Project Torogoz

Extensive Hacking of Media & Civil Society in El Salvador with Pegasus Spyware

By John Scott-Railton, Bill Marczak, Paolo Nigro Herrero, Bahr Abdul Razzak, Noura Al-Jizawi, Salvatore Solimano, and Ron Deibert

JANUARY 12, 2022
RESEARCH REPORT #148

munk school
OF GLOBAL AFFAIRS & PUBLIC POLICY
UNIVERSITY OF TORONTO
THECITIZENLAB

Copyright

Document Version: 1.0

Suggested Citation

John Scott-Railton, Bill Marczak, Paolo Nigro Herrero, Bahr Abdul Razzak, Noura Al-Jizawi, Salvatore Solimano, and Ron Deibert. "Project Torogoz: Extensive Hacking of Media & Civil Society in El Salvador with Pegasus Spyware," Citizen Lab Research Report No. 148, University of Toronto, January 2022.

Acknowledgements

We thank and acknowledge the many individuals that allowed us to analyze their devices as part of this investigation.

Special thanks to Mohammed Al-Maskati from Frontline Defenders for invaluable assistance.

Special thanks to the staff and incident handlers at the Access Now helpline for their invaluable support to this process and assistance to victims.

Special thanks to all of the organizations participating in this investigative collaboration including SocialTIC and Fundación Acceso.

Thanks to Siena Anstis, Celine Bauwens, Miles Kenyon, Adam Senft, and Mari Zhou for review, copy editing, and publication support.

Special thanks to TNG for invaluable assistance on this project.

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

The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs & 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

Proyecto Torogoz: Hackeo extensivo de los medios de comunicación y la sociedad civil en El Salvador con el programa espía Pegasus

Key Findings

- **The Citizen Lab and Access Now have conducted a joint investigation into Pegasus hacking in El Salvador in collaboration with Frontline Defenders, SocialTIC, and Fundación Acceso.**
- **We confirmed 35 cases of journalists and members of civil society whose phones were successfully infected with NSO's Pegasus spyware between July 2020 and November 2021. We shared a sample of forensic data with Amnesty International's Security Lab which independently confirms the findings.**
- **Targets included journalists at *El Faro*, *GatoEncerrado*, *La Prensa Gráfica*, *Revista Digital Disruptiva*, *Diario El Mundo*, *El Diario de Hoy*, and two independent journalists. Civil society targets included *Fundación DTJ, Cristosal*, and another NGO.**
- **The hacking took place while the organizations were reporting on sensitive issues involving the administration of President Bukele, such as a scandal involving the government's negotiation of a "pact" with the MS-13 gang for a reduction in violence and electoral support.**
- **While evidence linking a particular infection to a particular Pegasus customer is often unavailable, in this case we identified a Pegasus customer operating almost exclusively in El Salvador since at least November 2019 that we call TOROGOZ, and have connected this operator to an infection attempt against *El Faro*.**

1. Introduction

This report describes the results of a collaborative investigation into the abuse of NSO Group's Pegasus spyware to target members of the press and civil society in El Salvador. The investigation led to the identification of 35 Pegasus-infected individuals (37 devices) among members of El Salvador's media and civil society.

Our investigation began in September 2021 when a group of independent journalists contacted Access Now's Digital Security Helpline after testing their devices using the Amnesty International Security Lab's Mobile Verification Toolkit (MVT) tool to detect Pegasus spyware.

The resulting investigation was a collaboration between the Citizen Lab and Access Now, with investigative assistance and case referrals from Frontline Defenders, SocialTIC, and Fundación Acceso. We asked Amnesty International's Security Lab to conduct an independent review of our analysis for a sample of cases, and they have confirmed our findings.

Repression and Impunity in El Salvador

Like most central American countries, El Salvador has had a troubled history marked by authoritarianism, endemic civil war and numerous coups, official and clandestine foreign intelligence and military assistance (particularly during the Cold War), organized crime, corruption, and drug trafficking.

Between 1970 and 1992, the country was ravaged by the Salvadoran Civil War, fought between a right-wing military junta and a coalition of left-wing guerilla groups under the umbrella of the Farabundo Martí National Liberation Front (FMLN). The era was characterized by frequent extra-judicial killings, mass disappearances and massacres of civilians, and numerous other human rights abuses, many of which were undertaken by “death squads” (some of whom were reportedly supported and trained by United States military advisors).

This period of violence and authoritarianism left a deep legacy of impunity and a tradition of corruption in El Salvador’s armed forces and political establishment. The period also created opportunities for organized crime and corruption, as well as the growth of poorly regulated and unaccountable private security firms.

The Bukele Administration

El Salvador's current president is the charismatic 40 year old Nayib Bukele, who has been in office since winning the general election in June 2019. Bukele was formerly mayor of Nuevo Cuscatlán (2012-15) and mayor of San Salvador (2015-18). In both cases he represented leftist parties. Although Bukele represents an aesthetic break with the typical Latin American autocrat, and despite his many public denouncements against strongmen, he has shown growing autocratic tendencies.

In February 2020, Bukele entered the legislative assembly accompanied by soldiers and armed guards in an attempt to intimidate lawmakers into approving his platform. In May 2021, Bukele and his supporters in the legislature fired the country’s attorney general and several judges, in a move that Bukele described as "cleaning our house." Bukele was elected on a platform that included a plan to reduce the extraordinary violence in the country by encouraging cooperation between the country’s armed forces and organized criminal gangs.

Although official murder counts have declined in recent years, a 2021 report by the Foundation of Studies for the Application of Law (Fundación de Estudios para la Aplicación del Derecho, or FESPAD) found that pacts between gangs and state officials, originally intended to lower homicide rates, have instead increased the recurrence of forced disappearances. FESPAD found several unidentified mass graves in areas with the highest gang presence. While forced disappearances allow gangs to execute with impunity, Bukele’s administration also undertakes brutal crackdowns against imprisoned gang members across the country.

Unlike many past authoritarians, Bukele blends a particular fluency in social media and dexterity in the use of memes, with the use of large popular public events to capitalize on popular disenchantment with traditional political parties. A recent analysis described Bukele as embodying a new type of "millennial authoritarianism," defined as "a distinctive political strategy that combines traditional populist appeals, classic authoritarian behavior, and a youthful and modern personal brand built primarily via social media."

The State of Police and Private Security Firms

The policing of gang violence within a context of generalized insecurity in El Salvador warrants special attention. In 2019, President Bukele authorized the intervention of armed forces in police duties, resulting in numerous human rights concerns, as highlighted in a 2020 State Dept. Human Rights report. At present, Salvadorans are concurrently subjected to both gang violence and aggressive, authoritarian policing. The threat of violence has led to unprecedented internal displacement. In 2017 alone, 296,000 Salvadorans were forced to move out of their homes due to the threat of violence.

Approximately 450 private security firms are operating illegally in El Salvador, often due to a failure to obtain or renew proper authorization and paperwork. Salvadoran police claim to be unable to hold these firms accountable. As of 2016, roughly 24,100 private security guards were active in El Salvador, an estimate that dwarfs the number of active police officers.

With private security firms and militia lacking proper oversight, El Salvador's Private Security Services Law does little to solve the problem, as noted by Freedom House. Article 47 of this law indicates that severe offenses attributed to private security services must be sanctioned with a financial penalty on salaries, but the exact nature of the fine is vague. This gap leaves police forces unable to hold private security firms accountable for their conduct. *La Prensa Gráfica* has found that not a single private security firm has been held accountable. Instances where police did come close to sanctioning a firm were later dropped in court.

This lack of accountability is troubling in light of accounts that Mara Salvatrucha (MS-13) gang members have infiltrated private security firms to extort Salvadoran citizens. Indeed, extortion has been on the rise since the Salvadoran government struck a deal with gang leaders. Salvadoran police have also had trouble keeping their own personnel in check. For example, a 2017 *Insight Crime* report shows that while some police officers have been jailed for illegal smuggling of items into jail cells, others, accused of extrajudicial killings, remain free.

Salvadoran Media under Threat

While there is a lively press in El Salvador, with outlets such as *El Faro* and *Revista Factum* providing regular critical coverage, journalists face numerous challenges in the country.

Reporters Without Borders ranks El Salvador 82nd in its 2021 World Press Freedom Index (an eight-place drop since 2020). Freedom House ranks El Salvador's freedom and independence of media as "partially free" and highlights rampant corruption, censorship, and interventions such as barring access to journalists at homicide scenes. Both *El Faro* and *Revista Factum* have also been frequently barred from accessing government conferences. The Freedom House report also notes verbal attacks directed at the press by Bukele himself. For example, in September 2020, Bukele used two hours of national airtime to denigrate and accuse the media of being his enemies.

Verbal attacks and threats against the press are not limited to Bukele. In September 2021, Javier Argueta, Nayib Bukele's legal counsel, threatened two journalists at *GatoEncerrado* for reporting on a meeting he held with four members of the Salvadoran Supreme Electoral Court. In a Twitter diatribe, Argueta threatened legal action if the journalists did not reveal their sources.

In 2021 alone, the Journalists Association of El Salvador (APES) recorded more than 200 cases of aggression against journalists, ranging from denial of access to harassment. Instances of animosity toward the press have involved state ministers and legislators, as well as executives of El Salvador's Autonomous Executive Port Commission (CEPA), all found to have verbally abused reporters. June and July 2021 press releases from APES denounced abuses by members of the Supreme Court of Justice, Bukele's Office and the Ministry of Security and Justice. In addition, a 165% increase in aggressions against female journalists, recorded last year, also characterizes El Salvador's endemic problem of media repression.

The TOROGOZ Pegasus Operator and El Salvador

Through our ongoing Internet scanning and DNS cache probing, we identified a Pegasus operator focusing almost exclusively within El Salvador that we named ***TOROGOZ***. We first observed this operator in early 2020, though the domain names associated with the operator appear to have been registered as early as November 2019.

In a 2020 report *Running in Circles*, we identified a Salvadoran client of Circles, an NSO Group-affiliated company. The Circles system, which is an entirely separate product and uses different technology than Pegasus, allows its operator to track locations of phones around the world, and to intercept unencrypted SMS messages and phone calls in some cases. Unlike Pegasus, use of the Circles system does not involve hacking target devices, and instead involves attacks against the mobile phone signaling system. The forensic artifacts analyzed in this report have no relationship to Circles technology.

While there is no conclusive technical evidence that ***TOROGOZ*** represents the Salvadoran government, the strong country-specific focus of the infections suggests that this is very

likely. Additionally, in the single case of hacking in this investigation in which we recovered the domain names of the Pegasus servers used, the ***TOROGOZ*** operator was implicated.

2. Findings: Salvadoran Pegasus Targeting

Following the Citizen Lab's research and technical protocols, the Citizen Lab and Access Now obtained forensic artifacts, including logs, from each target's device. With their consent, we analyzed the logs for forensic signatures associated with NSO Group's Pegasus spyware.

We conclude that at least 35 individuals from media organizations *El Faro*, *GatoEncerrado*, *La Prensa Gráfica*, *Revista Digital Disruptiva*, *Diario El Mundo*, *El Diario de Hoy,* and two independent journalists were hacked with Pegasus. We also identified hacking against civil society organizations in El Salvador, including Fundación DTJ, Cristosal, and another NGO.

The infections described in this report have been identified with high confidence and a sample of the cases have been peer reviewed by Amnesty's Security Lab. Their peer review supports our finding of Pegasus infections.

Confirmed Targets[1]

Our forensic analysis focuses on determining whether specific processes or binaries linked to NSO Group's Pegasus spyware were running on the phone in question during a specified time. The forensic analysis involves both searching records of execution maintained by the phone, as well as searching for other traces associated with the execution or installation of Pegasus. See **Appendix A** for a full list of dates that exploits were fired at the phones resulting in successful hacking.

Pegasus attempts to delete evidence of its successful exfiltration, so evidence establishing exfiltration may not be available in all cases. This should not be interpreted as suggesting that exfiltration did not take place.

Target	Affiliation	Forensic Finding
Noah Bullock	Cristosal	Pegasus infection
(Individual #1)	Diario El Mundo	Pegasus infection
Ricardo Avelar	El Diario de Hoy	Pegasus infection
Ana Beatriz Lazo	El Faro	Pegasus infection
Carlos Dada	El Faro	Pegasus infection
Carlos Ernesto Martínez D'aubuisson	El Faro	Pegasus infection
Daniel Lizárraga	El Faro	Pegasus exfiltration

1 Whereas a number of targets preferred to remain anonymous, the other targets consented to be identified.

Target	Affiliation	Forensic Finding
Daniel Reyes	El Faro	Pegasus infection
Efren Lemus	El Faro	Pegasus exfiltration
Gabriel Labrador	El Faro	Pegasus exfiltration
Gabriela Cáceres	El Faro	Pegasus infection
José Luis Sanz	El Faro	Pegasus exfiltration
Julia Gavarrete (Phone #1)	El Faro	Pegasus exfiltration
Julia Gavarrete (Phone #2)	El Faro	Pegasus infection
María Luz Nóchez	El Faro	Pegasus exfiltration
Mauricio Ernesto Sandoval Soriano	El Faro	Pegasus exfiltration
Nelson Rauda	El Faro	Pegasus infection
Óscar Martínez	El Faro	Pegasus exfiltration
Rebeca Monge	El Faro	Pegasus infection
Roman Gressier	El Faro	Pegasus exfiltration
Roxana Lazo	El Faro	Pegasus exfiltration
Sergio Arauz	El Faro	Pegasus exfiltration
Valeria Guzmán	El Faro	Pegasus infection
Víctor Peña	El Faro	Pegasus infection
(Individual #2)	El Faro	Pegasus infection
(Individual #3)	El Faro	Pegasus exfiltration
Jose Marinero	Fundación DTJ	Pegasus infection
Xenia Hernandez	Fundación DTJ	Pegasus infection
Beatriz Benitez	GatoEncerrado	Pegasus exfiltration
Ezequiel Barrera	GatoEncerrado	Pegasus exfiltration
Xenia Oliva (Phone #1)	GatoEncerrado	Pegasus exfiltration
Xenia Oliva (Phone #2)	GatoEncerrado	Pegasus exfiltration
(Individual #4)	La Prensa Gráfica	Pegasus infection
Oscar Luna	Revista Digital Disruptiva	Pegasus infection
(Individual #5)	(NGO #1)	Pegasus infection
Mariana Belloso	(Independent Journalist)	Pegasus infection
Carmen Tatiana Marroquín	(Economist and Columnist for Independent Media)	Pegasus infection

Table 1: Confirmed individuals hacked with Pegasus Spyware in El Salvador.

Each positive result in this case represents a phone we identified with *high confidence* as successfully hacked with Pegasus spyware (denoted as “Pegasus infection” in **Table 1**). In a subset of the cases, we are able to establish an additional result: successful exfiltration (denoted as “Pegasus exfiltration” in **Table 1**), indicating high confidence that the spyware successfully uploaded data from the phone to Pegasus infrastructure. In several

cases, Pegasus apparently exfiltrated multiple gigabytes of data successfully from target phones using their mobile data connections.

We observed extensive targeting using zero-click exploits, however we also identified specific instances in which targets were sent one-click infection links via SMS message.

Zero-Click Exploits

We assess that at least two zero-click exploits were deployed against the journalists in El Salvador: ***KISMET*** and ***FORCEDENTRY***. Thirteen of the phones contained the ***KISMET FACTOR***, which we believe is an artifact left behind by the execution of NSO Group's zero-click ***KISMET*** exploit. We saw this exploit deployed between July and December 2020, and the exploit appears to have been a zero-day against iOS 13.5.1 and 13.7. The ***KISMET*** exploit has not yet been publicly captured and analyzed, but appeared to involve the use of JPEG attachments, as well as iMessage's *IMTranscoderAgent* process invoking a WebKit instance.

Additionally, we recovered a copy of the ***FORCEDENTRY*** exploit from one of the phones. The exploit appears to have been fired at a phone with iOS 14.8.1, which is not vulnerable to ***FORCEDENTRY***. The exploit does not appear to have run on the phone. It is unclear why the exploit was fired at a non-vulnerable iOS version, though it is possible that NSO operators cannot always determine the precise iOS version used by the target before firing an exploit.

We have not identified a long-lived forensic artifact associated with ***FORCEDENTRY*** that can differentiate that exploit from other techniques used to install Pegasus on a phone, but we believe that NSO iPhone hacking between February and November 2021 was generally conducted with the ***FORCEDENTRY*** exploit. ***FORCEDENTRY*** appears to be the same exploit that Amnesty's Security Lab observed traces of in their Pegasus Project analysis, which they refer to as "Megalodon."

One-Click Links

We fingerprinted Pegasus URL shortener websites and identified 244 domain names registered from 2019 through 2021 that appear to have been used by various NSO Group customers to distribute the Pegasus spyware via links. In the case of a single target at El Faro, we saw one-click SMS messages sent to the target containing links matching our Pegasus fingerprint.

Date	Original SMS	English Translation
Jul 4, 2020	Fiscalia tras periodistas del faro. https://info-urbano[.]com/SxUqnKe1	District attorney's office against journalists from El Faro

Date	Original SMS	English Translation
Jul 4, 2020	Personal de salud denuncia mala administracion del Gobierno https://informados24h[.]com/wNjzhTb	Health staff denounces bad administration by the government
Jul 7, 2020	Presidente sale en defensa de su ahijado politico. https://informados24h[.]com/ZKtywtTbM	The President comes out in defense of his political protégé
Jul 8, 2020	Nuevas Ideas eclipsa a sus oponentes. https://informados24h[.]com/VNCeEmT	Nuevas Ideas [the political party of El Salvador's President] eclipses their opponents
Sep 7, 2020[2]	Noticia de El Salvador trasciende a nivel mundial https://informados24h[.]com/nRG9mDx	News from El Salvador goes worldwide

The messages sent to the target contained links to the following Pegasus domain names:

```
informados24h[.]cominfo-urbano[.]com
```

The following four domains that we detected in our Pegasus scanning had similar registration characteristics to the two domains above above and thus may have been used by the same Pegasus customer:

```
mobile-analytics[.]netweb-cloud-services[.]com
```

```
solo-hoy[.]com
```

```
deportes24-7[.]com
```

Apple Notifications to Confirmed Pegasus Victims

On November 23rd, 2021 Apple began sending notifications to some iPhone users who had been targeted with NSO Group's ***FORCEDENTRY*** exploit. Apple also filed a lawsuit against NSO Group on the same day.

Many of the Pegasus targets that we confirm in this investigation also reported receiving "state-sponsored spyware" notifications from Apple, including twelve journalists at *El Faro*, and two members of *Fundación DTJ*.

3. Attribution

At this time Citizen Lab is not conclusively attributing the attacks to a particular government customer of NSO Group, however there is a range of circumstantial evidence pointing to a strong El Salvador government nexus.

2 Note that the original SMS contains a double-space between the words "Salvador" and "trasciende"

First, the cases share a troubling nexus with the interests of the Bukele government:

- Targeting coincides with moments that the organizations were working on issues of great interest to the Bukele government
- Targets work focuses on domestic issues, and thus would be most relevant to a domestic audience

Secondly, Citizen Lab network scanning-based evidence has revealed TOROGOZ, an operator whose activities are strongly suggestive of a Pegasus customer in El Salvador. Notably, the operator had a near-total focus of infections within El Salvador, which is strongly suggestive of a domestic Pegasus operator.

Thirdly, one of the targets at *El Faro* (Carlos Martínez) was targeted by TOROGOZ in an unsuccessful attempt with the ***FORCEDENTRY*** exploit. The exploit was fired at a non-vulnerable version of iOS (14.8.1).

4. Conclusion: Mercenary Spyware Continues to Harm Media, Civil Society

For years, researchers and civil society have sounded the alarm that the poorly regulated mercenary surveillance market is leading to widespread human rights and other abuses. The El Salvador case presents a textbook example of those concerns.

If indeed Pegasus was sold to El Salvador, it was done despite a panoply of warning signs that abuse would take place:

- An autocratic leaning President with a fascination with digital technology
- A long history of harassment of independent media and journalists
- A climate of insecurity and human rights abuses
- Poorly regulated police, intelligence, and private security firms
- A lengthy history of corruption, organized crime, state violence, and authoritarianism

The hacking of Salvadoran civil society organizations with Pegasus mercenary spyware reflects a familiar pattern observed time and again in authoritarian societies: the use of advanced technology to frustrate and interfere with this essential component of a democratic society. In this case, the hacking also fits within a broader trend of abusive targeting and attacks against civil society in El Salvador.

Especially troubling, however, is the pattern of targeting of independent Salvadoran media that this joint investigation has uncovered.

Pegasus and the Media

Media organizations and individual journalists are now a regular target of hacking for NSO Group's government clients. A free and independent press is a threat to autocratic

rule and many of NSO Group's government clients are illiberal regimes. The voluminous hacking of Salvadoran media organizations and journalists is shocking but should come as no surprise.

Only a little over a year ago, we discovered government operatives used NSO Group's Pegasus spyware to hack 36 personal phones belonging to journalists, producers, anchors, and executives at the news organization *Al Jazeera*. The Citizen Lab and Amnesty International have also documented numerous other cases where journalists' phones were hacked with Pegasus, including *the New York Times*' Ben Hubbard, Sevinc Vaqifqizi, a freelance journalist for independent media outlet *Meydan TV*, Siddharth Varadarajan and MK Venu, co-founders of India's the *Wire*, Dániel Németh, a photojournalist working out of Budapest, and numerous others. According to investigations undertaken as part of the Pegasus Project, at least 180 journalists were selected as targets for potential Pegasus hacking.

Further highlighting the consistent threat posed by Pegasus to journalists, Daniel Lizárraga—a journalist whose phone we confirmed was hacked with Pegasus in this case—was also targeted in 2016 by the Mexican Pegasus operator while in a previous role at a Mexican NGO. Given the lack of due diligence and proper regulations, it should come as no surprise that individual victims of Pegasus hacking may have been targeted by multiple NSO Group clients over time, as Lizárraga's case illustrates.

The lesson from this case is obvious: an unregulated spyware marketplace is a grave threat to media worldwide, and to civil society.

Appendix A: Hacking Timeline

The following table of dates of successful hacking *excludes* dates of attempted but unsuccessful hacking. This table is *not* intended to be a comprehensive inventory of every date that the spyware was active on a phone. Each entry represents a separate instance where NSO's exploits were fired at a phone resulting in successful infection.

Several factors can influence the number of times infections happen. For example, if a target is selected for persistent surveillance, the exploit may be fired more often if the user frequently reboots their phone, as modern versions of the Pegasus spyware are believed to feature persistence via re-exploitation. If the target does not reboot their phone, the spyware may run for some time without the exploit being fired again.

Individual	Organization	Dates of Successful Hacking
Noah Bullock	Cristosal	1. On or around 2021-09-04
		2. On or around 2021-09-28
		3. On or around 2021-11-12

Individual	Organization	Dates of Successful Hacking
(Individual #1)	Diario El Mundo	1. On or around 2021-06-03
		2. On or around 2021-06-30
Ricardo Avelar	El Diario de Hoy	1. On or around 2020-08-31
		2. On or around 2020-09-22
		3. On or around 2021-02-21
		4. On or around 2021-03-16
		5. On or around 2021-03-26
		6. On or around 2021-04-27
		7. On or around 2021-06-15
		8. On or around 2021-07-14
		9. On or around 2021-09-04
		10. On or around 2021-09-12
Ana Beatriz Lazo	El Faro	1. On or around 2021-10-04
Carlos Dada	El Faro	1. Sometime 2020-07-08 – 2020-07-17
		2. Sometime 2020-07-17 – 2020-07-24
		3. Sometime 2020-07-24 – 2020-07-30
		4. On or around 2020-07-31
		5. Sometime 2020-08-01 – 2020-08-14
		6. Sometime 2020-09-08 – 2020-10-22
		7. Sometime 2021-01-06 – 2021-01-12
		8. Sometime 2021-01-12 – 2021-01-20
		9. Sometime 2021-02-13 – 2021-02-23
		10. Sometime 2021-03-31 – 2021-04-17
		11. Sometime 2021-04-18 – 2021-05-12
		12. Sometime 2021-05-26 – 2021-06-09

Individual	Organization	Dates of Successful Hacking
Carlos Ernesto Martínez D'aubuisson	El Faro	1. Sometime 2020-06-29 – 2020-07-22
		2. Sometime 2020-07-25 – 2020-08-06
		3. Sometime 2020-09-07 – 2020-09-10
		4. Sometime 2020-09-10 – 2020-09-18
		5. Sometime 2020-09-18 – 2020-10-10
		6. Sometime 2020-10-10 – 2020-11-05
		7. Sometime 2020-11-05 – 2020-11-10
		8. Sometime 2020-11-23 – 2020-12-02
		9. Sometime 2020-12-02 – 2020-12-21
		10. Sometime 2020-12-26 – 2021-01-21
		11. Sometime 2021-02-11 – 2021-02-16
		12. Sometime 2021-02-17 – 2021-02-19
		13. Sometime 2021-02-23 – 2021-03-08
		14. Sometime 2021-03-08 – 2021-03-11
		15. Sometime 2021-03-19 – 2021-03-23
		16. Sometime 2021-04-03 – 2021-04-12
		17. Sometime 2021-04-12 – 2021-04-27
		18. Sometime 2021-04-28 – 2021-05-06
		19. Sometime 2021-05-06 – 2021-05-27
		20. Sometime 2021-05-29 – 2021-06-02
		21. Sometime 2021-06-16 – 2021-06-22
		22. Sometime 2021-06-22 – 2021-06-24
		23. Sometime 2021-06-27 – 2021-07-02
		24. On or around 2021-07-08
		25. On or around 2021-08-31
		26. On or around 2021-09-15
		27. On or around 2021-10-07
		28. On or around 2021-10-21
Daniel Lizárraga	El Faro	1. On or around 2021-04-12
		2. On or around 2021-04-15
		3. On or around 2021-04-27
		4. On or around 2021-05-20
		5. On or around 2021-06-04
		6. On or around 2021-06-15
		7. On or around 2021-06-23
		8. On or around 2021-07-08
Daniel Reyes	El Faro	1. Sometime 2020-10-01 – 2020-10-10
		2. On or around 2021-11-04

Individual	Organization	Dates of Successful Hacking
Efren Lemus	El Faro	1. On or around 2021-04-23
		2. On or around 2021-04-26
		3. On or around 2021-04-30
		4. On or around 2021-05-20
		5. On or around 2021-06-01
		6. On or around 2021-06-08
		7. On or around 2021-06-18
		8. On or around 2021-07-10
		9. On or around 2021-09-17
		10. On or around 2021-09-25
Gabriel Labrador	El Faro	1. Sometime 2020-08-06 – 2020-09-07
		2. Sometime 2020-09-11 – 2020-10-30
		3. On or around 2021-03-25
		4. On or around 2021-04-01
		5. On or around 2021-04-06
		6. On or around 2021-04-09
		7. On or around 2021-04-12
		8. On or around 2021-04-14
		9. On or around 2021-04-16
		10. On or around 2021-05-05
		11. On or around 2021-05-07
		12. On or around 2021-05-13
		13. On or around 2021-05-17
		14. On or around 2021-06-01
		15. On or around 2021-08-31
		16. On or around 2021-09-12
		17. On or around 2021-10-06
		18. On or around 2021-10-23
		19. On or around 2021-11-04
		20. On or around 2021-11-11
Gabriela Cáceres	El Faro	1. On or around 2021-04-17
		2. On or around 2021-05-11
		3. On or around 2021-05-15
		4. On or around 2021-05-21
		5. On or around 2021-06-06
		6. On or around 2021-06-15
		7. On or around 2021-06-17
		8. On or around 2021-06-21
		9. On or around 2021-07-14
		10. On or around 2021-08-31
		11. On or around 2021-09-08
		12. On or around 2021-09-17
		13. On or around 2021-09-24

Individual	Organization	Dates of Successful Hacking
José Luis Sanz	El Faro	1. Sometime 2020-07-04 – 2020-07-09
		2. Sometime 2020-07-09 – 2020-07-14
		3. On or around 2020-07-16
		4. On or around 2020-09-10
		5. On or around 2020-09-23
		6. On or around 2020-11-14
		7. On or around 2020-11-21
		8. On or around 2020-11-28
		9. On or around 2020-12-03
		10. On or around 2020-12-07
		11. On or around 2020-12-10
		12. On or around 2020-12-16
		13. On or around 2020-12-19
Julia Gavarrete (Phone #1)	El Faro	1. On or around 2021-03-16
		2. On or around 2021-04-08
		3. On or around 2021-04-13
		4. On or around 2021-04-14
		5. On or around 2021-04-16
		6. On or around 2021-04-18
		7. On or around 2021-04-20
		8. On or around 2021-04-23
		9. On or around 2021-04-26
		10. On or around 2021-05-05
		11. On or around 2021-05-20
		12. Sometime 2021-05-30 – 2021-06-06
		13. On or around 2021-06-10
		14. On or around 2021-06-28
		15. On or around 2021-09-08
Julia Gavarrete (Phone #2)	El Faro	1. On or around 2021-02-23
		2. On or around 2021-09-09
		3. On or around 2021-09-27
María Luz Nóchez	El Faro	1. On or around 2021-02-17
		2. On or around 2021-05-21
		3. On or around 2021-06-09
Mauricio Ernesto Sandoval Soriano	El Faro	1. Sometime 2020-08-19 – 2020-10-20
		2. On or around 2021-07-02
		3. On or around 2021-07-06
		4. On or around 2021-10-01
Nelson Rauda	El Faro	1. Sometime 2021-04-30 – 2021-05-01
		2. On or around 2021-05-18
		3. On or around 2021-06-16
		4. Sometime 2021-06-18 – 2021-08-11
		5. On or around 2021-08-31
		6. On or around 2021-09-10

Individual	Organization	Dates of Successful Hacking
Óscar Martínez	El Faro	1. On or around 2020-07-15
		2. On or around 2020-07-21 – 2020-07-28
		3. On or around 2020-08-12
		4. On or around 2020-08-17
		5. On or around 2020-08-19
		6. On or around 2020-09-12
		7. On or around 2020-09-29
		8. On or around 2020-10-01
		9. On or around 2020-10-03
		10. On or around 2020-10-29
		11. On or around 2020-11-12
		12. On or around 2020-11-16
		13. On or around 2020-11-18
		14. On or around 2020-12-07
		15. On or around 2020-12-10
		16. On or around 2020-12-18
		17. On or around 2020-12-20
		18. On or around 2020-12-22
		19. On or around 2021-01-08
		20. On or around 2021-01-10
		21. On or around 2021-01-13
		22. On or around 2021-01-26
		23. On or around 2021-01-27
		24. On or around 2021-02-21
		25. On or around 2021-03-08
		26. On or around 2021-03-15
		27. On or around 2021-03-18
		28. On or around 2021-03-25
		29. On or around 2021-04-01
		30. On or around 2021-05-03
		31. On or around 2021-05-21
		32. On or around 2021-06-02
		33. On or around 2021-06-16
		34. On or around 2021-06-22
		35. On or around 2021-06-23
		36. On or around 2021-07-07
		37. On or around 2021-08-30
		38. On or around 2021-09-08
		39. On or around 2021-09-27
		40. On or around 2021-10-08
		41. On or around 2021-10-25
		42. On or around 2021-10-30
Rebeca Monge	El Faro	1. On or around 2021-10-07

Individual	Organization	Dates of Successful Hacking
Roman Gressier	El Faro	1. On or around 2021-05-17
		2. On or around 2021-05-21
		3. On or around 2021-06-21
		4. On or around 2021-06-23
Roxana Lazo	El Faro	1. On or around 2021-04-19
		2. On or around 2021-04-27
		3. On or around 2021-06-02
		4. On or around 2021-06-07
		5. On or around 2021-06-23
		6. On or around 2021-06-24
		7. On or around 2021-07-06
		8. On or around 2021-09-10
		9. On or around 2021-09-24
		10. On or around 2021-10-02
		11. On or around 2021-10-21
		12. On or around 2021-11-02
Sergio Arauz	El Faro	1. Sometime 2020-08-12 – 2020-08-19
		2. Sometime 2020-09-10 – 2020-09-11
		3. Sometime 2020-09-13 – 2020-09-14
		4. Sometime 2020-09-18 – 2020-09-22
		5. On or around 2021-05-07
		6. On or around 2021-06-02
		7. Sometime 2021-06-09 – 2021-06-10
		8. On or around 2021-06-11
		9. On or around 2021-06-17
		10. On or around 2021-06-24
		11. On or around 2021-06-25
		12. On or around 2021-07-02
		13. On or around 2021-07-09
		14. On or around 2021-10-21
Valeria Guzmán	El Faro	1. Sometime 2020-07-04 – 2020-07-14
		2. On or around 2021-09-03
		3. On or around 2021-09-29
		4. On or around 2021-10-12
		5. On or around 2021-10-25
		6. On or around 2021-11-04
		7. On or around 2021-11-11
		8. On or around 2021-11-19
Víctor Peña	El Faro	1. Sometime 2021-11-22 – 2021-11-23
(Individual #2)	El Faro	1. Sometime 2020-09-09 – 2020-09-16
		2. On or around 2021-09-30
		3. Sometime 2020-11-16 – 2020-11-26

Individual	Organization	Dates of Successful Hacking
(Individual #3)	El Faro	1. Sometime 2020-09-07 – 2020-10-17
		2. Sometime 2020-11-30 – 2021-01-16
		3. On or around 2021-05-21
Jose Marinero	Fundación DTJ	1. On or around 2021-04-08
		2. On or around 2021-09-12
Xenia Hernandez	Fundación DTJ	1. On or around 2021-02-23
		2. On or around 2021-03-17
		3. On or around 2021-04-29
		4. On or around 2021-05-01
		5. On or around 2021-05-04
		6. Sometime 2021-05-04 – 2021-05-07
		7. On or around 2021-05-07
		8. On or around 2021-05-11
		9. On or around 2021-05-17
		10. On or around 2021-05-21
		11. On or around 2021-06-02
		12. On or around 2021-06-13
		13. On or around 2021-06-15
		14. On or around 2021-06-28
		15. On or around 2021-06-30
		16. On or around 2021-11-09
		17. On or around 2021-11-16
Beatriz Benitez	GatoEncerrado	1. On or around 2021-07-01
Ezequiel Barrera	GatoEncerrado	1. Sometime 2020-09-10 – 2020-09-11
		2. Sometime 2021-04-06 – 2021-04-11
		3. Sometime 2021-04-13 – 2021-04-16
		4. Sometime 2021-04-23 – 2021-04-25
		5. On or around 2021-06-07
		6. On or around 2021-06-21
		7. On or around 2021-06-30
		8. On or around 2021-07-08
		9. On or around 2021-09-19
Xenia Oliva (Phone #1)	GatoEncerrado	1. Sometime 2020-11-12 – 2020-11-25
		2. Sometime 2021-02-17 – 2021-02-26
		3. Sometime 2021-02-28 – 2021-03-09
		4. On or around 2021-04-08
		5. On or around 2021-05-21
Xenia Oliva (Phone #2)	GatoEncerrado	1. On or around 2021-10-26
		2. On or around 2021-11-04
(Individual #4)	La Prensa Gráfica	1. On or around 2021-09-27
Oscar Luna	Revista Digital Disruptiva	1. On or around 2021-04-18
		2. On or around 2021-09-29
(Individual #5)	(NGO #1)	1. On or around 2021-05-21

Individual	Organization	Dates of Successful Hacking
Mariana Belloso	(Independent Journalist)	1. On or around 2021-09-29
		2. On or around 2021-10-09
Carmen Tatiana Marroquín	(Economist and Columnist for Independent Media)	1. On or around 2021-09-05