RECKLESS VII

Wife of Journalist Slain in Cartel-Linked Killing Targeted with NSO Group's Spyware

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

MARCH 20, 2019
RESEARCH REPORT #117

munk school
OF GLOBAL AFFAIRS & PUBLIC POLICY

UNIVERSITY OF TORONTO

THECITIZENLAB

Copyright

Document Version: 1.0

Suggested Citation

John Scott-Railton, Bill Marczak, Siena Anstis, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert. "Reckless VII: Wife of Journalist Slain in Cartel-Linked Killing Targeted with NSO Group's Spyware," Citizen Lab Research Brief No. 117, March 2019.

Acknowledgements

Citizen lab would like to thank Griselda Triana for consenting to share this case with the collaborating organizations, especially Article 19, 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 particular case.

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

This report is Part 8 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

This research brief details how Griselda Triana, journalist and the wife of slain journalist Javier Valdez Cárdenas, was targeted with NSO Group's Pegasus spyware in the days after his killing.

Key Findings

- **Griselda Triana, a journalist and the wife of slain journalist Javier Valdez, was targeted with NSO Group's Pegasus spyware following his assassination.**
- **Triana was targeted a week after infection attempts against two of Valdez's colleagues, Andrés Villarreal and Ismael Bojórquez.**
- **A total of 25 individuals are now known to have been abusively targeted with Pegasus malware in Mexico.**

Introduction

On May 15th, 2017, journalist Javier Valdez was shot dead as he left the offices of *Riodoce*, the newspaper that he founded to investigate cartels and organized crime in Sinaloa, Mexico. His killers pulled him from his car, shot him a dozen times, and stole his files, laptop, and mobile phone. His killing has been widely reported as a cartel hit.

In the days following the killing, his colleagues Andrés Villarreal and Ismael Bojórquez received carefully crafted text messages designed to trick them into clicking on exploit links. Clicking on the links would have infected their phones with Pegasus spyware. The spyware, developed by Israeli company NSO Group, is designed to infect and remotely monitor mobile phones. In that investigation, we linked the infection attempts to a group that we call RECKLESS-1, which we linked to the Mexican government.

Figure 1: Javier Valdez Cárdenas (left)[1]. On May 15, 2017, Cárdenas was shot 12 times as he left the Ríodoce offices. Griselda Triana (right) at a march demanding justice for Javier Valdez.

With the assistance of our investigative partners R3D, SocialTic, and Article 19, we can now report that, one week after Javier Valdez Cárdenas was murdered, his wife, journalist Griselda Triana, was also targeted with multiple infection attempts using NSO Group's Pegasus malware.

1 Image credit: Cronica de Xalpa. Image courtesy of Griselda Triana.

Figure 2: The 25 known targets with Pegasus in Mexico as of March 2019.

Javier Valdez's colleagues were among more than two dozen Mexican and American citizens targeted with Pegasus spyware by Mexican NSO Group customers. After we identified infection attempts[2] against a Mexican journalist and government critic in 2016, Mexican civil society groups R3D, SocialTic, and Article 19 began collaborating with us to identify additional targets. This investigative partnership resulted in seven reports detailing 25 infection attempts against multiple Mexican journalists, lawyers, international investigators, public health practitioners, senior politicians, and anti-corruption activists.

The Targeting of Griselda Triana with NSO Group's Spyware

Griselda Triana has produced and hosted the show "La otredad" (English: "Otherness") for the radio station of the Autonomous University of Sinaloa (UAS). Triana has also served as communications director for the Centre for Gender Policy and Equity Between Men and Women at UAS.

On May 25th and 26th, 2017, eleven days after her husband was slain, Triana received text messages designed to trick her into clicking on malicious links. The messages

2 We believe that the operator in this first case is RECKLESS-1, however we are unable to say so conclusively due to technical limitations.

arrived during a period when she recalls actively cooperating with the authorities investigating his killing, and publicly protesting his death and demanding a serious official investigation.

The first infection attempt arrived on May 25th and masqueraded as an update about the killing from Mexican news magazine *Proceso*. According to the message, the Mexican Office of the Prosecutor (PGR) had announced that his assassination was in fact an attempted carjacking. The idea was farcical and Triana did not click on the link.

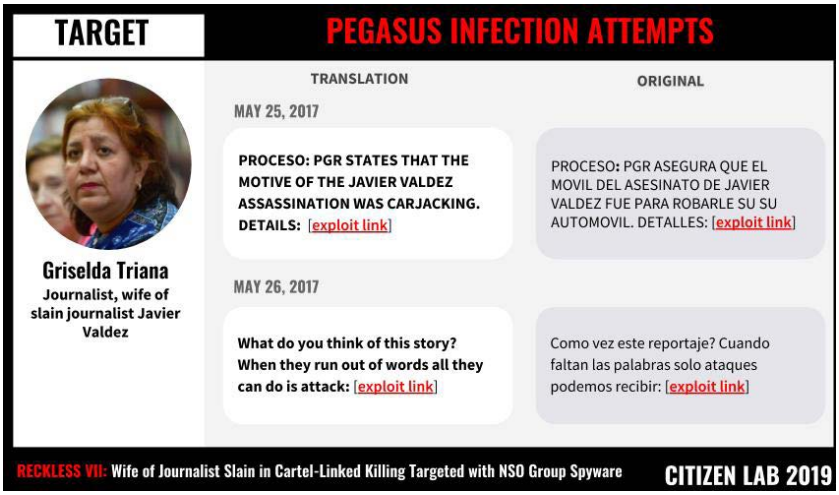

Figure 3: Infection Attempts using Pegasus spyware against Griselda Triana.

A day later, Triana received a second infection attempt. The message played on her grief at the loss of her husband and hinted that she might have been attacked in the press. Again, she recalls abstaining from clicking.

Clicking on the links in either message would have resulted in the infection of her phone with NSO Group's Pegasus spyware. Griselda later provided the messages to Article 19 and R3D, who shared them with Citizen Lab researchers.

Links to NSO Group Exploit Infrastructure

The links in the messages sent to Griselda Triana pointed to domains identified in prior Citizen Lab investigations as exploit infrastructure operated by RECKLESS-1. Both domains had been previously used to target Javier Valdez's colleagues (See: Table 1).

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

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

In our recent publications on RECKLESS-1 and other NSO Group operators, we reported that the operator was active until June 2017, when we published a third report describing abuses of Pegasus in Mexico and pointed to further evidence indicating that the operator was the Mexican government.

While the original RECKLESS-1 infrastructure was not re-enabled, our recent scanning results indicate that Mexican government-linked NSO Group operators have been active as recently as late September 2018.

Conclusion: Journalists in the Spyware Crosshairs

There is an undeniable pattern of abuse and due diligence failures in how NSO Group's spyware is sold and used. By the time Griselda Triana was targeted in May 2017, Mexican NSO customers had already targeted at least two dozen members of Mexican civil society with Pegasus. By then, NSO Group had already been made aware of public reports of the misuse of its products by Mexico for almost eight months. This public reporting included multiple publications by Citizen Lab and multiple front page *New York Times* stories.

The targeting of Griselda Triana increases the number of Mexican journalists targeted with Pegasus to nine and the total number of Mexican targets to 25. Taking into account investigations by Citizen Lab and Amnesty International on a Saudi Arabian government operator, there are now 11 publicly-reported cases of journalists targeted with Pegasus spyware (Figure 4). The number increases if family members, such as the minor child of Carmen Aristegui who was targeted while at boarding school in the United States, are included.

The repeated use of Pegasus to target journalists and their family members over multiple years suggests a pattern of official abuse. In Mexico, journalists appear more frequently among Pegasus targets than any other group that we have identified, such as politicians or lawyers (See: Figure 2). This pattern is disturbing as Mexican journalists are also frequent targets for physical violence and assassination.

Figure 4: Journalists and civic media targeted with NSO Group's Pegasus Spyware.

A degree of official involvement has been reported in half the killings of journalists in Mexico, making it especially troubling that family members and colleagues of a slain journalist were digitally targeted by a Mexican government-linked entity.

Questions about Abuses to NSO Group and Novalpina Capital Remain Unanswered

Citizen Lab has sent multiple communications to NSO Group, its financial partners, and its backers. These have included letters laying out our findings along with specific questions about individual cases. We have also asked questions about oversight and due diligence. These questions have largely gone unanswered.

Citizen Lab has also written to Novalpina Capital, a UK-based private equity fund directed by Stephen Peel. Novalpina is currently in the process of purchasing a majority stake in NSO Group. Unfortunately, Novalpina Capital has also chosen to not address the many cases of abuse identified by Citizen Lab, Amnesty International, and others.

For example, Novalpina recently wrote a letter to civil society groups stating their commitment to human rights and transparency in the spyware market and outlining their plans for NSO. Unfortunately, Novalpina's 11 page letter spends only

two paragraphs addressing, and then dismissing, the nearly three years of reports connecting NSO Group to specific abuses.

Citizen Lab has also written to Jefferies Financial Group, which is reportedly "advising and leading the financing" of the acquisition of NSO Group by Novalpina. That letter has not received a response.

Appendix A: Full List of Messages

Date	Original Message	Translation	Link	Unshortened Link (if applicable)
May 25th 2017	PROCESO: PGR ASEGURA QUE EL MOVIL DEL ASESINATO DE JAVIER VALDEZ FUE PARA ROBARLE SU SUTOMOVIL. DETALLES:	PROCESO: PGR STATES THAT THE CELLPHONE OF ASSASSINATION VICTIM JAVIER VALDEZ WAS STOLEN FROM HIS AUTOMOBILE	http://bit[.]ly/2r1gawm	https://savephotos[.]net/eGd8iDIHg
May 26th 2017	Como vez este reportaje? Cuando faltan las palabras solo ataques podemos recibir:	What do you think of this story? Sometimes when words can't be found, all you can do is attack:	https://animal-politico[.]com/5C6FIWAJ	