RECKLESS EXPLOIT

Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware

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

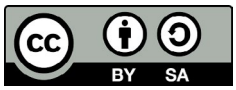
JUNE 19, 2017
RESEARCH REPORT #93

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 Exploit: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware," Citizen Lab Research Report No. 93, University of Toronto, June 2017.

Acknowledgements

We thank the targets of these infection attempts who accepted to share their cases with the collaborating organizations, and with the public.

Citizen lab would like to thank the collaborating organizations including R3D, SocialTic and Article19, for their careful and important investigative work. Without their assistance, this report would not have been possible

We would like to especially thank and highlight the contribution of Luis Fernando García of R3D for his support of our investigation.

We thank Access Now, especially their Help Line team, and Amnesty International for assistance compiling evidence, and ensuring that the initial NSO case in Mexico came to our attention. With special thanks to Claudio Guarnieri, Senior Technologist at Amnesty International, and Co-Founder of Security Without Borders.

Thanks to the whole Citizen lab team, especially: Amitpal Singh, Irene Poetranto, Adam Senft, Adam Hulcoop.

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

Key Findings 6

Summary 7

Background 9

- NSO's Spyware 9
  - NSO's Claims of Due Diligence & Lawful Use 10
- Journalism Under Threat in Mexico 11
- The Investigation 12

Part 1: The Targets 12

- Targeted Journalists 13
  - Targets: Aristegui Noticias 13
  - Special Note: Targeting Mother and Child 14
  - Target: Carlos Loret de Mola 15
  - Targets: Mexicanos Contra la Corrupción y la Impunidad (MCCI) 17
- Civil Society Groups 17
  - Targeted Org: Centro Miguel Agustín Pro Juárez 18
  - Targeted Org: Mexican institute for Competitiveness 18

Part 2: Reckless Infection Attempts 19

- Infection Attempts Against A Minor in the United States 19
- Impersonating the United States Embassy in Mexico 20
- Fake Amber Alerts 20
- Messages related to personal safety 21
- Upsetting Personal Messages 22
- Urgent Work-related messages 22
- Financial Concerns 23

Part 3: Connecting the SMSes to NSO Exploit Infrastructure 23

Part 4: Discussion 25

- Digital Targeting Mirrors Physical Risks to Journalists 25
- Reckless Targeting 25
- Lack of Oversight and Accountability 26

Conclusion: The "Principle of Misuse" 27

Appendix A: Full Message List 29

This report is Part 2 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

Update (Monday June 19 2017): According to a recent report, NSO Group may be re-branding itself as "Q Cyber Technologies"or "Q."

Key Findings

- **Over 76 messages with links to NSO Group's exploit framework were sent to Mexican journalists, lawyers, and a minor child (NSO Group is a self-described "cyber warfare" company that sells government-exclusive spyware).**
- **The targets were working on a range of issues that include investigations of corruption by the Mexican President, and the participation of Mexico's Federal authorities in human rights abuses.**
- **Some of the messages impersonated the Embassy of the United States of America to Mexico, others masqueraded as emergency AMBER Alerts about abducted children.**
- **At least one target, the minor child of a target, was sent infection attempts, including a communication impersonating the United States Government, while physically located in the United States.**

Summary

In the past five years it has become increasingly clear that civil society is under threat from the misuse of powerful spyware tools exclusively sold to governments. Research has repeatedly shown how governments around the world use digital spying tools designed for criminal investigations and counterintelligence to target journalists, human rights defenders, and others.

In August 2016, Citizen Lab released a report uncovering how United Arab Emirates (UAE) activist Ahmed Mansoor was targeted with "Pegasus" (sophisticated government-exclusive spyware) and "The Trident" (a chain of iOS zero day exploits) designed to infect his iPhone 6 via a malicious link in an SMS text message. We attributed Pegasus and The Trident exploit chain to an Israel-based "cyber warfare" company, NSO Group.

In February 2017 Citizen Lab, with assistance of Mexican non-governmental organizations (NGOs) R3D and SocialTic, documented how Mexican government food scientists, health, and consumer advocates also received links to infrastructure that we connected to NSO Group. We suspect that the links were designed to install Pegasus on their phones.

Figure 1: Selected Mexican NSO Targets in media, human rights and anti corruption advocacy, and public health.

This report expands the Mexican investigation and shows how 10 Mexican journalists and human rights defenders, one minor child, and one United States citizen, were targeted with NSO's Exploit Framework. Our investigation was conducted with the collaboration and assistance of R3D, SocialTic and Article 19. With their assistance, we have confirmed over 76 additional messages containing NSO exploit links. They are co-publishing an extensive investigation (in Spanish).

The targets share a basic connection: they have been involved in investigating or working on reports of high-level official corruption, or government involvement in

human rights abuses. The infection attempts often coincided with work on specific high-profile investigations and sensitive issues between January 2015 and August 2016, at which time our previous report likely led to the shutdown of the operations.

The targets received SMS messages that included links to NSO exploits paired with troubling personal and sexual taunts, messages impersonating official communications by the Embassy of the United States in Mexico, fake AMBER Alerts, warnings of kidnappings, and other threats. The operation also included more mundane tactics, such as messages sending fake bills for phone services and sex-lines. Some targets only received a handful of texts, while others were barraged with dozens of messages over more than one and a half years. A majority of the infection attempts, however, took place during two periods: August 2015 and April-July 2016 (See: Figure 2).

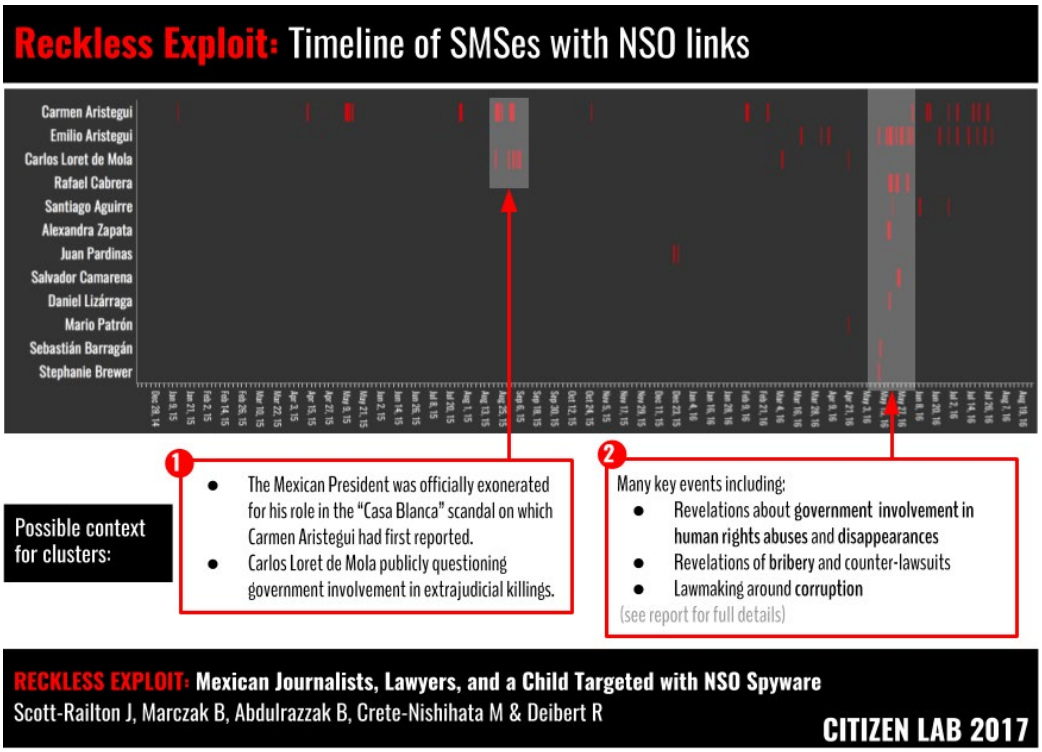


Figure 2: Timeline of receipt of SMSes with NSO Exploit Links

The timeline shows at least two periods of intense targeting that our collaborators have connected to key events in Mexican politics.

- **Period 1 (August 2015)** During this period the Mexican President was officially exonerated for his role in the "Casa Blanca" scandal on which Carmen Aristegui had first reported, and Carlos Loret de Mola was questioning the government's role in extrajudicial killings.

- **Period 2 (April- July 2016):** A range of key events concerning revelations of government involvement in human rights abuses and extra-judicial killings, and questions around official accounts happened during this time frame. Revelations of bribery and counter-lawsuits, and lawmaking around corruption and government accountability also occurred around this period.

Even more disturbing, we have determined that the minor child of at least one target was also sent upsetting messages with NSO exploit links, presumably in attempt to spy on the child's mother. In addition, at least one target was located within the United States during some of infection attempts.

The NSO Group, which is reportedly being offered for sale at a price of one billion dollars, claims that its products are restricted "to authorized government agencies." We have no conclusive evidence attributing these messages to specific government agencies in Mexico. However, circumstantial evidence suggests that one or more governmental of NSO's government customers in Mexico are the likely operators.

- The infrastructure and SMS content is exclusively Mexico specific
- Targets work on domestic issues of immediate concern to powerful Mexican interests, and the governmen
- Multiple government agencies in Mexico are reportedly NSO customers

Regardless of the specific client, however, the cases we outline here provide evidence that clearly shows the lack of oversight and the misuse potential of NSO Group's products, and of "government-exclusive" spyware more generally.

Background

This section provides background on the NSO Group and its spyware suite, threats faced by journalists in Mexico, and our investigation.

NSO's Spyware

The NSO Group is an Israel-based company that sells remote intrusion solutions to governments. NSO markets their product, known as Pegasus, as a fully featured tool to remotely compromise and then monitor mobile phones of all popular operating systems.

To remotely compromise phones, NSO's government customers trick targets to click on a link. When the link is clicked, the phone visits a server that checks the handset model (iPhone, Android, etc) and then sends the phone a remote exploit for its operating system. These servers are part of what we call NSO's Exploit Framework.

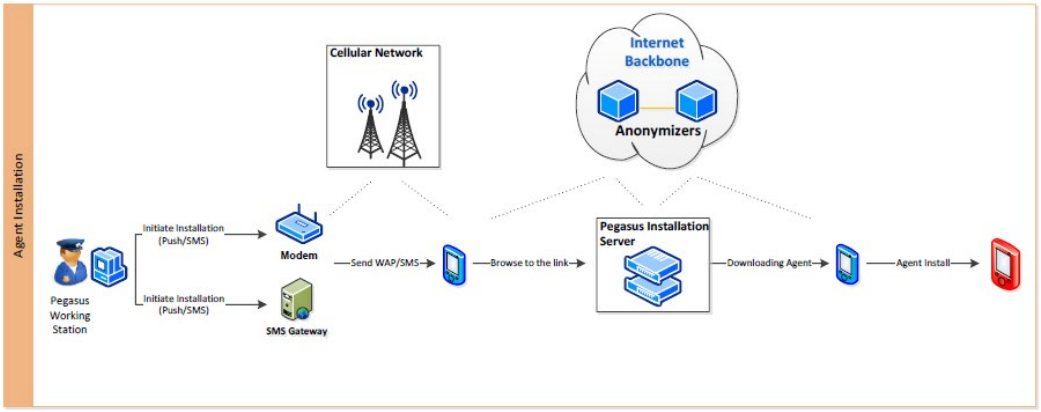


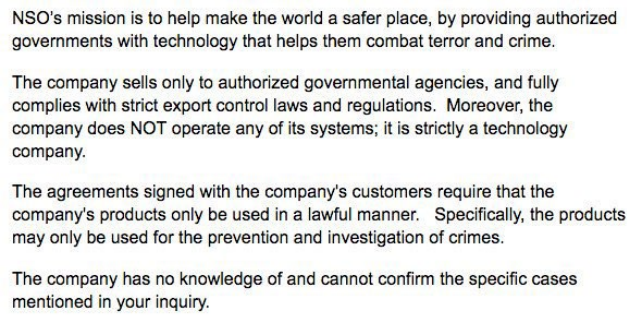
Figure 3: NSO's Exploit Framework [Source: Hacking Team E-mails]

In 2016, when human rights defender Ahmed Mansoor was sent messages with links to NSO's Exploit Framework he provided the messages to Citizen Lab. When we clicked on the messages in a controlled environment, we observed a chain of three zero day exploits used to remotely jailbreak and infect the phone with NSO's Pegasus spyware. In 2017, Lookout and Google released details on an Android version of Pegasus.

Once infected, a phone becomes a digital spy in the pocket of a victim, fully under the control of the operator. An infected phone can be configured to report back all activities on the device, from messages and calls (even those via end-to-end-encrypted messaging apps), to recording audio and taking pictures.

NSO's Claims of Due Diligence & Lawful Use

In response to prior Citizen Lab reporting, NSO has claimed that "their mission is to help make the world a safer place, by providing authorized governments with technology that helps them combat terror and crime." The company claimed that it "fully complies with strict export control laws and regulations." Implying that they have limited ability to see exactly how their product is used, NSO Group stated that "the company does NOT operate any of its systems." Furthermore, NSO Group claims that its "products may only be used for the prevention and investigation of crimes."


NSO's mission is to help make the world a safer place, by providing authorized governments with technology that helps them combat terror and crime.

The company sells only to authorized governmental agencies, and fully complies with strict export control laws and regulations. Moreover, the company does NOT operate any of its systems; it is strictly a technology company.

The agreements signed with the company's customers require that the company's products only be used in a lawful manner. Specifically, the products may only be used for the prevention and investigation of crimes.

The company has no knowledge of and cannot confirm the specific cases mentioned in your inquiry.

Figure 4: NSO Group's Claims of Oversight [Source]

Despite these claims, Citizen Lab has repeatedly uncovered abuses of NSO's spyware, demonstrating a failure to control the end-uses of their products. The misuse of NSO's products is part of a larger problem, abuse of government-exclusive spyware to target individuals and organizations who are neither criminal, nor terrorists, but members of civil society. In our previous investigation of NSO use in Mexico we found targeting of civil society even included scientists. It is also worth noting that for many authoritarian or otherwise democratically-challenged governments, what constitutes a "crime" can be very broad, and include any activity that challenges powerful elites. The infection attempts against investigative journalists and civil society members in Mexico that we outline here is a case in point.

Journalism Under Threat in Mexico

Mexico is one of the most dangerous places in the world for journalists. Reporters covering sensitive issues often face threats of kidnapping, intimidation, or physical violence as a result of their work. Mexican organized criminal groups are responsible for much of this violence. However, according to a recent report from human rights group Article 19, at least 53% of the 426 acts of violence and intimidation against journalists in 2016 were linked to officials. The report also found that virtually none of these actions resulted in legal consequences for the aggressor. In spite of these risks, reporters and editors continue to report on important issues, including corruption at the highest levels of the country. Reporters working on these topics often face threats in an attempt to intimidate them into silence.

Many Mexican journalists have stated their belief that their communications are monitored by elements within the Mexican government and security services. Prior Citizen Lab research on NSO group also included an example of a targeted Mexican journalist (Rafael Cabrera). In another case indicating surreptitious monitoring, a recording of a private phone call between Santiago Aguirre and the parent of one

of the victims of the Iguala Mass Disappearance appeared online. Aguirre is one of the targets of infection attempts using NSO exploit links that we examine here.

While these cases provide indications that Mexican journalists are under digital surveillance, their clandestine nature can make them hard to document. This report, and corresponding reporting by R3D, Social Tic, and Article 19, provide the clearest evidence yet that government-exclusive spyware is being used in an effort to infect and monitor Mexican journalists.

The Investigation

We worked closely with Mexican NGOs R3D, SocialTic, and Article 19 to collect a large number of suspect text messages sent to journalists and members of civil society. We then compared the ultimate destination of the links with known NSO exploit servers. At the time of writing, we have collected over 76 confirmed (and previously unreported) messages sent to 11 targets. All of the targets described in this report have consented to be named. However, the text content of several messages have been redacted because of the personal or confidential information they contain.

This report includes four parts:

- **Part 1: The Targets** Describes 11 individuals targeted over a period of more than one and a half years with SMS messages containing links to NSO's Exploit Framework.
- **Part 2: Reckless Infection Attempts** Details the reckless characteristics of the infection attempts against journalists and other targets.
- **Part 3: Connecting the SMSes to NSO Exploit Infrastructure** Analyzes the connection between the SMS messages sent to the targets and server infrastructure used to operate NSO exploits.
- **Part 4: Discussion** Discusses the implications of such a reckless approach to infection attempts, and the apparent lack of oversight in the Mexican case.

Part 1: The Targets

Six Mexican journalists and television personalities received text messages with NSO links. The minor child of one journalist was also targeted. Five members of

Mexican nongovernmental organizations also received such messages. The targets range across Mexico's political spectrum, and paint a picture of an effort to track key figures in Mexican media.

The targeting described in this report took place between January 2015 and August 2016. In the following sections, we detail the targeting of journalists and civil society groups.

Targeted Journalists

Television personality and investigative journalist Carmen Aristegui, along with her son Emilio Aristegui (a minor), were the most heavily targeted individuals we identified. Other media targets include several journalists working with *Aristegui Noticias* (a well known Mexican news organization that emphasizes independent, investigative journalism), including Rafael Cabrera and Sebastián Barragán. From a more mainstream media direction, *Televisa* anchor Carlos Loret de Mola, was also extensively targeted. In addition, Salvador Camarena and Daniel Lizárraga, both journalists specializing in investigating corruption with Mexicanos Contra la Corrupción y la Impunidad (MCCI: Mexicans Against Corruption and Impunity), were also targeted with infection attempts. Both Camarena and Lizárraga had previously collaborated with *Aristegui Noticias*.

Targets: Aristegui Noticias

In the past several years, *Aristegui Noticias* has been heavily involved in major investigations. In the original Citizen Lab report on NSO Group, we presented evidence that journalist Rafael Cabrera (a reporter with *Aristegui Noticias*, and now *BuzzFeed*) was targeted with NSO exploit links. We now know that his colleagues Sebastián Barragán and Carmen Aristegui were also among the targets.

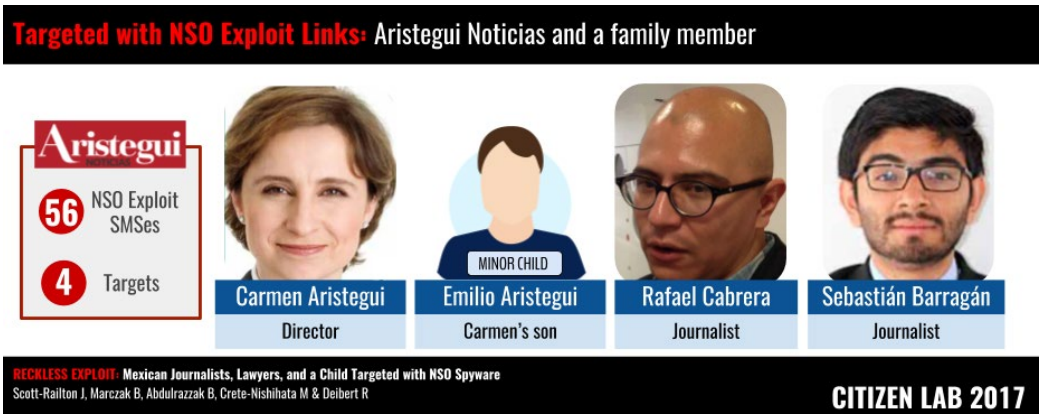


Figure 5: Aristegui Noticias Journalists and a minor child targeted with NSO exploit links. Note: Rafael Cabrera now works with BuzzFeed.

Aristegui Noticias has conducted several investigations of corrupt practices among Mexican officials. However, the timeline of targeting with NSO links corresponds to their work on the so-called "Casa Blanca scandal".

The scandal, which was first reported on by *Aristegui Noticias*, concerns a luxurious house provided to the Mexican President Peña Nieto's wife, but paid for by the subsidiary of a Mexican company (Groupo Higa, which is led by a friend of the President, and linked to a consortium of Chinese investors). Groupo Higa was given a series of highly lucrative contracts during the period when Peña was governor of the State of Mexico. After the scandal broke, the Mexican Federal government made the unusual step of rescinding the contracts.

While three individuals working with *Aristegui Noticias* were targeted during the period, Carmen Aristegui (see above) and her son were the most heavily targeted with infection attempts.

The messages targeting *Aristegui Noticias* reporters were exceptionally varied, and covered all of the themes highlighted in **Section 3**.

Special Note: Targeting Mother and Child

On January 12 2015, Carmen Aristegui received a text message saying that the "previous message was not sent" along with a link that led to NSO Group's Exploit Framework. Over the next year and a half, Aristegui received a further 25 messages that included NSO links purporting to come from: the US Embassy in Mexico, Amber Alerts, colleagues, people in her personal life, her bank, phone company, and notifications of kidnappings.

Emilio Aristegui, Aristegui's son, who was a minor when the messages were sent, was also intensively targeted. Emilio was located within the United States when he was targeted with many of these infection attempts.

We confirmed that over 21 messages with NSO exploit links were sent Emilio Aristegui. A further set were not confirmed as we were unable to view the original links, but are highly suspect as they used language found in other targeting, or came from the same phone number as NSO exploit link messages. Some of these infection attempts contained crude sexual taunts, others impersonated the United States' Embassy, or his mother's reporting and activities.

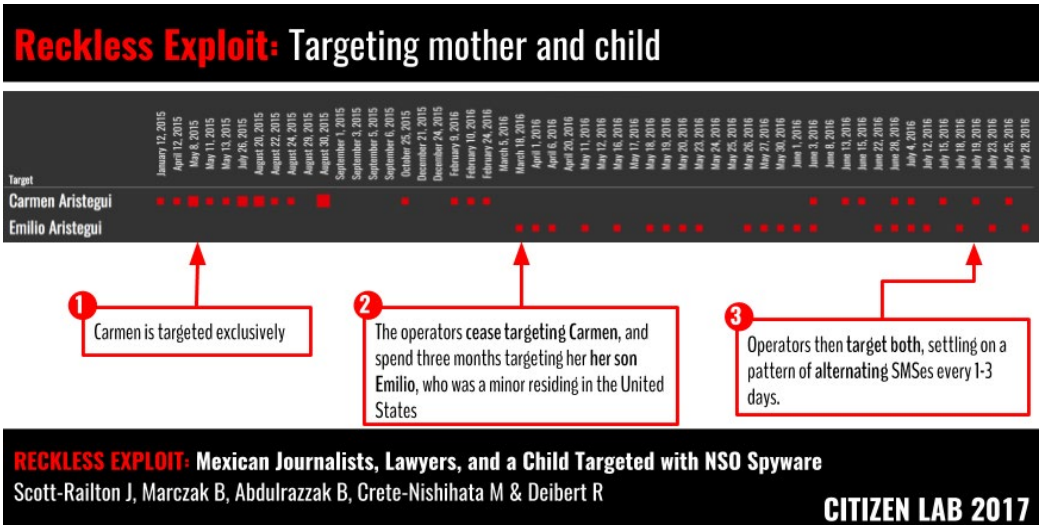


Figure 6: Targeting of Carmen Aristegui and her son Emilio

After heavily targeting Carmen Aristegui for more than a year, in March 2016 the operators appear to cease targeting her and instead focus their efforts on her son, Emilio (See: Figure 6). The infection attempts then focus on Emilio Aristegui for approximately three months, before returning to target both mother and son in June 2016. In July 2016, the operators alternate between targets every one to three days (see Figure 6).

We speculate that this "off center" targeting was an attempt to indirectly monitor Emilio Aristegui's mother Carmen. **This is the first example of which we are aware of a minor being targeted with infection attempts using governmental spyware.** Moreover, as we discuss below, sending Emilio Aristegui a message impersonating a United States Government communication while he was located in the United States may have violated US Law.

Target: Carlos Loret de Mola

Carlos Loret de Mola is a well known journalist and on-air personality for the Mexican national television channel *Televisa*. The NSO messages first arrived in August 2015 during a period when he was covering a massacre that took place on May 22, 2015 at a farm known as "Rancho El Sol" in western Mexico. Loret was reporting on the possible involvement and subsequent cover up of elements of the Mexican Federal government in the disappearance of 42 persons that took place at Rancho El Sol.

On August 8, 2015, Loret published an article in which he claimed new evidence from the Mexican Federal Public Prosecutor's Office contradicted official claims at the time of the massacre, and showed Mexican security forces had actually committed extrajudicial killings. Many of the victims were killed with point-blank gunshot wounds to the back of their heads.

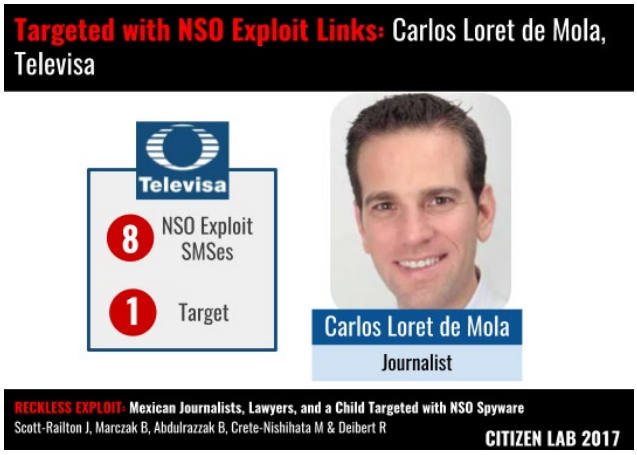


Figure 7: Televisa Journalist Carlos Loret de Mola targeted with NSO exploit links

On August 20, 2015, Loret received the following SMS message purporting to be from the US Embassy involving issues with his visa application.

USEMBASSY.GOV/ DETECTAMOS UN PROBLEMA CON TU VISA POR FAVOR ACUDE PRONTAMENTE A LA EMBAJADA. VER DETALLES: [exploit link]	USEMBASSY.GOV/ WE DETECTED A PROBLEM WITH YOUR VISA PLEASE GO PROMPTLY TO THE EMBASSY. SEE DETAILS [exploit link]

On August 29, 2016, Loret then received another SMS message, this time claiming that he was being watched by people in a suspicious van. The SMS included a link to what was purported to be pictures of the van:

estas personas vinieron preguntando por usted vienen en camioneta sin placas tome foto los conoce? mire [exploit link]	these people came asking for you they come in a van without license plates i took a picture do you know them? look:[exploit link]

From September 1 to September 6, 2015 Loret then received a further four messages with topics ranging from AMBER Alerts, service charges, to pictures of alleged rumours being spread of Loret. On March 5, 2016, Loret then received another SMS message with links to NSO infrastructure, this time with a message about the supposed death of a friend's father and the funeral details:

Loret hoy fallecio mi padre estamos devastados envio datos del velatorio espero contar contigo mau[exploit link]	Loret my father died today and we are devastated I am sending you the dates for the wake I hope I can count on you mau [exploit link]

As we detailed in our prior research, similar text messages with details of a supposed "father's death" with links to NSO infrastructure were received on July 8, 2016 by Mexican health advocate Alejandro Calvillo, and on July 13, 2016 by the Mexican health scientist Dr. Simon Barquera.

Finally, on April 20, 2016, Loret received another SMS message with links purporting to show inappropriate behavior:

Querido Loret, fijate que tvnotas tiene fotos tuyas donde estas con una chava cenando. Dales una checada:[exploit link]	Dear Loret, look that tvnotas has photos of you in which you are dining with a chick. Look at them:[exploit link]

Targets: Mexicanos Contra la Corrupción y la Impunidad (MCCI)

Shortly after Mexicanos Contra la Corrupción y la Impunidad (MCCI: Mexicans against Corruption and Impunity) was founded, Salvador Camarena and Daniel Lizárraga received text messages containing links to NSO's Exploit Framework.

Figure 8: *Mexicanos Contra la Corrupción y la Impunidad* Journalists targeted with NSO exploit links.

During the period of the targeting, Camarena and Lizárraga were working on topics that included the Panama Papers, and investigating evidence of offshore holdings linked to corrupt officials and prominent individuals in Mexico.

Civil Society Groups

Staff and directors of two Mexican civil society organizations were also targeted using NSO exploit links: Centro Miguel Agustín Pro Juárez (Centro PRODH) and the Mexican institute for Competitiveness (IMCO).

Targeted Org: Centro Miguel Agustín Pro Juárez

Centro PRODH is a Mexican human rights and legal aid organization. At the time of targeting with NSO exploit links they were representing the families of the 43 students disappeared in the Iguala Forced Disappearance case. The attempts at infection took place shortly before the public announcement of an investigation that cast doubt on an official account of the events.

Figure 9: *Centro PRODH* Director and staff targeted with NSO exploit links

Targets at Centro PRODH included their Director Mario Patrón as well as Stephanie Brewer and Santiago Aguirre. Patrón and Aguirre are Mexican citizens, Brewer is a United States citizen.

There is public evidence suggesting the monitoring of Centro PRODH communications, and these individuals in particular. Audio from a purported phone call between Santiago Aguirre and the parent of one of the victims of the Iguala Forced Disappearance was released in Mexican media as a video. The same video included audio of another lawyer working with the families, and seemed intended to impugn the character of the lawyer.

Targeted Org: Mexican institute for Competitiveness

The Mexican Institute for Competitiveness is a Mexican NGO that works on supporting economic competitiveness. Legislative and policy engagement and activism around anti-corruption form a core part of their work.

From December 21 2015 to May 18 2016, IMCO staff Juan Pardinas and Alexandra Zapata received four messages containing NSO links.

Figure 10: IMCO Director and an investigator targeted with NSO exploit links

Message themes included fake news updates of stories about corruption within IMCO, messages referring to other IMCO staff, a warning of armed men outside a house, and a message about a fictitious death.

Part 2: Reckless Infection Attempts

The journalists and human rights defenders targeted for infection with NSO links were sent a wide variety of messages designed to trick them into clicking, and being infected. Some of the tactics used by the operators are common, such as using alarming false notifications, offers of enticing information, and other personal content. What sets this targeting apart is the reckless and brazen nature of some of the lures, such as impersonating the United States Embassy. The targeting also used sexual themes and taunts, which we also highlighted in previous reporting on Mexican government food scientists, health, and consumer advocates targeted with NSO spyware.

Infection Attempts Against A Minor in the United States

Emilio Aristegui was a minor at the time that many of the messages were sent and received. He was also residing in the United States. On June 3rd, 2016, Emilio received a message purporting to come from the US Embassy in Mexico, concerning the status of his visa (See: Figure 11). The message was sent from a Mexican number to a phone located in the US. While his mother Carmen Aristegui, and Carlos Mola also received similar messages in 2015, the fact that the message, among others, was sent to someone in the US may have violated US law (See Section 4: Reckless Targeting).

Impersonating the United States Embassy in Mexico

On August 20, 2015, journalists Carlos Loret de Mola and Carmen Aristegui separately received alarming messages from the US Embassy in Mexico. The messages claimed that there were problems with their United States visas, and advised them to go to the US Embassy immediately.

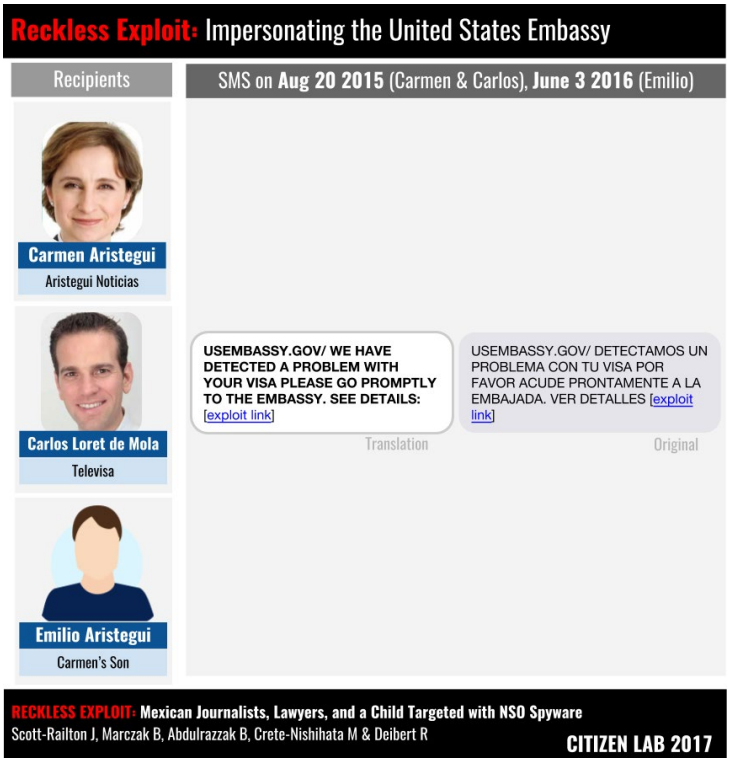


Figure 11: Messages impersonating the United States Embassy in Mexico

The messages were fakes, and contained links to the NSO Group's Exploit Framework. Impersonating official communications from the United States Embassy is an alarming precedent, and suggests that the NSO customer had little concern for the possibility of violating diplomatic norms, such as not impersonating foreign consular activities.

Fake Amber Alerts

On August 24, 2015 journalist Carmen Aristegui received a message purporting to be an AMBER Alert (an emergency broadcast) about the kidnapping of a nine year old boy. On September 29, 2015 another journalist, Carlos Loret de Mola, also received a fake Amber Alert, this time referring to a missing university student. By impersonating Amber Alert, the operators of the NSO deployment run the risk of sowing suspicion around real alerts, with potential consequences for actual kidnapped children.

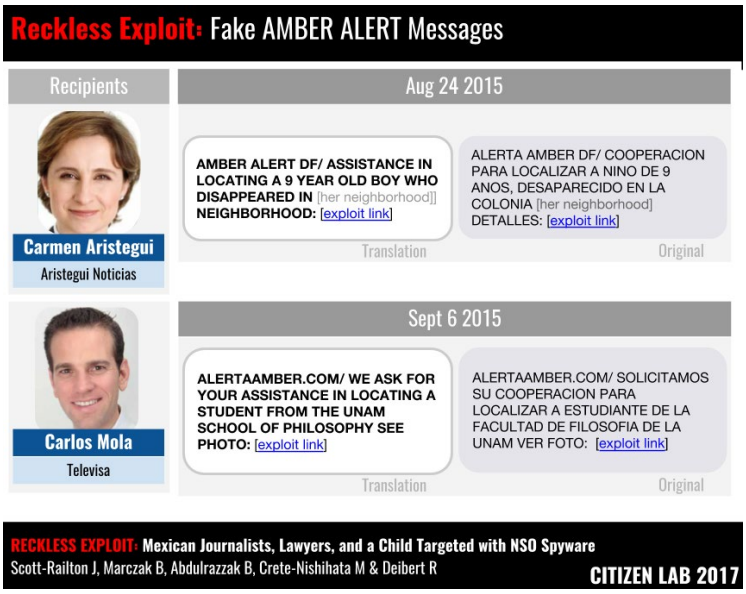


Figure 12: Fake Amber Alerts with NSO exploit links

Messages related to personal safety

Several journalist received messages purportedly warning them about threats to their personal safety. On August 29, 2015, journalist Carlos Loret de Mola received a message claiming that a group of people had come looking for him in a van with a purported link to a picture of the van. Human rights defender Juan Pardinas received a message on December 24, 2015 warning him that two armed men were waiting for him in a van at his house. On May 25, 2016 Salvador Camarena received a similar message, referring to a group of people conducting surveillance of his house. These messages appear to play on concerns for personal safety and the physical threats that journalists face in Mexico.

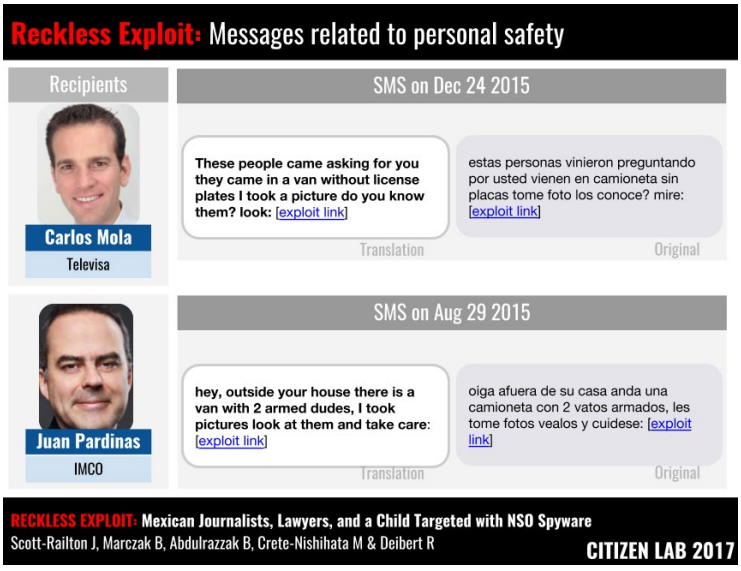


Figure 13: Upsetting messages about personal safety

Upsetting Personal Messages

The operators use a variety personal and upsetting themes in their messages. Many of the messages were sexual in tone, suggesting a preference for the theme on the part of the NSO customer. Themes of the messages included:

- Crude sexual taunts and accusations
- Promises of nude pictures of a partner or spouse
- Fake stories about leaks of affairs and leaked sexual videos
- Death or loss of family members, strangers

These messages are clearly attempts to play on the emotions of the target intensified by reference to family members and partners. For example, journalists Rafael Cabrera & Salvador Camarena each separately received an identical message on the exact same day purporting to show someone having sex with their spouses.

Figure 14: Upsetting sexual taunts

Urgent Work-related messages

Messages included urgent notifications of workplace issues including:

- Notifications of kidnappings of colleagues
- Breaking news about major issues
- Notifications of website errors
- Notifications of defamation lawsuits

Not all of the work related messages were so urgent. On June 8 and 28, 2016, human rights defender Santiago Aguirre received messages asking him to comment on the thesis of a student that was supposedly was based on Aguirre's own dissertation. Aguirre is also an instructor, and it would not be uncommon to receive such messages.

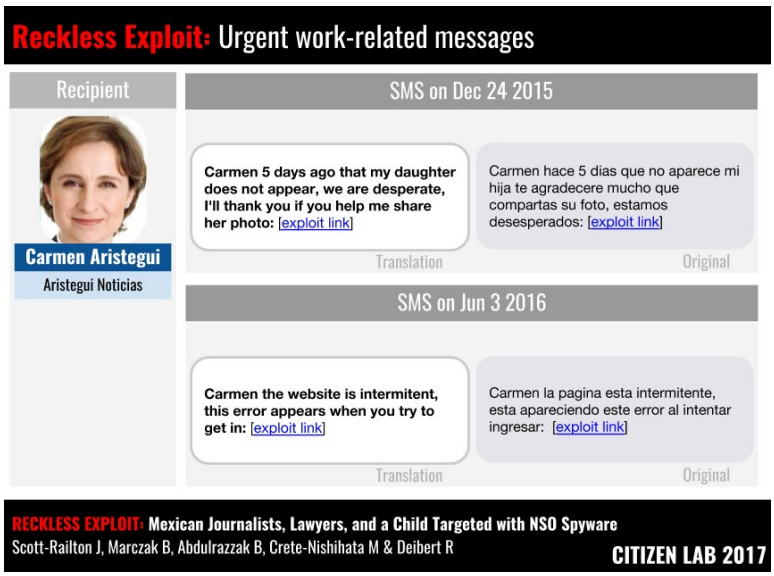


Figure 15: Urgent work-related messages sent to Carmen Aristegui

Financial Concerns

The operators made frequent use of fake bills and other concerns to get the attention of their target including:

- A fake phone bill
- Fake credit card purchase notifications
- Fake phone sex billing notifications

These messages reflect more conventional social engineering approaches.

Part 3: Connecting the SMSes to NSO Exploit Infrastructure

In our prior investigation of NSO targeting against Ahmed Mansoor, we scanned the Internet looking for NSO Group's exploit domain names. The targets discussed in this report were sent messages pointing to domains on this previously identified

list. In total, we identified 10 NSO exploit domains used in the targeting:

NSO Exploit Domain	Messages
secure-access10[.]mx	3
network190[.]com	3
iusacell-movil[.]com.mx	2
mymensaje-sms[.]com	1
smscentro[.]com	1
unonoticias[.]net	27
fb-accounts[.]com	5
smsmensaje[.]mx	31
ideas-telcel.com[.]mx	5
twiitter.com[.]mx	1

Figure 17 shows the connection between these domains and messages sent to targets in Mexico.

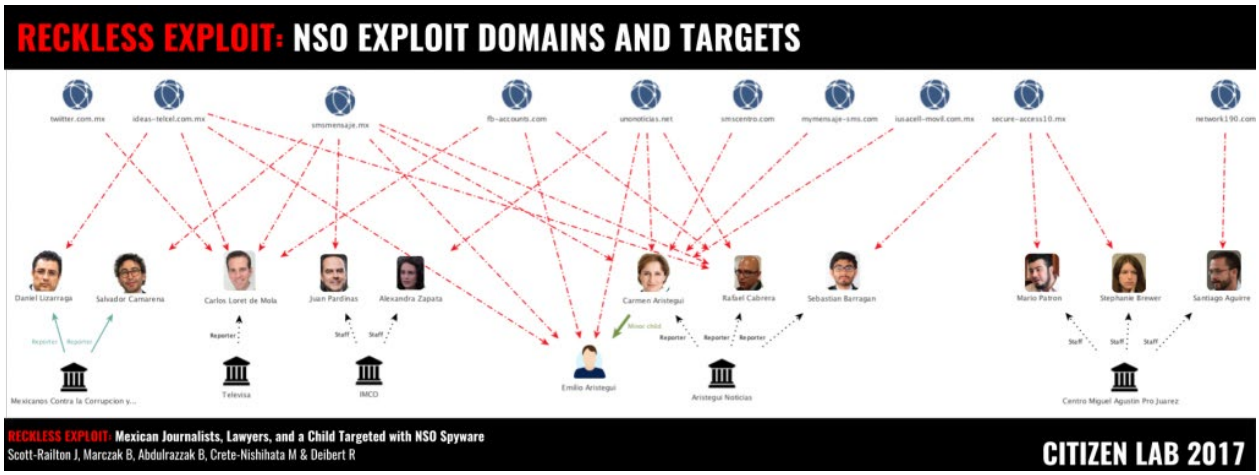


Figure 17: NSO Exploit Domains and Targets

Importantly, we are unsure whether the domains were all used by a single government operator, or reflect targeting by multiple government operators.

Interestingly, some of the earliest NSO Group exploit domains first served their exploits over HTTP rather than HTTPS. If NSO was using zero-day exploits at this time, their exploits may have been exposed to interception by third parties with visibility over the network traffic through which such exploits passed.

Part 4: Discussion

Digital Targeting Mirrors Physical Risks to Journalists

The physical threats journalists face in Mexico as a result of their work are well documented. Our investigation makes it clear that these threats extend to the digital realm. In the cases we describe in this report, the text messages included violent taunts and threats reflecting the pervasiveness of physical threats that Mexican media face. There were at least 426 documented attacks and incidents of intimidation against Mexican journalists in 2016 and more than half of them had an official origin.

The digital targeting that we describe compounds physical threats and harassment in several ways. Many of the journalists and civil society members who were targeted with infection attempts using NSO links, and their colleagues, were similarly targeted for other forms of harassment, and intimidation.

Reckless Targeting

A feature of the Mexican case that bears special discussion is the intensity of the targeting with NSO links, as well as the often extreme content of the messages.

NSO's Pegasus solution is designed for surreptitious monitoring of phones. Getting a victim to click and then remain infected without raising suspicion is a delicate task. Contrary to this imperative, the entities operating NSO products in this case were, at best, using the tool for something closer to a digital smash-and-grab operation: the messages were both brazen and extremely obvious. Not only did most of the messages use deceptions that were easy to falsify, but the Mexican operators show a recurring preference for crude, sexual taunts, as we have noted in both prior reports. Someone clicking on them would be likely to almost immediately recognize their mistake.

The recklessness of the operation extends to impersonating official programs and entities including AMBER Alerts and the United States Embassy in Mexico, which can trigger negative consequences. Creating fake malicious AMBER Alerts threatens to reduce the credibility of real AMBER Alerts. Meanwhile, impersonating messages

from the United States Embassy runs the risk of violating diplomatic norms, and upsetting a major ally and trading partner. Were these messages sent to lower-profile private individuals, the ruse may never have been discovered. But instead, the messages were sent to very high profile and well known journalists, increasing the likelihood of discovery.

We highlighted several of these themes in previous reporting about the misuse of NSO spyware to target Mexican food scientists and health advocates. The findings in this investigation make it clear that substantial additional abuse took place.

The infection attempts against the minor child who was physically residing in the United States may have criminal ramifications. For example, under Section 18 U.S. Code § 912, impersonating a federal official is a federal criminal offense. Further, under the Computer Fraud and Abuse Act (18 U.S.C. § 1030), attempts to access a computer without authorization may be criminal offenses. Moreover, the US Wiretap Act has been previously cited with respect to other cases of cross-border targeting on US soil using commercial malware.

Lack of Oversight and Accountability

The choice of targets, and the style of targeting, provides strong evidence that the targeting was conducted without proper oversight and judicial accountability.

Like the federal food scientists and consumer advocates who were also targeted with NSO exploit links, the targets in this report are neither criminals nor terrorists, but widely respected journalists and human rights defenders.

The recklessness of the targeting also points to a lack of oversight. R3D, SocialTic, and Article 19 highlight the legal issues surrounding this case in their report. Mexico does not have specific legal regulations governing the use of malware, but the constitution and law (under Article 16) does authorize several legal entities to conduct intercepts. Interception of this type requires federal judicial authorization. Mexico's Centro de Investigación y Seguridad Nacional (CISEN) is authorized to conduct interceptions when there is an imminent threat to national security, Mexico's Federal police is authorized when there is probable cause to believe certain crimes are being committed, and Mexican local and federal prosecutors are similarly authorized. However, such surveillance always requires the approval of a judge. R3D provides a detailed discussion of the legal issues governing surveillance in Mexico in this report.

Our investigation also provided the first example that we are aware of in which a minor child was targeted with government exclusive spyware. Emilio Aristegui received at least 21 confirmed NSO messages, and several more that we strongly suspect to be NSO messages. The relentless targeting included many of the same upsetting and highly personal themes as the adult recipients.

It is difficult to conceive of what legitimate investigation would include these journalists, human rights defenders, and a minor child. There is no clear basis for them to be categorized as threats to national security. The same could be said for prior evidence of the NSO spyware campaign against Mexican government food scientists, health, and consumer advocates. Regardless of the legitimacy of the targets, this type of aggressive surveillance with malware may not pass the necessary and proportionate tests under Mexican law.

Furthermore, it seems unlikely that a federal judge, or other source of operational oversight, would have authorized such a politically risky act as masquerading as the United States Embassy to two of the country's highest profile journalists, or targeting an individual located within the United States.

Conclusion: The "Principle of Misuse"

There is extensive research into the market for government-exclusive spyware and cases of abuse. Around the globe, spyware sold to governments ostensibly to track terrorists and investigate criminals is, in a growing number of documented incidents, abused for nakedly political ends.

More recently, several spyware manufacturers, including Gamma Group (FinFisher) and Hacking Team, were subject to breaches, and had their customer data posted online. Some customers appeared to be engaged in what many would consider legitimate investigations. However, the breach also revealed a global list of government customers in countries known to abuse human rights. Taken together, these findings made it clear that misuse of government-exclusive spyware is a global problem.

This report, taken together with the results of two previous investigations into NSO Group, suggest that their product and corporate behavior fits the same pattern of proliferation and misuse.

After cases of abuse come to light, spyware companies are often asked by the media for comment. Typically company executives respond with a mixture of evasiveness and allusions to their own internal due-diligence processes. The evidence, however, continues to mount that self-regulation, as well as international regulatory efforts, have failed to stop the continued proliferation and abuse of these technologies.

As a result, we think that there is evidence of an informal "principle of misuse" for government-exclusive spyware: when the technology is sold to a government without sufficient oversight, it will eventually be misused. This principle highlights the need to hold spyware manufacturers accountable for their contributions to global cyber insecurity.

In a recent publication, Citizen Lab researchers outlined a checklist of measures that could be taken to reign in such abuses. Until steps are taken to limit the possibility of abusive use, we anticipate finding more cases where highly-invasive spyware is used to stifle dissent and block opposition to powerful elites.

Appendix A: Full Message List

Target	Text Message Date	Text Message Original	Sender Phone Number	Text Message Translated	Link in SMS	Unshortens to
Carmen Aristegui	1/12/2015	El siguiente mensaje no ha sido enviado [malicious link]	5511393877	The next message has not been sent [malicious link]	hxxp://bit[.]ly/1z2NQdh	hxxp://smscentro[.]com/9480260s/
Carmen Aristegui	4/12/2015	Notificación de compra con tarjeta [REDACTED] monto $3,500.00 M.N, ver detalles en: [malicious link]	5525715066	Purchase notification with card [REDACTED] amount $3,500.00 M.N. see details at: [malicious link]	hxxp://smsmensaje[.]mx/1493024s/	
Carmen Aristegui	5/8/2015	Aviso de vencimiento de pago asociado a tu servicio con cargo a tu tarjeta [REDACTED] , ver mas detalles: [malicious link]	5525715066	Due date payment notification associated with your service with charge to card [REDACTED] , see more details: [malicious link]	hxxp://smsmensaje[.]mx/6445761s/	
Carmen Aristegui	5/8/2015	Haz realizado un Retiro/Compra en Tarjeta [REDACTED] M.N monto $3,500.00 verifica detalles de operacion: [malicious link]	5525715066	You have made a Withdrawal/Purchase in card [REDACTED] M.N. ammount $3,500.00 verify operation details: [malicious link]	hxxp://smsmensaje[.]mx/9936510s/	
Carmen Aristegui	5/11/2015	Estimado cliente informamos que presentas un problema de pago asociado a tu servicio, ver detalles.. [malicious link]	5525715066	Dear client we inform you that there is a payment problem associated with your service, see details. [malicious link]	hxxp://smsmensaje[.]mx/[unavailable]	
Carmen Aristegui	5/13/2015	UNONOTICIAS. [REDACTED] [malicious link]	5525715066	UNONOTICIAS. [REDACTED] [malicious link]	hxxp://unonoticias[.]net/6218095s/	
Carmen Aristegui	7/26/2015	Haz realizado un Retiro/Compra en Tarjeta [REDACTED] M.N monto $3,500.00 verifica detalles de operacion: [malicious link]	5525715066	You have made a Withdrawal/Purchase in card [REDACTED] M.N. ammount $3,500.00 verify operation details: [malicious link]	hxxp://smsmensaje[.]mx/9936510s/	
Carmen Aristegui	7/26/2015	UNOTV.COM/ ANONYMUS ANUNCIA QUE ATACARA PAGINA DE ARISTEGUI VER DETALLES: [malicious link]	5525715066	UNOTV.COM/ ANONYMUS ANNOUNCES IT WILL ATTACK ARISTEGUI'S WEBSITE SEE DETAILS [malicious link]	hxxp://unonoticias[.]net/9250302s/	
Carlos Loret de Mola	8/20/2015	USEMBASSY.GOV/ DETECTAMOS UN PROBLEMA CON TU VISA POR FAVOR ACUDE PRONTAMENTE A LA EMBAJADA. VER DETALLES: [malicious link]	5585583974	USEMBASSY.GOV/ WE DETECTED A PROBLEM WITH YOUR VISA PLEASE GO TO THE EMBASSY QUICKLY. SEE DETAILS [malicious link]	hxxp://bit[.]ly/1MAzTZ7	hxxp://smsmensaje[.]mx/3990495s/
Carmen Aristegui	8/20/2015	IUSACELL/ Estimado cliente su factura esta lista, agradeceremos pago puntual por $17401.25	5525715066	IUSACELL/ Dear client your bill is ready, we will thank your punctual payment for $17401.25	hxxp://iusacell-movil[.]com[.]mx/8595070s/	
Carmen Aristegui	8/20/2015	USEMBASSY.GOV/ DETECTAMOS UN PROBLEMA CON TU VISA POR FAVOR ACUDE PRONTAMENTE A LA EMBAJADA. VER DETALLES: [malicious link]	5525715066	USEMBASSY.GOV/ WE HAVE DETECTED A PROBLEM WITH YOUR VISA PLEASE GO PROMPTLY TO THE EMBASSY. SEE DETAILS: [malicious link]	hxxp://bit[.]ly/1MAAWrO	hxxp://smsmensaje.mx/9439115s/
Carmen Aristegui	8/22/2015	IUSACELL.COM/ EL SIGUIENTE MENSAJE ESTA MARCADO COMO URGENTE REVISALO DESDE NUESTRO PORTAL VER [malicious link]	5525715066	iUSACELL.COM/ THE FOLLOWING MESSAGE IS MARKED AS URGENT REVISE IT IN OUR WEBSITE SEE [malicious link]	hxxp://iusacell-movil[.]com[.]mx/7918310s/	

Target	Text Message Date	Text Message Original	Sender Phone Number	Text Message Translated	Link in SMS	Unshortens to
Carmen Aristegui	8/24/2015	ALERTA AMBER DF/ COOPERACION PARA LOCALIZAR A NINO DE 9 ANOS, DESAPARECIDO EN LA COLONIA [REDACTED] . DETALLES [malicious link]	5525715066	AMBER ALERT DF/ ASSISTANCE IN LOCATING A 9 YEAR OLD BOY WHO DISAPPEARED IN [redacted] NEIGHBORHOOD: [malicious link]	hxxp://bit[.]ly/1EQYOkG	hxxp://mymensaje-sms[.]com/6649365s/
Carlos Loret de Mola	8/29/2015	estas personas vinieron preguntando por usted vienen en camioneta sin placas tome foto los conoce? mire	5585583974	these people came asking for you they came in a van without license plates i took a picture do you know them? look: [malicious link]	hxxp://bit[.]ly/1JDkjuX	hxxp://fb-accounts[.]com/2069487s/
Emilio Aristegui	8/30/2015	UNOTV.COM/ POR TEMA DE CASA BLANCA PRESIDENCIA PODRIA ENCARCELAR REPORTEROS MIENTRAS INVESTIGA VER NOMBRES: [malicious link)	UNKNOWN	UNOTV.COM/ BECAUSE OF THE CASA BLANCA ISSUE THE PRESIDENCY COULD JAIL REPORTERS WHILE IT INVESTIGATES SEE NAMES: [malicious link]	hxxp://bit[.]ly/1LLYT15	hxxp://unonoticias[.]net/5819525s/
Emilio Aristegui	8/30/2015	UNOTV.COM/ PRESIDENCIA DEMANDARÁ POR DIFAMACIÓN A QUIENES PUBLICARON REPORTAJE DE LA CASA BLANCA. NOTA: [malicious link]	UNKNOWN	UNOTV.COM/ PRESIDENCY WILL SUE FOR DEFAMATION AGAINST THOSE THAT PUBLISHED THE CASA BLANCA REPORT. STORY: [malicious link]	hxxp://unonoticias[.]net/9804185s/	
Emilio Aristegui	8/30/2015	UNOTV.COM/ DETIENEN A PRESUNTO LIDER DE CARTEL DE SINALOA EN RESTAURANTE LA MANCION DE [REDACTED] VER: [malicious link]	UNKNOWN	UNOTV.COM/ PRESUMPTIVE LEADER OF THE SINALOA CARTEL IS DETAINED AT RESTAURANT LA MANCION OF [REDACTED] SEE: [malicious link]	hxxp://bit[.]ly/1KufGUy	hxxps://unonoticias[.]net/1214510s/
Carlos Loret de Mola	9/1/2015	TELCEL.COM/ Estimado cliente su factura esta proxima a vencer, agradeceremos su pago por $19750.26 Detalles: [malicious link]	5535044351	TELCEL.COM/ Dear client your bill will soon be due, your payment is $19750.26 Details: [malicious link]	hxxp://ideas-telcel[.]com[.]mx/7757294s	
Carlos Loret de Mola	9/3/2015	Carlos, buen día. Otra vez estan sacando chismes tuyos, supuestamente te tomaron fotos en UNIVISION mira: [malicious link]	5535044351	Carlos, good day. Again they are spreading rumors about you, supposedly they took pictures of you in UNIVISION look: [malicious link]	hxxp://bit[.]ly/1QbgONr	hxxp://twiitter.com[.]mx/2857663s/
Carlos Loret de Mola	9/5/2015	TELCEL.COM/ ESTIMADO USUARIO LE RECORDAMOS QUE TIENE UN SALDO PENDIENTE DE $4280.00 M/N VERIFICA DETALLES DEL CARGO: [malicious link]	5549576224	TELCEL.COM/ DEAR USER WE REMIND YOU THAT YOU HAVE A PENDING BALANCE OF $4280.00 VERIFY THE DETAILS OF THE CHARGE: [malicious link]	hxxp://bit[.]ly/1JW0JFQ	hxxp://ideas-telcel.com[.]mx/2110126s/
Carlos Loret de Mola	9/6/2015	ALERTAAMBER.COM/ SOLICITAMOS SU COOPERACION PARA LOCALIZAR A ESTUDIANTE DE LA FACULTAD DE FILOSOFIA DE LA UNAM VER FOTO [malicious link]	5549576224	ALALERTAAMBER.COM/ WE ASK FOR YOUR ASSISTANCE IN LOCATING A STUDENT FROM THE UNAM SCHOOL OF PHILOSOPHY SEE PHOTO [malicious link]	hxxp://bit[.]ly/1O77vPb	hxxp://smsmensaje[.]mx/1331744s/
Carmen Aristegui	10/25/2015	Hola te envio invitacion electronica con detalles por motivo de mi fiesta de disfraces espero contar contigo alonso: [malicious link]	5525715066	Hi I am sending you an electronic invitation with details about my costume party I hope I can count with you alonso: [malicious link]	hxxp://tinyurl[.]com/o2tq8rl	
Juan Pardinas	12/21/2015	en la madrugada fallecio mi padre, estamos devastados, te envio los datos del velatorio, espero puedas venir: [malicious link]	5551923720	my father died this morning, we are devastated, I am sending you the information about the funeral, I hope you can come: [malicious link]	hxxp://bit[.]ly/1Nz2RZe	hxxps://smsmensaje[.]mx/5732641s/

Target	Text Message Date	Text Message Original	Sender Phone Number	Text Message Translated	Link in SMS	Unshortens to
Juan Pardinas	12/24/2015	oiga afuera de su casa anda una camioneta con 2 vatos armados, les tome fotos vealos y cuidese: [malicious link]	5551923720	hey, there is a van outside your house with 2 armed dudes, I took pictures look at them and take care: [malicious link]	hxxp://bit[.]ly/1JzfmW1	hxxps://smsmensaje[.]mx/7893029s/
Carmen Aristegui	2/9/2016	Carmen hace 5 dias que no aparece mi hija te agradecere mucho que compartas su foto, estamos desesperados: [malicious link]	5552899427	Carmen my daughter has been missing for 5 days, we are desperate, I would be grateful if you help me by sharing her photo: [malicious link]	hxxp://bit[.]ly/1KDekJ9	hxxp://smsmensaje.mx/1239663s/
Carmen Aristegui	2/10/2016	Querida Carmen fallecio mi hermano en un accidente, estoy devastada, envio datos del velorio, espero asistas: [malicious link]	5552899427	Dear Carmen my brother died in an accident, I'm devastated, I send you the information about the funeral, I hope you can come: [malicious link]	hxxp://bit[.]ly/1TTjm6D	hxxp://smsmensaje.mx/6056487s/
Carmen Aristegui	2/24/2016	UNOTV.COM/ LANZA TELEVISA DESPLEGADOS EN TODOS SUS MEDIOS;CRITICA POSTURA DE ORGANIZACION ARTICULO 19. VER: [malicious link]	5552899427	UNOTV.COM/ TELEVISA LAUNCHES ANNOUNCEMENTS IN ALL ITS MEDIA; CRITICIZES THE POSITION OF THE ORGANIZATION ARTICLE 19 SEE: [malicious link]	hxxp://bit[.]ly/1SU5N7q	hxxps://unonoticias[.]net/6809853s/
Carlos Loret de Mola	3/5/2016	Loret hoy fallecio mi padre estamos devastados envio datos del velatorio espero contar contigo mau [malicious link]	9993191309	Loret my father died today we are devastated I am sending you the information of the wake I hope I can count on you mau [sic] [malicious link]	hxxp://tinyurl[.]com/j7luz86	hxxps://smsmensaje[.]mx/2683786s/
Emilio Aristegui	3/18/2016	UNOTV.COM/ EN ENTREVISTA PARA DIARIO DE EU; MIGUEL ANGEL MANCERA ACEPTA SU HOMOSEXUALIDAD. DETALLES: [malicious link]	8120754062	UNOTV.COM/ IN INTERVIEW WITH NEWSPAPER FROM THE U.S.; MIGUEL ANGEL MANCERA ACCEPTS HIS HOMOSEXUALITY. DETAILS: [malicious link]	hxxps://unonoticias[.]net/1419678s/	hxxp://unonoticias[.]net/1214510s/
Emilio Aristegui	4/1/2016	ARISTEGUI NOTICIAS ESTRENA SERVICIO DE SMS, SUSCRIBASE Y RECIBIRA RESUMEN DE LAS NOTICIAS MÁS IMPORTANTES: [malicious link]	8114116769	ARISTEGUI NOTICIAS RELEASES SMS SERVICE, SUBSCRIBE AND RECEIVE A SUMMARY OF MOST IMPORTANT NEWS [malicious link]	smsmensaje[.]mx [full link unavailable]	
Emilio Aristegui	4/6/2016	ARISTEGUINOTICIASONLINE.MX ESTRENA SERVICIO DE SMS. SUSCRIBASE Y RECIBIRA LAS NOTICIAS MAS IMPORTANTES: [malicious link]	8121200623	ARISTEGUINOTICIASONLINE.MX RELEASES SMS SERVICE. SUBSCRIBE AND RECEIVE THE MOST IMPORTANT NEWS [malicious link]	smsmensaje[.]mx [full link unavailable]	
Mario Patrón	4/20/2016	EL GOBIERNO DE MEXICO MADRUGA AL GIEI [malicious link]	18112898080	THE GOVERNMENT OF MEXICO TAKES GIEI OFF GUARD [malicious link]	hxxp://bit[.]ly/20Y9r10	hxxps://secure-access10[.]mx/4257391s/
Carlos Loret de Mola	4/20/2016	Querido Loret, fijate que tvnotas tiene fotos tuyas donde estas con una chava cenando. Dales una checada: [malicious link]	5539326314	Dear Loret, look tvnotas has photos of you dining with a girl. Look at them: [malicious link]	hxxp://bit[.]ly/1NlM0ME	hxxps://smsmensaje[.]mx/8643330s/
Stephanie Brewer	5/11/2016	y segun ustedes que hace Derechos Humanos ante esto, y la dignidad de ellos que… [malicious link]	8112487399	And according to you what does Human Rights do about this, what about their dignity… [malicious link]	hxxp://bit[.]ly/1Nr0Vpb	hxxps://secure-access10[.]mx/7161504s/
Emilio Aristegui	5/11/2016	UNOTV.COM/ CONFIRMA PGR QUE HIJO MAYOR DE AMLO LLEVA 48 HRS DESAPARECIDO. DETALLES: [malicious link]	5560741842	UNOTV.COM/ PGR CONFIRMS THAT AMLO'S ELDEST SON HAS BEEN MISSING FOR 48 HRS. DETAILS: [malicious link]	hxxp://bit[.]ly/1QYVJU9	hxxps://unonoticias[.]net/6843502s/

Target	Text Message Date	Text Message Original	Sender Phone Number	Text Message Translated	Link in SMS	Unshortens to
Sebastián Barragán	5/12/2016	Tengo pruebas clave y fidedignas en contra de servidores publicos, ayudame tiene que ver con este asunto [malicious link]	8112889362	I have key and thrustworthy evidence against public servants, help me it has to do with this issue [malicious link]	hxxp://bit[.]ly/1s2eguc	hxxps://secure-access10[.]mx/2618844s/
Emilio Aristegui	5/16/2016	UNOTV.COM/ ASESINAN AL CITY MANAGER ARNE DEN RUHEN. DETALLES: [malicious link]	8120754115	UNOTV.COM/ CITY MANAGER ARNE DEN RUHEN IS MURDERED. DETAILS: [malicious link]	hxxps://unonoticias[.]net/2046803s/	
Alexandra Zapata	5/17/2016	UNOTV.COM/ REPORTAJE: LA HISTORIA DE CORRUPCION DETRAS DEL INTITUTO MEXICANO PARA LA COMPETITIVIDAD. VER: [malicious link]	8120754119	UNOTV.COM/ REPORT: THE STORY OF CORRUPTION BEHIND THE MEXICAN INSTITUTE FOR COMPETITIVENESS. SEE: [malicious link]	hxxps://unonoticias[.]net/6532946s/	
Rafael Cabrera	5/18/2016	TELCEL.COM/ EL SIGUIENTE MENSAJE SE HA MARCADO COMO URGENTE Y NO SE RECIBIO COMPLETAMENTE RECUPERELO EN [malicious link]	8121209616	TELCEL.COM/ THE FOLLOWING MESSAGE HAS BEEN MARKED AS URGENT AND WAS NOT COMPLETELY RECEIVED. RECOVER IT AT [malicious link]	hxxp://bit[.]ly/1NzkyeZ	hxxps://smsmensaje[.]mx/8435662s/
Daniel Lizárraga	5/18/2016	TELCEL.COM/ ESTIMADO USUARIO LE RECORDAMOS QUE PRESENTA UN ADEUDO DE $8,854.90 M/N VERIFIQUE DETALLES: [malicious link]	8181852839	TELCEL.COM/ DEAR USER WE REMIND YOU THAT YOU OWE $8,854.90 VERIFY THE DETAILS [malicious link]	hxxp://ideas-telcel[.]com[.]mx/1930327s	
Alexandra Zapata	5/18/2016	UNOTV.COM/ [redacted] [malicious link]	8120531609	UNOTV.COM/ [redacted] [malicious link]	hxxps://unonoticias[.]net/4392216s/	
Emilio Aristegui	5/18/2016	UNOTV.COM/ FILTRAN VIDEO DONDE LORET DE MOLA MANTIENE RELACIONES SEXUALES CON [REDACTED]. VER VIDEO [malicious link]	8120531349	UNOTV.COM/ LEAKED VIDEO WHERE LORET DE MOLA HAS SEXUAL RELATIONS WITH [REDACTED]. SEE VIDEO [malicious link]	hxxps://unonoticias[.]net/4709973s/	
Rafael Cabrera	5/19/2016	TELCEL.COM/ ESTIMADO USUARIO LE RECORDAMOS QUE PRESENTA UN ADEUDO DE $8,854.90 M/N VERIFIQUE DETALLES: [malicious link]	8120953203	TELCEL.COM/ DEAR USER WE REMIND YOU THAT YOU OWE $8,854.90 VERIFY THE DETAILS [malicious link]	hxxps://ideas-telcel[.]com[.]mx/3975827s	
Emilio Aristegui	5/19/2016	UNOTV.COM/ POSIBLE CORRUPCION REVELA AUDIO TELEFONICO ENTRE EPN Y PRESIDENTE DE OHL. AUDIO EN: [malicious link]	8120531329	UNOTV.COM/ POSSIBLE CORRUPTION REVEALED BY TELEPHONE AUDIO BETWEEN EPN AND OHL PRESIDENT AUDIO AT: [malicious link]	hxxps://unonoticias[.]net/3651023s/	
Santiago Aguirre	5/20/2016	SrJorge soy Juan Magarino ayuda con mi hermano Heriberto se lo llevo la policia por ser maestro es un delito [malicious link]	8122090332	Mr Jorge I'm Juan Magarino please help with my brother Heriberto, the police took him for being a teacher this is a crime [malicious link]	hxxp://bit[.]ly/1XFaS4F	hxxps://network190[.]com/8361397s/
Rafael Cabrera	5/20/2016	Facebook reporta intentos de acceso a la cuenta: Rafa Cabrera. Evite bloqueo de cuenta, verifique en: [malicious link]	8120754118	Facebook reports an attempt to access your account: Rafa Cabrera. Avoid the blocking of your account, verify in: [malicious link]	hxxps://fb-accounts[.]com/2408931s	
Emilio Aristegui	5/20/2016	TELCEL.COM/ ESTIMADO USUARIO LE RECORDAMOS QUE PRESENTA UN ADEUDO DE $10,854.90 M/N VERIFIQUE DETALLES [malicious link]	8121228698	TELCEL.COM/ DEAR USER WE REMIND YOU THAT YOU HAVE A DEBT OF $10,854.90 MN VERIFY DETAILS [malicious link]	hxxps://ideas-telcel[.]com[.]mx/5706662s	

Target	Text Message Date	Text Message Original	Sender Phone Number	Text Message Translated	Link in SMS	Unshortens to
Rafael Cabrera	5/23/2016	UNOTV.COM/ PODRIA IR CARMEN ARISTEGUI COMO CANDIDATA INDEPENDIENTE EN 2018. DETALLES: [malicious link]	5561089094	UNOTV.COM/ CARMEN ARISTEGUI COULD RUN AS AN INDEPENDENT CANDIDATE IN 2018. DETAILS: [malicious link]	hxxps://unonoticias[.]net/1867745s/	
Emilio Aristegui	5/23/2016	UNOTV.COM/ PODRIA IR CARMEN ARISTEGUI COMO CANDIDATA INDEPENDIENTE EN 2018. DETALLES: [malicious link]	5560741842	UNOTV.COM/ CARMEN ARISTEGUI COULD RUN AS AN INDEPENDENT CANDIDATE IN 2018. DETAILS: [malicious link]	hxxps://unonoticias[.]net/8167459s/	
Rafael Cabrera	5/24/2016	No tienes los huevos de ver como me fajo a tu pareja. Mira nada mas como co****s bn rico y en tu cama: [malicious link]	3131051501	You don't have the balls to watch how I make out with your partner. Look how we f**k so good and in your bed: [malicious link]	hxxp://bit[.]ly/246dkRy	hxxps://smsmensaje[.]mx/4667624s/
Salvador Camarena	5/24/2016	No tienes los huevos de ver como me fajo a tu pareja. Mira nada mas como co****s bn rico y en tu cama: [malicious link]	5562925040	You don't have the balls to watch how I make out with your partner. Look how we f**k so good and in your bed: [malicious link]	hxxp://bit[.]ly/246doke	hxxps://smsmensaje[.]mx/4878494s/
Salvador Camarena	5/25/2016	Afuera de tu casa esta una camioneta sospechosa y estan tomando video de la casa. Les tome foto mira: [malicious link]	5562925040	There is a suspicious van outside your house and they are taking video of the house. I took pictures of them look: [malicious link]	hxxp://bit[.]ly/1Xxf32k	hxxps://smsmensaje[.]mx/5478753s/
Emilio Aristegui	5/26/2016	UNOTV.COM/ HAYAN DECAPITADO A PERIODISTA EN VERACRUZ Y DEJAN NARCOMENSAJE AMENAZADOR. FOTOS Y DETALLES: [malicious link]	8120957553	UNOTV.COM/ BEHEADED JOURNALIST IS FOUND IN VERACRUZ WITH THREATHNING NARCOMESSAGE. PHOTOS AND DETAILS: [malicious link]	hxxps://unonoticias[.]net/8439927s/	
Emilio Aristegui	5/27/2016	UNOTV.COM/ DECOMISAN CARGAMENTO DEL CIDA/ OSAMA BIN LADEN NO HA MUERTO/ DETIENEN A LUPITA DALESIO [malicious link]	8120958612	UNOTV.COM/ SEIZURE OF CIDA SHIPMENT/ OSAMA BIN LADEN IS NOT DEAD ALIVE/ LUPITA DALESIO DETAINED [malicious link]	hxxp://bit[.]ly/25nmH1O	hxxps://unonoticias[.]net/8592764s/
Rafael Cabrera	5/30/2016	UNOTV.COM/ PRESIDENCIA DEMANDARA POR DIFAMACION A QUIENES PUBLICARON REPORTAJE DE LA CASA BLANCA. NOTA: [malicious link]	5561067277	UNOTV.COM/ THE PRESIDENCY WILL SUE FOR DEFAMATION AGAINST THE PUBLISHERS OF THE CASA BLANCA REPORT	hxxp://bit[.]ly/1hMG15k	hxxp://fb-accounts[.]com/1074139s/
Rafael Cabrera	5/30/2016	UNOTV.COM/ POR TEMA DE CASA BLANCA PRESIDENCIA PODRIA ENCARCELAR REPORTEROS MIENTRAS INVESTIGA VER NOMBRES: [malicious link]	5561067277	UNOTV.COM/ BECAUSE OF THE CASA BLANCA ISSUE THE PRESIDENCY COULD INCARCERATE REPORTERS WHILE IT INVESTIGATES SEE NAMES: [malicious link]	hxxp://bit[.]ly/1LLY8oK	hxxp://unonoticias[.]net/3423768s/
Emilio Aristegui	5/30/2016	UNOTV.COM/ EJECUTAN PERIODISTA Y DEJAN NARCOMENSAJE/ CONTINUA DOBLE NO CIRCULA/ NOVIA ENLOQUECE DE CELOS [malicious link]	8181852839	UNOTV.COM/ JOURNALIST EXECUTED AND NARCOMESSAGE IS LEFT/ DOUBLE NO-DRIVE DAY CONTINUES/ GIRLFRIEND GOES CRAZY WITH JEALOUSY [malicious link]	hxxp://bit[.]ly/1X9kJRJ	hxxps://smsmensaje[.]mx/4494681s/
Emilio Aristegui	6/1/2016	UNOTV.COM/ CARMEN ARISTEGUI SE DESTAPA COMO CANDIDATA AL GOBIERNO DE LA CDMX PARA EL 2018. DETALLES: [malicious link]	8121961566	UNOTV.COM/ CARMEN ARISTEGUI REVEALED AS CANDIDATE FOR CDMX GOVERNMENT IN 2018. DETAILS: [malicious link]	hxxps://unonoticias[.]net/5851721s/	

Target	Text Message Date	Text Message Original	Sender Phone Number	Text Message Translated	Link in SMS	Unshortens to
Carmen Aristegui	6/3/2016	Carmen la pagina esta intermitente, esta apareciendo este error al intentar ingresar: [malicious link]	5585401299	Carmen the website is intermitent, this error appears when you try to get in: [malicious link]	hxxp://bit[.]ly/1WzrZ8T	hxxp://smsmensaje.mx/9371877s/
Emilio Aristegui	6/3/2016	USEMBASSY.GOV/ DETECTAMOS UN PROBLEMA CON TU VISA POR FAVOR ACUDE PRONTAMENTE A LA EMBAJADA VER DETALLES: [malicious link]	5560741842	USEMBASSY.GOV/ WE HAVE DETECTED A PROBLEM WITH YOUR VISA PLEASE GO PROMPTLY TO THE EMBASSY. SEE DETAILS: [malicious link]	hxxp://bit[.]ly/1Wzryvp	hxxps://smsmensaje[.]mx/7831163s/
Santiago Aguirre	6/8/2016	Mtro, tuve un incidente, le envio nuevamente mi tesis, basada en su tesina para que me de su comentarios [malicious link]	8122090340	Professor, I had a problem, I am resending my thesis, based in your dissertation so you can give me comments: [malicious link]	hxxp://bit[.]ly/292heXd	hxxps://network190[.]com/2066781s/
Carmen Aristegui	6/13/2016	Hace 3 días que no aparece mi hija, estamos desesperados, te agradecere que me ayudes a compartir su foto: [malicious link]	5585401299	my daughter has been missing for 3 days, we are desperate, I would be grateful if you help me by sharing her photo: [malicious link]	hxxp://bit[.]ly/235giae	hxxp://smsmensaje.mx/5957475s/
Carmen Aristegui	6/15/2016	Buenas tardes Carmen, unicamente paso a saludarte y enviarte esta nota de Proceso que es importante retomar: [malicious link]	8122090316	Good afternoon Carmen, I only came to say hello and send you this story from Proceso that is important to pick up: [malicious link]	hxxp://bit[.]ly/1twXSDl	hxxp://smsmensaje.mx/1911343s/
Emilio Aristegui	6/22/2016	UNOTV.COM/ REVELAN VIDEO DONDE CRISTIANO RONALDO SE ENFADA Y AVIENTA MICROFONO DE REPORTERO. VIDEO EN [malicious link]	8120957553	UNOTV.COM/ REVEALED VIDEO WHERE CRISTIANO RONALDO GET ANGRY AND THROWS REPORTER'S MICROPHONE. VIDEO AT [malicious link]	hxxps://unonoticias[.]net/7564969s/	
Santiago Aguirre	6/28/2016	Buen día Mtro. trabajo en mi tesis, tome como base su tesina, me interesa su opinion, le mando los adelantos [malicious link]	8122090340	Good day professor, I'm working in my thesis, I took your dissertation as a base, I'm interested in your opinion, I am sending you an advanced copy [malicious link]	hxxp://bit[.]ly/1U0yzVG	hxxps://network190[.]com/6214010s/
Carmen Aristegui	6/28/2016	UNOTV.COM/ ATENTADO TERRORISTA EN ESTAMBUL DEJA 30 MUERTOS/SECUESTRAN REPORTERO DE TELEVISA/ FALLECE CHACHITA [malicious link]	8120696998	UNOTV.COM/ TERRORIST ATTACK IN ISTANBUL LEAVES 30 DEAD/ KIDNAPPING OF TELEVISA REPORTER/ CHACHITA DIES [malicious link]	hxxp://bit[.]ly/295RNq7	hxxp://smsmensaje.mx/1656017s/
Emilio Aristegui	6/28/2016	UNOTV.COM/ ATENTADO TERRORISTA EN ESTAMBUL DEJA 30 MUERTOS/SECUESTRAN REPORTERO DE TELEVISA/ FALLECE CHACHITA [malicious link]	8122090346	UNOTV.COM/ TERRORIST ATTACK IN ISTANBUL LEAVES 30 DEAD/ KIDNAPPING OF TELEVISA REPORTER/ CHACHITA DIES [malicious link]	hxxp://bit[.]ly/295RmfH	hxxps://smsmensaje[.]mx/5840625s/
Carmen Aristegui	7/4/2016	UNOTV.COM/ AMARILLISMO DE ARISTEGUI VS REALIDAD/ VAN 30 DETENIDOS EN ATENTADO DE ESTAMBUL/ CHILE CAMPEON [malicious link]	8121050415	UNOTV.COM/ ARISTEGUI'S SENSACIONALISM AGAINST REALITY/ 30 DETAINEES IN ISTANBUL ATTACK/ CHILE IS THE CHAMPION [malicious link]	hxxp://bit[.]ly/29eWzzv	hxxps://unonoticias[.]net/9436744s/

Target	Text Message Date	Text Message Original	Sender Phone Number	Text Message Translated	Link in SMS	Unshortens to
Emilio Aristegui	7/4/2016	UNOTV.COM/ AMARILLISMO DE ARISTEGUI VS REALIDAD/ VAN 30 DETENIDOS EN ATENTADO DE ESTAMBUL/ CHILE CAMPEON [malicious link]	8120733949	UNOTV.COM/ ARISTEGUI'S SENSACIONALISM AGAINST REALITY/ 30 DETAINEES IN ISTANBUL ATTACK/ CHILE IS THE CHAMPION [malicious link]	hxxp://bit[.]ly/29eWFqz	hxxps://unonoticias[.]net/5027740s/
Emilio Aristegui	7/12/2016	UNOTV.COM/ FILMAN A REPORTERO Y PERIODISTA CUANDO SON LEVANTADOS POR COMANDO ARMADO EN TAMAULIPAS. VIDEO: [malicious link]	6675198654	UNOTV.COM/ REPORTER AND JOURNALIST ARE FILMED WHEN THE GET KIDNAPPED BY ARMED COMANDO IN TAMAULIPAS. VIDEO: [malicious link]	hxxps://unonoticias[.]net/5723329s/	
Carmen Aristegui	7/15/2016	[Redacted] [malicious link]	8122090286	[Redacted] [malicious link]	hxxp://bit[.]ly/29lQvyh	hxxp://smsmensaje.mx/3376811s/
Emilio Aristegui	7/18/2016	Hola oye abriste nuevo facebook? Me llego una solicitud de un face con tus fotos pero con otro nombre mira: [malicious link]	3313221176	Hi hey did you open a new facebook? I received a request of a facebook with your photos but with another name look: [malicious link]	fb-accounts[.]com [full link not available]	
Carmen Aristegui	7/19/2016	Hola buen martes. Oye que p*do con el p*to Lopez Doriga? Mira lo que escribió sobre ti hoy, urge desmentirlo: [malicious link]	8113788852	Hello good tuesday. Hey what the **k with f**king Lopez Doriga? Look what he wrote about you today, it is urgent to deny it: [malicious link]	hxxp://bit[.]ly/29LfZfD	hxxp://smsmensaje.mx/9093723s/
Emilio Aristegui	7/23/2016	Amigo, hay una pseudo cuenta de fb y twitter identica a la tuya checala para que la denuncies mira checala: [malicious link]	5560741842	Friend, there is a pseudo account on fb and twitter identical to yours check it out so you can report it look check: [malicious link]	fb-accounts[.]com [full link not available]	
Carmen Aristegui	7/25/2016	Bienvenido Club [redacted] se ha aplicado un cargo de $875.85 a su linea, si desea cancelar ingrese a: [malicious link]	8122090359	Welcome to [Redacted] Club, $875.85 has been charged to your line, if you want to cancel enter to: [malicious link]	hxxp://bit[.]ly/2a0hZ2l	hxxp://smsmensaje.mx/6881768s/
Emilio Aristegui	7/28/2016	UNOTV.COM/ VIRAL EL VIDEO DE FUERTE GOLPE QUE RECIBE EN LA CARA OSORIO CHONG PROPINADO POR MAESTRO. VIDEO: [malicious link]	5573313263	UNOTV.COM/ VIRAL VIDEO OF STRONG BLOW TO THE FACE RECEIVED BY OSORIO CHONG FROM TEACHER. VIDEO: [malicious link]	hxxps://unonoticias[.]net/7972736s/	