet operation, circumstantial evidence suggests that this is a strong possibility.

Only a government can purchase NSO's products: NSO Group explicitly limits the sales of its products to governments. Therefore, we can reasonably conclude that a government's NSO deployment was used in this attack.

The Mexican Government is a confirmed NSO User: The Mexican government reported that it signed a $ 20 million dollar deal with NSO Group in 2012. Thus, elements of the Mexican government likely had access to NSO products at the time of the Bitter Sweet operation.

The targets work on multiple domestic Mexican issues: The same infrastructure used for the Bitter Sweet operation (the unonoticias[.]net domain) was also used to target a Mexican journalist who wrote a story about government corruption involving the Mexican President's wife and a high-speed rail contractor, among other domestic targeting.

The targets of the Bitter Sweet operation work on issues related to soft drink consumption and parties outside Mexico may object to their work. A large multinational food and beverage company could conceivably have sufficient influence to encourage *a different government* that has purchased NSO to target Dr. Simon Barquera, Alejandro Calvillo, and Luis Encarnación. However, it is not clear that another government would be equally interested in all of the other targets we have identified.

Noisy targeting: The heavy handed targeting is also a factor suggesting that the Bitter Sweet operator is a Mexican governmental client: it is unlikely that a foreign country would use the NSO tool on Mexican soil so brazenly and so clearly risking discovery.

Conclusion: Government-Exclusive Spyware's Many Misuses

The targets of the Bitter Sweet operation have not been accused by anyone of being criminals or terrorists. They are, instead, concerned scientists and public-health campaigners trying to limit the overconsumption of sugary drinks in Mexico. Yet, they have been targeted with a sophisticated piece of government-exclusive spyware.

Research by the Citizen Lab and others has consistently shown that some governments are willing to use "lawful intercept" tools like NSO Group's Pegasus to recklessly target and harass journalists, activists, and human rights defenders. Prior Citizen Lab reporting on NSO Group spyware highlighted, for example, the targeting of a Mexican journalist who reported on a presidential scandal (See: Section 7.1. Mexico: Politically Motivated Targeting?). Governments may view these people, however incorrectly, as threats to the state.

The advocacy work of Dr. Simon Barquera, Alejandro Calvillo, and Luis Encarnación cannot be construed as threats to the state. They have, however been critical of the influence of the soft drink industry in government, and supported measures that are projected to save over 18,000 lives from illness. These actions do threaten some interests: the revenues of companies selling sugary drinks, and the fortunes and reputations of their investors and allies in government.

This case suggests that NSO's surveillance tool may have been misused for special commercial interests, not for fighting crime or terrorism. We hope that this report and the evidence that it includes will result in an urgent investigation by the Mexican government, as well as the Israeli government, which approves exports of NSO products.

This case also highlights that the current regulatory environment has been unsuccessful at preventing egregious misuses of spyware. As spyware companies continue to sell to customers who abuse their products, they invite stronger regulation by concerned governments and multilateral bodies. Their lack of due diligence and the brazen abuses of their products by government clients are potent arguments in favor of more effective regulation.

Dealing With Suspicious SMS Messages

This campaign relied on upsetting, personalized messages combined with highly sophisticated government-exclusive spyware. Even though the spyware that was delivered was sophisticated, the path to infection started by exploiting human emotions. A target needs to click on the link for the infection to happen, which means the first line of defense is being vigilant and mindful of our own behaviours.

Here are several basic suggestions for avoiding SMS-based spyware:

- Do not click on SMS-links sent from people you do not know.
- Be especially careful with upsetting, unsolicited messages that contain links
- If you get an SMS from a service, like your phone company, visit their website rather than clicking on a link in the message.

If you believe you have been the victim of targeted spyware, you should consider sharing it with a trusted expert, or a helpline such as that of Access Now.

Citizen Lab strongly suspects that there may be other targets. If you suspect you have been the target of this particular operation, or have seen very similar text messages (same themes, same URLs, etc) please contact the Citizen Lab at **bittersweet@citizenlab.ca**.

The Importance of Documentation

The discovery that led to the findings in this report is the result of vigilance on the part of Dr. Simon Barquera, Alejandro Calvillo, and Luis Encarnación. It is also the result of a careful documentation effort by R3D and SocialTIC, and their willingness to share the case with Access Now's Help Line. Documentation of suspicious incidents is one of the most important practices civil society groups can adopt to raise awareness of and defenses against these kinds of espionage operations. Documentation can take the form of a simple set of notes with dates, times, and saved messages, or ideally be part of a more complete incident documentation process.

Appendix A

Messages containing NSO exploit infrastructure links sent to Dr Simon Barquera, Alejandro Calvillo, and Luis Encarnación

2016 Date	Target	Original	NSO EXPLOIT FRAMEWORK LINK
July 8	Alejandro Calvillo	Alejandro perdon pero acaba de fallecer mi padre, estamos mal, t envio los datos del velatorio, espero asistas: [malicious link]	**hxxp://bit[.]ly/29xpUI0** *resolves to:* **hxxps://smsmensaje[.]mx/9158534s/**
July 11	Dr. Simón Barquera	PGR ABRE INVESTIGACION A EMPLEADOS DE CLINICA COEM POR NEGLIGENCIA Y ACTOS ILICITOS. DETALLES [malicious link]	**hxxps://unonoticias[.]net/7740009s/**
July 11	Alejandro Calvillo	Alejandro buen dia, te envio esta nota de proceso donde hacen mencion de tu nombre, se esta viralizando mira: [malicious link]	**hxxp://bit[.]ly/29COxD2** *resolves to:* **hxxps://smsmensaje[.]mx/5062299s/**
July 12	Dr. Simón Barquera	Buen dia companero, solo para compartirte esta nota de proceso donde hacen mencion de tu nombre [malicious link]	**hxxps://unonoticias[.]net/2995027s/**
July 12	Luis Encarnación	Luis buen dia, te envio esta nota de proceso donde hacen mencion de tu nombre, se esta viralizando mira: [malicious link]	**hxxps://bitly[.]com/29xc0lp** *resolves to:* **hxxps://smsmensaje[.]mx/8744937s/**

2016 Date	Target	Original	NSO EXPLOIT FRAMEWORK LINK
July 13	Dr. Simón Barquera	Simon amigo acaba de morir mi padre estamos devastados, te envio datos del velatorio, espero puedas venir [malicious link]	**hxxp://bit[.]ly/29xwXh5** *resolves to:* **hxxps://smsmensaje[.]mx/4168377s/**
July 14	Dr. Simón Barquera	eres un pendejo SIMON xq mientras trabajas yo me ando cogiendo a tu vieja y de prueba te mando esta foto [malicious link]	**hxxp://bit[.]ly/29EZ50G** *resolves to:* **hxxps://smsmensaje[.]mx/1208803s**/
Aug 9	Dr. Simón Barquera	Simon buen dia,Como vez este reportaje? Cuando faltan las palabras solo ataques podemos recibir:[malicious link]	**hxxp://bitly[.]com/2aD97AA** *resolves to:* **https://smsmensaje[.]mx/6459115s**/
Aug 11	Dr. Simón Barquera	Ere un hijo de tu puta madre Simon ya te vi q sales con mi esposa y no lo niegues xq te tomamos esta foto: [malicious link]	**hxxps://bitly[.]com/29EZ50G** to: **hxxps://smsmensaje[.]mx/1208803s/**
Aug 12	Dr. Simón Barquera	UNOTV.COM/ PGR ABRE INVESTIGACION CONTRA LA SNI-CONAYCT POR DESVIO MILLONARIO DE RECURSOS. DETALLES:	**hxxps://unonoticias[.]net/3127471s/**
Aug 15	Dr. Simón Barquera	Simon hoy aparece una nota en milenio donde te hacen acusaciones serias de corrupcion. checala urge desmentir [malicious link]	**hxxps://bitly[.]com/29EZ50G** *to:* **hxxps://smsmensaje[.]mx/8492980s/**
Aug 17	Dr. Simón Barquera	Sr. Simon se acaba de accidentar Aby, esta muy grave, espero venga, le paso los datos donde esta internada [malicious link]	**http://bit.[.]ly/2b2cdOM** *to:* **https://smsmensaje[.]mx/6349847s/**