RECKLESS VI

Mexican Journalists Investigating Cartels Targeted with NSO Spyware Following Assassination of Colleague

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

NOVEMBER 27, 2018
RESEARCH REPORT #116

munk school
OF GLOBAL AFFAIRS & PUBLIC POLICY

UNIVERSITY OF TORONTO

THECITIZENLAB

Copyright

Suggested Citation

John Scott-Railton, Bill Marczak, Siena Anstis, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert. "Reckless VI: Mexican Journalists Investigating Cartels Targeted with NSO Spyware Following Assassination of Colleague," Citizen Lab Research Report No. 116, University of Toronto, November 2018.

Acknowledgements

Citizen Lab would like to thank Andrés Villarreal and Ismael Bojórquez for consenting to share this case with the collaborating organizations, and with the public. We are also grateful to the many other targets and victims of Pegasus for having shared the cases on which our continuing work is based.

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

Thanks to the whole Citizen Lab team, especially Sarah McKune, Miles Kenyon, and Adam Senft, as well as Mari Zhou for graphical assistance.

Thanks to Amnesty International and Access Now for assistance in earlier phases of the investigation.

About the Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto

The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs and Public Policy, University of Toronto, focusing on research, development, and high-level strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security.

We use a “mixed methods” approach to research that combines methods from political science, law, computer science, and area studies. Our research includes investigating digital espionage against civil society, documenting Internet filtering and other technologies and practices that impact freedom of expression online, analyzing privacy, security, and information controls of popular applications, and examining transparency and accountability mechanisms relevant to the relationship between corporations and state agencies regarding personal data and other surveillance activities.

Contents

Introduction 5

- By May 2017, Abuses of Pegasus Had Been Known For Eight Months 7
- NSO Group: A Spyware Company Linked To A Growing List of Abuses 7
- Journalists at Río Doce Targeted With Pegasus 8
- Links to NSO Group's Exploit Infrastructure 9
- A Pattern of Failed Oversight at NSO Group 10
- Claims of Oversight and Vetting 10
  - NSO Group's Repeated Failures of Oversight 11

Conclusion & Discussion 12

- Pegasus: A Favoured Tool for Targeting Journalists 13
  - Journalists at Physical and Digital Risk in Mexico 13
- Hollow Claims of Oversight 15
  - Questions To Francisco Partners Go Unanswered 16

Appendix 17

This report is Part 7 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

- **Award winning journalist Javier Valdez Cárdenas was the founder of *Río Doce*, a Mexican newspaper known for investigating cartels. He was gunned down near his office in May 2017.**
- **Two days after the killing, *Río Doce*'s director and a colleague began receiving infection attempts with NSO Group's Pegasus spyware. Several of the infection attempts purported to provide information about the Cárdenas killing.**
- **The Mexican government-linked NSO Group customer had already been publicly exposed for abusing Pegasus months before, suggesting that NSO Group failed to take effective action to prevent the continuing abuse.**
- **A total of 24 individuals are now known to have been abusively targeted with Pegasus in Mexico.**

Introduction

"I'm going to die," Javier Valdez Cárdenas told his mother at the family's Friday lunch in his hometown of Culiacán, Sinaloa. It should have been a day for celebration. Valdéz had been receiving medical treatment and that day had gotten the news that he was cancer free. Days later, on May 15th, 2017, Cárdenas was killed. He was shot 12 times as he left the Sinaloa offices of Río Doce, the newspaper he had co-founded to investigate cartels and organized crime. The killers had pulled him from his car, taking his investigative files, laptop, and mobile phone.

Figure 1: Javier Valdez Cárdenas (left). On May 15, 2017, Cárdenas was shot 12 times as he left the Río Doce offices. [Credits: Cronica de Xalpa, EL DEBATE]

On the afternoon of the second day after the killing, Andrés Villarreal, a close colleague, received a text message with a news alert: Cárdenas' killers had been identified.

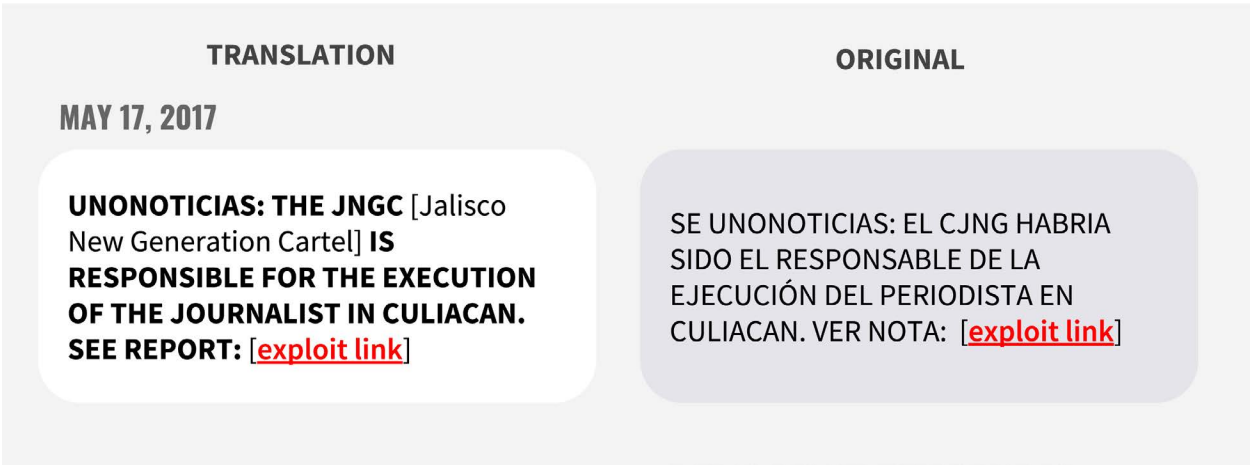

Figure 2: Message received by Andrés Villarreal appearing to confirm that the JNGC (Jalisco New Generation Cartel) was responsible for the murder of his colleague.

The message was, in fact, a carefully crafted attempt to infect his phone with Pegasus spyware. Had Villarreal clicked on the link, his phone would have been turned into a digital spy in his pocket. He would go on to receive several more infection attempts in the ensuing days. Shortly afterwards, Río Doce's Director Ismael Bojórquez also began to receive suspect messages. The same Mexican government-linked Pegasus operator (which we call RECKLESS-1) was trying to infect his phone, too.

Figure 3: Río Doce's Director Ismael Bojórquez and Director of Information Andrés Villarreal were targeted with Pegasus 48h after the murder of the newspapers' founder. Image credits: Noroeste, Parainfo 85

By May 2017, Abuses of Pegasus Had Been Known For Eight Months

We first reported on Pegasus in Mexico in August 2016 when we disclosed infection attempts sent to Mexican journalist Rafael Cabrera.[1] In a second investigative report, published in February 2017, with the assistance of Mexican non-governmental organizations R3D, SocialTic, and Article 19, we disclosed that health advocates and a government food scientist were targeted by a Mexican government-linked operator. We later named this operator RECKLESS-1. The disturbing implication was that RECKLESS-1 might have been using Pegasus on behalf of a commercial interest in the soft drinks industry.

1 While this Mexico government-linked operator is likely to be RECKLESS-1, technical limitations prevent us from conclusively saying so.

By the time Villarreal and Bojórquez were targeted by RECKLESS-1 in May 2017, it had been clear for almost eight months that Pegasus was being abused in Mexico. The case had even made two front page *New York Times* stories. Despite the attention, the Mexican government-linked operator did not appear to have felt sufficient pressure to stop targeting civil society. Nor did it appear that NSO Group, its supplier, stopped their client from continuing to abuse Pegasus.

Fortunately, recognizing the messages to be suspicious and familiar with our prior reporting on Pegasus, Villarreal and Bojórquez did not click. Later they shared the messages with Mexican collaborating organizations Article 19 and R3D. Citizen Lab and our Mexican collaborators, including SocialTic, have previously disclosed 22 targets of Pegasus in Mexico. With their assistance, and their close coordination to identify these two individuals, **we are now able to identify a total of 24 targets linked to Mexican Pegasus customers**.

NSO Group: A Spyware Company Linked To A Growing List of Abuses

Developed by NSO Group, an offensive "cyber warfare" company based in Israel, Pegasus is a sophisticated tool for spying on mobile phones. Pegasus is designed to allow an operator to monitor targets' iPhone or Android devices. Among its many functions, Pegasus allows an operator to read text messages (including encrypted messages) examine photos, and track a phone's location. Pegasus can also silently enable microphones and cameras, turning the phone into a bug to snoop on conversations happening in the phone's vicinity, such as in rooms or cars.

According to NSO Group, Pegasus is exclusively sold to governments for the purposes of fighting terror and investigating crime. However, in the past two years, we have discovered Pegasus has been used by repressive governments to spy on human rights defenders, journalists, and others who they may deem as threats to their power. In the United Arab Emirates (UAE), a human rights defender critical of the government was targeted with Pegasus and later imprisoned. In Canada, a critic of the Saudi regime and confidant of slain journalist Jamal Khashoggi was targeted in the months prior to Khashoggi's killing. An Amnesty International researcher and a prominent Saudi blogger were targeted by the same NSO Group customer, as was a Saudi dissident based in the UK. In the United States, the minor child of a Mexican journalist was targeted while at boarding school.

Journalists at Río Doce Targeted With Pegasus

Beginning on May 17, 2017, *Río Doce* journalist and Director of Information Andrés Villarreal began receiving suspicious text messages. The first of these messages promised information about the killing of his colleague. The message, disguised as a news alert, stated that the Jalisco New Generation Cartel had been linked to the slaying.

After a week of attempting to compromise Villarreal's phone, the operator selected a new victim: *Río Doce's* Director Ismael Bojórquez.

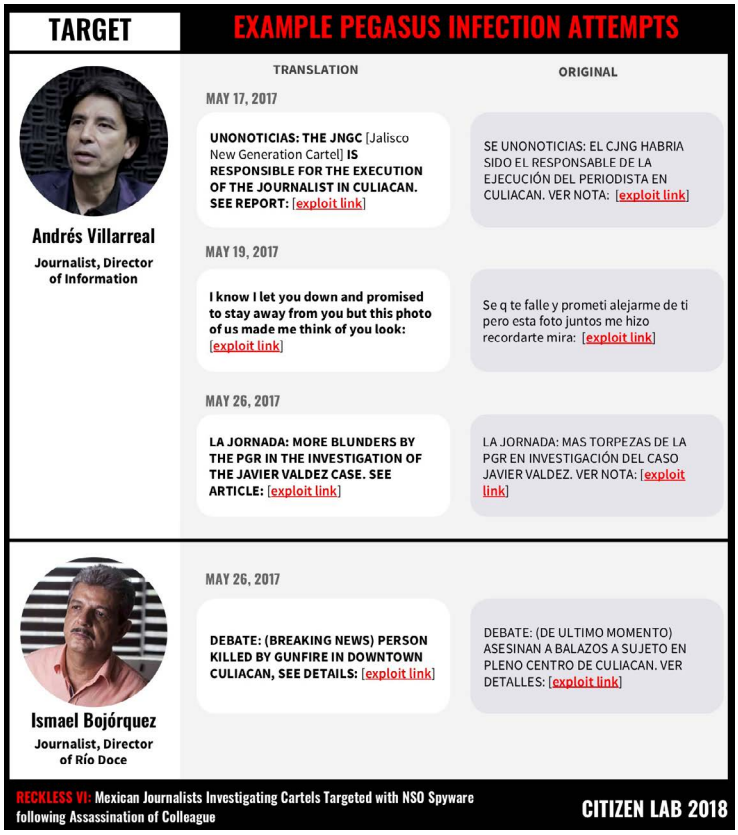

Figure 4: Example of Pegasus infection attempts beginning on May 17, 2017. Image credits: Noroeste, Parainfo 85.

The messages sent to both targets followed themes common to other cases of targeting. The messages were personalized and related to work or family issues including purportedly compromising romantic material, news alerts, and alarming billing notifications. The variation in content suggests that the operators were likely experimenting with different approaches as initial infection attempts failed.

According to the targets, immediately prior to the initial targeting on May 17th, 2017, representatives of the Criminal Investigation Agency (Agencia de Investigación Criminal), which is part of the Mexican Office of the Attorney General (Procurador

General de la República (PGR)), had arrived in Culiacán and was given responsibility for the investigation into the killing of Javier Valdéz. Importantly, although our recent research has identified multiple current and former Pegasus deployments in Mexico (and by implication, NSO Group customers), the PGR is the only entity publicly identified as an NGO Group customer.

Links to NSO Group's Exploit Infrastructure

The links in the messages sent to *Río Doce* staff point to previously reported NSO Group exploit infrastructure linked to the operator we call **RECKLESS-1**, which we discuss in detail in a recent investigation. The infrastructure associated with the RECKLESS-1 operator was active until June 2017, when we published a third report describing abuses, including the second in Mexico. While that infrastructure was disabled, our recent scanning results indicate that Mexican government-linked NSO Group operators have been active as recently as late September 2018.

Of the six messages analyzed as part of this report, several contained links shortened with bit.ly that unshortened to the exploit URLs, while others included links directly containing previously–identified NSO Group exploit domains.

banca-movil[.]net
animal-politico[.]com
savephotos[.]net

Table 1. NSO Group Pegasus Exploit Domains Used in this Operation

Based on prior Citizen Lab analysis of NSO Group exploit servers, we conclude that clicking on any of the links would have resulted in the silent infection of the device with Pegasus spyware.

A Pattern of Failed Oversight at NSO Group

Months after being publicly exposed, a suspected Mexican government-linked NSO Group client was sending infection attempts to the Andrés Villarreal and Ismael Bojórquez as they grieved the death of their colleague. Whatever pressure NSO Group may have felt after the initial reporting of abuses in Mexico, this customer continued to use Pegasus.[2] While there is very little publicly-available information

2 This is despite the fact that NSO Group has claimed that they maintain the ability to cancel existing agreements with customers.

on NSO Group's oversight practices, the continued use of Pegasus in Mexico suggests that their current procedures are problematic both substantively and in their implementation and application.

Claims of Oversight and Vetting

In February 2017, after the Citizen Lab published its second report on the use of Pegasus in Mexico, NSO Group stated to The New York Times that it sells only to law enforcement agencies for the purposes of tracking terrorists, criminals, and drug lords. The company claims to have "a strict vetting process" to determine which countries to sell to – a process which apparently included a "Business Ethics Committee" made up of employees and an outside counsel vetting potential government clients. Sources close to the company speaking to the media have stated that the committee makes decisions "based on human rights rankings set by the World Bank and other bodies." Executives have claimed, without presenting evidence, that they had pulled contracts after discovering human rights violations.

In September 2018, prior to the publication of another Citizen Lab report on NSO Group's Pegasus spyware, NSO Group reiterated that it "develops products that are licensed only to legitimate government agencies for the sole purpose of investigating and preventing crime and terror." The company also maintained that it operates in compliance with all applicable laws, including export control laws. It further stated that its product was only licensed to operate in countries approved under the "Business Ethics Framework". It elaborated further on the composition of the ethics committee, explaining that it included "outside experts from various disciplines" and that the committee reviews and approves each transaction and is authorized to reject or cancel agreements where there is improper use.

NSO Group's Repeated Failures of Oversight

The way NSO Group describes its oversight and vetting process is contradicted by the very indicators that they claim to take into account when determining whether or not to make a sale. Assuming that NSO Group was referring to the World Bank Worldwide Governance Indicators in its interview with *The New York Times*, Mexico ranks very poorly in issues like voice and accountability, rule of law, and control of corruption. Moreover, Mexico has an extremely poor human rights record, particularly in relation to journalists and freedom of the press.

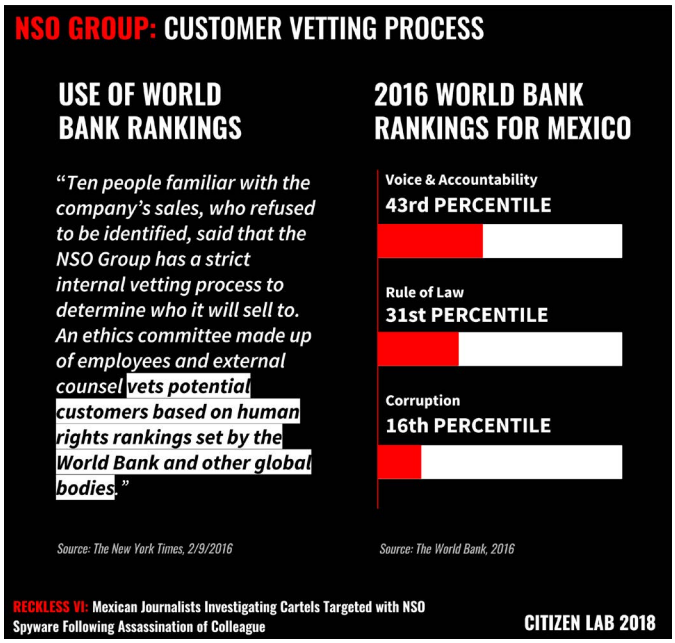

Figure 5: NSO Group claims about business ethics and customer vetting process contrasted with World Bank World Governance Indicators from 2016.

Without concrete information on the composition, mandate, and decision-making outcomes of the ethics committee, there is also no reason to believe that NSO Group's purported oversight committee is any different from what commercial spyware provider Hacking Team purported to have in place. Hacking Team's products regularly appeared in the hands of dictatorial regimes engaged in human rights abuses. When these abuses were discovered, Hacking Team would claim that it had a due diligence process in place. A review conducted by Human Rights Watch of internal emails from Hacking Team made it clear that these claims were largely for show and no rigorous process existed. Finally, the fact that NSO Group asserts that it follows Israeli export control laws is unhelpful in terms of ensuring that Pegasus is not used for repressive purposes when it appears that such licenses are granted to sell the product to countries with problematic human rights records, like the UAE.

This case is another demonstration of why spyware industry oversight mechanisms need to be articulated, transparent, and provide for a legitimate grievance process. These are principles included in the United Nations (UN) Guiding Principles on Business and Human Rights and reflect a global consensus on what companies need to be doing to ensure respect for human rights.[3]

3 In particular, see, for example, Principles 15, 16, and 31 of the UN Guiding Principles on Business and Human Rights.

Conclusion & Discussion

With this seventh publication on abuses of NSO Group spyware in Mexico, Citizen Lab and our partners R3D, SocialTic, and Article 19 have identified a total of 24 cases of abusive targeting by Mexico-linked NSO Group customers. Our previous investigations identified infection attempts against multiple journalists, lawyers, international investigators, public health practitioners, senior politicians, and anti-corruption activists.

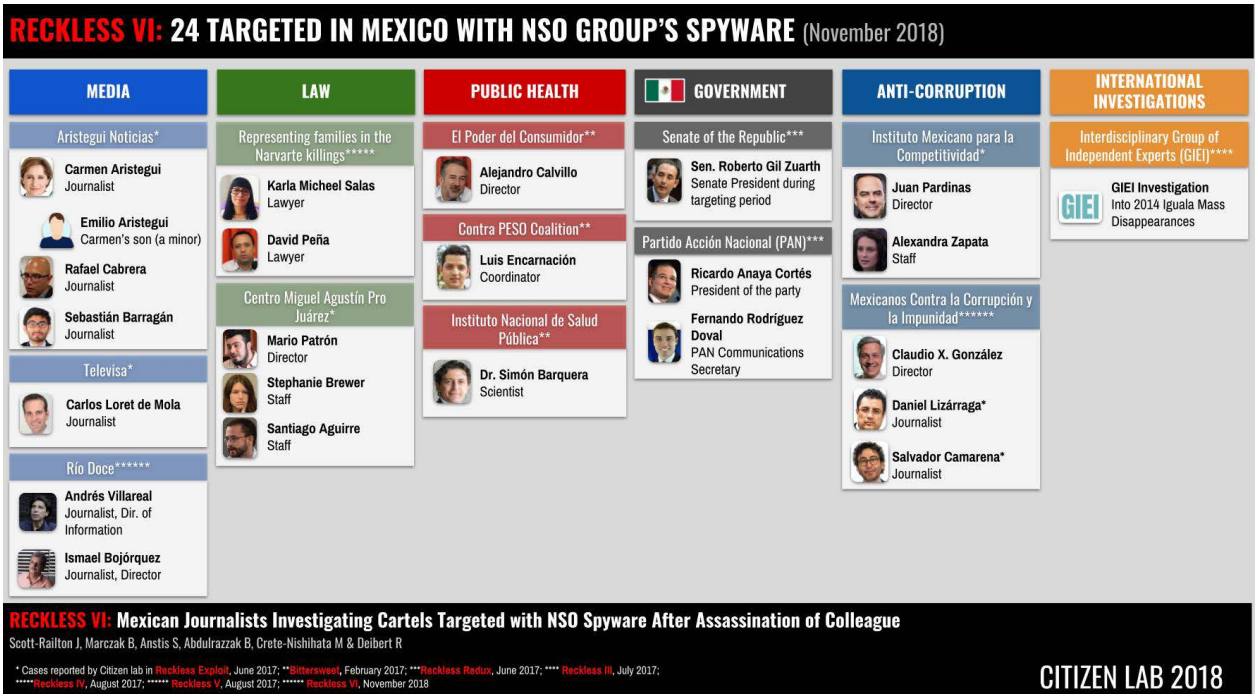

Figure 6: Targets of Mexican Government-linked Pegasus operators.

Taking into account other reporting, including work by Citizen Lab, Amnesty International, and Forbes, we count a total of **at least 28 targets** (where infection attempts have been confirmed) physically located in Canada, Mexico, the UAE, the United Kingdom and the United States.

While some Mexican operations, including RECKLESS-1, appear to have been disabled (or moved to new infrastructure) following a third report of abuses, published in June 2017, as recently as September 2018 we identified continuing evidence of multiple Pegasus operators that appear to be active in Mexico.

Pegasus: A Favoured Tool for Targeting Journalists

Journalists now stand out as a regular target for infection attempts with Pegasus around the world.

Pegasus spyware has been used to target journalists and civic media in Mexico, Canada, and the UK. In total, at least eight Mexican journalists are confirmed as having been targeted with Pegasus. In some cases, targets also included family members, such as the case of Carmen Aristegui, whose minor child was targeted while in boarding school in the United States.

Figure 7: Confirmed cases of journalists targeted with NSO Group's Pegasus spyware.

Other targets have been reported, but not confirmed, such as *New York Times* journalist Azam Ahmed who recalled receiving a similar message while working in Mexico. This case also demonstrates the deeply troubling intersection between digital and physical threats, such as those experienced by journalists in Mexico.

Journalists at Physical and Digital Risk in Mexico

Mexico is one of the most dangerous countries in the world in which to work as

a journalist.[4] Moreover, over half of the killings of journalists in Mexico have links suggesting some degree of official government involvement, according to a recent report. The lack of successful investigation into and prosecution of individuals responsible for killing journalists in Mexico has contributed to the perception that those who murder journalists enjoy relative impunity. Indeed, Mexico ranks very low in the World Press Freedom Index.[5]

The use of Pegasus spyware to target the colleagues of a slain journalist, similar to its use to target the lawyers in the Navarte killings, the investigations into the mass forced disappearances of 43 students from Ayotzinapa, as well as the lawyers representing the students' families, has another disturbing implication: Pegasus spyware might have been used by officials covertly trying to ascertain just how much victims' families, lawyers, and investigators knew about who was responsible for the crimes.

Troublingly, in multiple cases, individuals were targeted with Pegasus before or after the killing of a journalist with whom they had worked, or whose families they represented. While it is not yet possible to conclusively draw a link between those responsible for the murderous acts, and the use of Pegasus, the pattern highlights the potential nexus between digital and physical threats faced by journalists.

The use of Pegasus and other spyware to target journalists may have a chilling effect on reporting, grounded in fears that activities may be monitored. As one Ivory Coast journalist said, after reading about the possible use of NSO Group technology in his country, "[i]f journalists and their sources are realizing that they can be listened to without their knowledge, freedom of the press would be emptied of its contents."

Hollow Claims of Oversight

By the time that Andrés Villarreal and Ismael Bojórquez were targeted with Pegasus by RECKLESS-1 in May 2017, Citizen Lab had published two investigations (in August 2016 and February 2017) that made it clear that NSO Group's Pegasus spyware was being abused in Mexico. The operator that we identified in the February 2017 report was RECKLESS-1. We suspect (but cannot confirm) that the same operator

4 In 2017, 11 journalists were killed in Mexico and, in 2018, seven journalists and two citizen journalists were killed in Mexico according to Reporters Without Borders. The Committee to Protect Journalists noted that in 2017 the number of journalists killed in Mexico "reached a historical high." The International Press Institute called Mexico the "most deadly country for journalists" in 2017.

5 Mexico ranks 147th out of the 180 countries reviewed in the World Press Freedom Index.

was responsible for the targeting that we described in 2016.

After each case, NSO Group made public statements about due diligence and made claims about oversight. Yet, as this report makes clear, months later RECKLESS-1 was still engaging in abusive targeting.

When "cyber warfare" providers like NSO Group are presented with clear evidence of abuses, they promise to investigate, highlight their compliance with applicable laws, and make claims about taking into account human rights in their due diligence processes. NSO Group has boasted of being the "only company of its kind in the world" that has an independent ethics committee with outside experts in law and international relations. Sources "familiar with" NSO Group have claimed that the committee includes former United States government officials and human rights lawyers. NSO Group has also claimed to have terminated unspecified clients for unspecified abuses.

As we have repeated in numerous reports, this case – along with others we have previously reported on – raises serious doubts as to the actual oversight and human rights due diligence processes in place at NSO Group. Since our first report on NSO Group in 2016, NSO Group's Pegasus spyware continues to be used in connection with human rights abuses and the company appears to have failed to take steps to remedy this situation. That said, the lack of transparency in NSO Group oversight mechanisms makes it difficult to thoroughly assess what NSO Group has or has not done. This serves to further underline the importance of publicly articulated and transparent oversight mechanisms that also provide for a legitimate grievance process and are compliant with the UN Guiding Principles on Business and Human Rights.

Questions To Francisco Partners Go Unanswered

In November 2018, we asked Francisco Partners (a global private equity firm that invests in technology and which has a majority stake in NSO Group) to engage in a constructive dialogue regarding human rights due diligence processes and the UN Guiding Principles on Business and Human Rights. We also highlighted the many concerns raised by NSO Group's Pegasus. To date, we have received no response. Prior to the publication of this report we also invited NSO Group to comment on our findings and undertook to publish any response received by November 26th, 2018. Our request remains unanswered.

Appendix

Date	Target	Original Message	Translated Message	Link in Message	Unshortened Link (if applicable)
May 17, 2017	Andrés Villarreal	SE UNONOTICIAS: EL CJNG HABRIA SIDO EL RESPONSABLE DE LA EJECUCIÓN DEL PERIODISTA EN CULIACAN. VER NOTA: [malicious link]	UNONOTICIAS: THE JNGC IS RESPONSIBLE FOR THE EXECUTION OF THE JOURNALIST IN CULIACAN. SEE REPORT:[malicious link]	hxxp://bit[.]ly/2qwIhD8	hxxps://animal-politico[.]com/Ofxtu0W
May 19, 2017	Andrés Villarreal	Se q te falle y prometi alejarme de ti pero esta foto juntos me hizo recordarte mira: [malicious link]	I know I let you down and promised to stay away from you but this photo of us made me think of you look: [malicious link]	hxxps://savephotos[.]net/BLiWHNkEZ	
May 24, 2017	Andrés Villarreal	Has realizado un Retiro/Compra Tarjeta **** monto $21,750 M.N. Verifica detalles de operacion: [malicious link]	You made a withdrawal/purchase Card **** amount $21,750 M.N. Verify details of the transaction::[malicious link]	hxxps://banca-movil[.]net/IDIC3aO5	
May 26, 2017	Andrés Villarreal	LA JORNADA: MAS TORPEZAS DE LA PGR EN INVESTIGACIÓN DEL CASO JAVIER VALDEZ. VER NOTA: [malicious link]	LA JORNADA: MORE BLUNDERS BY THE PGR IN THE INVESTIGATION OF THE JAVIER VALDEZ CASE. SEE ARTICLE:[malicious link]	hxxp://bit[.]ly/2qjEM6q	hxxps://savephotos[.]net/e6N0RQ80
May 26, 2017	Ismael Bojórquez	DEBATE: (DE ULTIMO MOMENTO) ASESINAN A BALAZOS A SUJETO EN PLENO CENTRO DE CULIACAN. VER DETALLES: [malicious link]	DEBATE: (LAST MINUTE) PERSON IS MURDERED BY GUNFIRE IN CULIACAN DOWNTOWN: SEE DETAILS [malicious link]	hxxp://bit[.]ly/2qjLeu7	hxxps://animal-politico[.]com/CtkmZePR
May 26, 2017	Ismael Bojórquez	DEBATE: (DE ULTIMO MOMENTO) ASESINAN A BALAZOS A SUJETO EN PLENO CENTRO DE CULIACAN. VER DETALLES: [malicious link]	DEBATE: (BREAKING NEWS) PERSON KILLED BY GUNFIRE IN DOWNTOWN CULIACAN, SEE DETAILS: [malicious link]	hxxp://bit[.]lly/2qjLeu7	hxxps://animal-politico[.]com/CtkmZePR