# New Pegasus Spyware Abuses Identified in Mexico - The Citizen Lab



## Key Findings

- The Citizen Lab provided technical support for R3D's analysis and validated the infections.
- Victims include two journalists that report on issues related to official corruption and a prominent human rights defender.
- Opposition politician Agustín Basave Alanís was also infected with Pegasus spyware in 2021.
- The infections occurred years after the first revelations of Pegasus abuses in Mexico.
- Mexican digital rights organization R3D (Red en los Defensa de los Derechos Digitales) has identified Pegasus infections against journalists and a human rights defender taking place between 2019-2021.
- They also occurred after Mexico's current President, Andrés Manuel López Obrador, assured the public that the government no longer used the spyware and that there would be no further abuses.

**Note**: Report updated on October 19, 2022 to add the additional case of Mexican opposition politician Agustín Basave Alanís (see: "**October 19, 2022 Update: Agustín Basave Alanís**," below).

Click here to read the full R3D report.

## Background

In 2017, the Citizen Lab, along with partners R3D, SocialTic and Article19, released a series of eight reports on widespread Pegasus targeting in Mexico. Many sectors of Mexican civil society were targeted, including investigative journalists and lawyers for cartel victims' families, anti-corruption groups, prominent lawmakers, international investigators examining enforced disappearances, and even the spouse of a journalist killed in a cartel slaying.

A public scandal ensued when the Pegasus targeting was first revealed, resulting in extensive scrutiny into the surveillance practices of Mexican authorities, and especially prosecutors. A still-ongoing criminal investigation was also opened in Mexico.

In 2021, as part of the Pegasus Project revelations (a collaboration between Forbidden Stories, Amnesty International's Security Lab, and a coalition of media organizations), it was reported that at least 50 people in the circle of Andrés Manuel López Obrador, Mexico's current president, were among individuals potentially selected for surveillance with Pegasus between 2016-2017. The targets included the now-President's children and spouse. The same report indicated that at least 45 Mexican governors and former governors may have been similarly selected for surveillance.

The Pegasus Project also found that a wide swath of Mexican civil society, from teachers to journalists, lawyers and international investigators examining enforced disappearances, may have been selected for surveillance.

In 2019, after taking power, López Obrador assured Mexicans in a televised press conference that there would be no more Pegasus abuses in Mexico:

"*We are not involved with that. Here we decided that there would not be any persecution against anyone. When we were in the opposition we were spied on (…) now that is prohibited. We have not purchased systems for interceptions, among other things because of the corruption that was involved in the purchase of all of this equipment at very elevated prices, to foreign companies, spy systems, a lot of money was spent, there is still unused equipment purchased in the previous government. We don't do that. And we don't do it because it is a matter of principle*". [informal translation]

In 2021, Mexico's president reiterated his claim that the Mexican government was not spying with Pegasus, saying in response to a question: *"This does not happen. The government does not spy on anyone."* [informal translation]

The latest findings by R3D indicate that Pegasus abuses continued in Mexico. Their report also highlights evidence of recent contracts between Mexico's Secretary of National Defense (SEDENA), and companies linked to prior sales of Pegasus to the Mexican government.

## New Findings

R3D, with technical support from the Citizen Lab, has determined that Mexican journalists and a human rights defender were infected with Pegasus between 2019 and 2021.

These cases differ from previous findings in two important ways:

- We validate the 2019-2021 Pegasus infections using forensic analysis of artifacts collected from devices. Prior Citizen Lab findings in Mexico only confirmed Pegasus targeting (as evidenced by a malicious message sent to a device).
- The 2019-2021 infections leveraged zero-click attacks: no deception was required to trick victims into clicking. The Citizen Lab's previous reports on Mexican cases found malicious text messages designed to trick targets into clicking on a link that would trigger an infection.

Our technical validation of forensic artifacts collected from the devices of these individuals with their consent leads us to conclude with high confidence that:

- Human rights defender Raymundo Ramos was hacked with Pegasus at least three times between August and September 2020.
- Journalist and author Ricardo Raphael was hacked with Pegasus at least three times in October and December 2019, and again in December 2020. He was also previously targeted and infected in 2016, and targeted in 2017.
- An anonymous journalist from prominent online media outlet Animal Politico was hacked in June 2021.

Further details for each case are provided in Appendix A.

We assess with high confidence that these individuals were hacked with Pegasus spyware. The technical data available for these recent cases (2019-2021) does not enable us to attribute the hacking to a particular NSO Group customer at this time. However, each of the victims would be of intense interest to entities within the Mexican government and in some cases, troublingly, to cartels.

## Hacking Timeframe

The report published by R3D provides helpful context for understanding the potential triggers for Pegasus targeting and infections, which we summarize here:

**Raymundo Ramos Vázquez**

Ramos has spent years documenting human rights violations committed by the Mexican Army and Navy in the state of Tamaulipas:

- Ramos was infected with Pegasus in August and September 2020. R3D found that the infections occurred after the publication of a video showing the extrajudicial killing of civilians by the Mexican army in Tamaulipas. Ramos had spoken to the media about the case.
- During the timeframe of the targeting, Ramos was meeting with representatives of the Office of the United Nations High Commissioner for Human Rights (OHCHR), Mexico's National Human Rights Commission (CNDH), officials from Mexico's Navy and Secretary of Defense, and members of the media.

**Ricardo Raphael**

Raphael, a prominent journalist and author who focuses on themes including official corruption and the nexus between the Mexican government and cartels, was extensively targeted and infected with Pegasus spyware:

- Raphael was first targeted and infected 2016, and again targeted in 2017 during a period of critical reporting on investigations into the Iguala Mass Disappearances (the 43 students disappeared in Ayotzinapa in 2014).
    - We attribute the 2017 targeting to an operator that we call ***RECKLESS-1***, which also targeted the spouse and colleagues of an assassinated Mexican journalist, as well as Mexican public health researchers. Circumstantial evidence connects ***RECKLESS-1*** to the Mexican Government, as the operator was spying exclusively in Mexico.
- In 2019, he was repeatedly infected with Pegasus while on tour for a book that provides a fictionalized account of Los Zetas Cartel and its origins in the Mexican Army.
- In 2020, he was infected after writing on extrajudicial detentions and official impunity, such as this *Washington Post* editorial. Not long before he was infected in December 2020, he had accused Mexico's Attorney General of serious misconduct in their investigation of the Iguala Mass Disappearances case. This critique was cited by prominent news outlet *Aristegui Noticias* the day prior to the hacking.

According to the R3D report, Raphael stated that, in 2022, snippets of a private communication were taken out of context and shared with his contacts in an apparent effort to discredit him.

**Anonymous Journalist at Animal Politico**

Animal Politico is a prominent online news website that reports on themes such as official corruption, extrajudicial killings, and accountability:

- A journalist at the outlet was infected on the same day they published a report on human rights violations by the Mexican Armed Forces.

**October 19, 2022 Update: Agustín Basave Alanís**

On October 18, 2022, we publicly confirmed that an analysis of forensic indicators from the device of Mexican opposition lawmaker Agustín Basave Alanís identified a Pegasus spyware infection occurring sometime between 2021-09-05 and 2021-09-11. Basave, a member of the Chamber of Deputies, is secretary of the Citizen Security Commission, and belongs to the Movimiento Ciudadano party ("Citizens' Movement"). Reporting by *Reuters* notes that Basave is close to Luis Donaldo Colosio Riojas, who is viewed as a potential presidential candidate for 2024. A report by R3D indicates that the infection timeframe coincides with a visit by Colosio Riojas to the Chamber of Deputies.

## Need for an Independent Investigation

These latest cases, which come years after the first revelations of problematic Pegasus targeting in Mexico, illustrate the abuse potential of mercenary spyware in a context of flawed public accountability and transparency. Even in the face of global scrutiny, domestic outcry, and a new administration that pledged to never use spyware, the targeting of journalists and human rights defenders with Pegasus spyware continued in Mexico.

## Appendix: Victim Details

### Pegasus Victim: Raymundo Ramos

Analysis of forensic indicators collected from the device of human rights defender Raymundo Ramos shows that it was infected with the KISMET zero-click exploit on or around:

- 2020-08-28
- 2020-09-02
- 2020-09-03

### Pegasus Victim: Ricardo Raphael

An analysis of forensic indicators from journalist Ricardo Raphael's phone indicates that he was hacked three times with what we refer to as the HOMAGE zero-click exploit in 2019, on or around:

- 2019-10-30
- 2019-11-07
- 2019-11-16

Raphael was then hacked with a different zero-click exploit on or around:

- 2020-12-27

Analysis of Raphael's device also found evidence of prior Pegasus hacking and targeting as far back as 2016.

Raphael was first targeted on **May 26, 2016** via a Pegasus SMS:

**Date**: 26 May 2016
**From**: +525572778337Tomar justicia x propia mano es prueba del Edo. fallido y la crisis institucional, este video es prueba ello hxxp://bit[.]ly/1sB5xiP (Translation:
Taking justice by one's own hand is proof of a failed state and an institutional crisis, this video is proof of that [malicious link])

The URL, which is shortened with bit.ly, redirects to the Pegasus infection domain hxxps://network190[.]com/5557819s/.

This targeting resulted in a persistent Pegasus infection.

Raphael was **again, twice, targeted via SMS in 2017**. We found no evidence that this targeting resulted in successful infections.

**Date:** 22 February 2017
**From:** +523338200726Mi estimado Ricardo hoy publique mi columna en 24 horas, esperando tu mejor opinion saludos: hxxp://bit[.]ly/2lM9jqp (Translation:
Dear Ricardo, my column was published today in 24 Horas, I'd love your opinion, greetings: [malicious link])

The URL redirects to hxxps://notisms[.]net/bNBzPerL. The domain notisms[.]net was part of NSO Group's Pegasus infection infrastructure when the message was sent. We link the domain notisms[.]net to the operator we call ***RECKLESS-1***, which we link to the Mexican Government.

**Date:** 24 February 2017
**From:** +522222607851Has realizado un Retiro/Compra Tarjeta **** monto $23,500.00 M.N. Verifica detalles de operacion: hxxps://banca-movil[.]net/Fy9yZJUR (Translation:
You have made a withdrawal /purchase Card **** amount $23,500.00 M.N. Verify transaction details: [malicious link])

The domain banca-movil[.]net was also part of NSO Group's Pegasus infection infrastructure when the message was sent. We link the domain banca-movil[.]net to the operator we call ***RECKLESS-1***, which we link to the Mexican Government.

## Pegasus Victim: Anonymous Journalist from Animal Politico

Analysis of forensic indicators collected from the device of a journalist who prefers to remain anonymous shows that it was infected once with the FORCEDENTRY zero-click on or around:

- 2021-06-10

---