Hacktivism in Latin America: The Case of Guacamaya

James Barr & Sofia Liemann Escobar
Digital Security in Latin America Research Group
April 2023

An image released by Guacamaya which they describe as "[a] photo of us at work hacking Pronico."[1]

On March 6th 2022, Enlace Hacktivista, a website dedicated to documenting hacker history[2], was sent a statement and video to publish from a group calling itself Guacamaya. The materials concerned two companies, CGN and Pronico, subsidiaries of the Swiss-registered mining consortium Solway[3], and the production of ferronickel in the Fenix nickel project near El Estor in eastern Guatemala. This project has been historically mired in accusations of human rights

[1] Laurent Richard, "'The Struggle of One Territory Must Be the Struggle of All'," *Forbidden Stories*, March 6, 2022, https://forbiddenstories.org/about-mining-secrets/.
[2] "Enlace Hacktivista," accessed April 13, 2023, https://enlacehacktivista.org/.
[3] "FENIX PROJECT, GUATEMALA – Solway Investment Group," accessed April 13, 2023, https://solwaygroup.com/our-business/fenix-project-guatemala/.

abuses, environmental damage, and local resistance[4]. The video shows the hackers breaking into company networks and downloading files, before finally wiping data and various applications from the company's systems[5]. Through these hacks, Guacamaya openly made available over four terabytes (TB) of documents exposing the harsh working conditions at the mines along with attempts from the company to silence anyone trying to report on it. The leaked documents made the headlines across multiple news outlets in the world including *El País*, *Le Monde* and *The Guardian*[6]. But for Guacamaya this hack was just the start.

1) Who are Guacamaya?

In 2022, Guacamaya leaked over 25 TB of emails and documents in four leaks spanning nine Latin American states (see Table 1 for details). These hacks have largely targeted extractive industries, military, and law enforcement. Each leak is accompanied by a statement outlining the group's motivations and demands (see Table 1). Their statements and actions, along with limited interviews the group has granted to journalists, reveal insights into how Guacamaya wants to be perceived.

TABLE 1: SUMMARY OF GUACAMAYA LEAKS

LEAK	COUNTRY	ENTITY
LEAK 1 March 6, 2022 (*Statement* & *Video*)	Guatemala	Solway, Pronico & CGN *(All involved with 'Fenix' project)*
LEAK 2 August 1, 2022 (*Statement*)	Brazil	Tejucana *(Mining Company)*
	Chile	Quiborax *(Mining Company)*
	Colombia	Agencia Nacional Hidrocarburos *(National*

[4]Guardian Staff Reporter, "Guatemala Mine's Ex-Security Chief Convicted of Indigenous Leader's Murder," *The Guardian*, October 19, 2022, https://www.theguardian.com/global-development/2021/jan/07/guatemala-nickel-mine-death-adolfo-ich.
[5] For more information on steps taken in the hack see: "Pronico - Enlace Hacktivista," accessed April 14, 2023, https://enlacehacktivista.org/index.php?title=Pronico.
[6]"Mining Secrets - Distributed Denial of Secrets," accessed April 13, 2023, https://ddosecrets.com/wiki/Mining_Secrets.

		Hydrocarbon Agency)
	Colombia	New Granada Corporation *(Oil Subsidiary)*
	Ecuador	ENAMI EP *(Mining Company)*
	Guatemala	Ministerio de Ambiente y Recursos Naturales *(Environment and Natural Resources Ministry)*
	Venezuela	Oryx *(Oil Company)*
LEAK 3 August 7, 2022 *(Statement)*	Colombia	Fiscalía General de la Nación *(Attorney General"s Office)*
LEAK 4 September 19, 2022 *(Statement, Poem, & Video)*	Chile	Estado Mayor Conjunto de las Fuerzas Armadas de Chile *(Joint Chiefs of Staff of the Chilean Armed Forces)*
	Colombia	Comando General de las Fuerzas Militares de Colombia *(General Command of Colombia's Military Forces)*
	El Salvador	Fuerzas Armadas de El Salvador *(El Salvador's Armed Forces)*
	El Salvador	Policía Nacional Civil de El Salvador *(National Civil Police of El Salvador)*
	Peru	Comando Conjunto de las Fuerzas Armadas *(Joined Command of Armed Forces)*

	Peru	Ejército del Perú *(Peruvian Army)*
	Mexico	Secretaría de la Defensa Nacional de México *(Mexican Ministry of National Defence)*

The name Guacamaya is derived from the Mayan word for the macaw parrot. Hiram Camarillo of Seekurity suggests that the group could originate from Guatemala or Costa Rica, where these birds are commonly found[7]. Throughout their statements, the group plays up to popular stereotypes of indigenous groups, particularly positive traits such as ideas of oneness with the earth, their ancestors, and nature[8]. For example, each of the first three statements begin with "We are not defenders of nature, we are nature!"[9]. Every statement refers to the continent of the Americas as the Abya Yala, a name used by native peoples derived from the Kuna language of Panama meaning "land in full maturity"[10].

Throughout the statements, there are numerous critiques of what they see as the 'neo-colonial', 'civilising' projects of the Global North. In these, they explicitly condemn North American 'imperialism' through political intervention and projects of extractivism fostered through multinational corporations, acts which they characterise as being practised through mechanisms of 'terror' and 'genocide'. This is also reflected in their targets. Their statements tend to have a wide focus, though some are more specific to relate to the contents of their attached leak. For instance, the statement accompanying the fourth leak, focuses on state domination through military and police force, arguing that these institutions serve to protect the modern nation state and its capitalist functioning. In this, the narrative shifts to more of a class-based analysis, albeit with a strong racial focus, highlighting how those of "creole" heritage who have generally governed nation states across the

[7] Recorded Future, "58. Enemy of the State (Part 2): ¿Quién Es Guacamaya? (Who Is Guacamaya?)," interview by Dina Temple-Raston (Recorded Future, March 14, 2023), https://open.spotify.com/episode/4HasAAokUKxeHGMEg71juY.
[8] The characterisation of indigeneity around its positive relationships to nature can be reductive. Not all groups fit this depiction. For further information see: Michael Dove, "Indigenous People and Environmental Politics," *Annual Review of Anthropology, 2006* 35, (2006): 195-203. Nevertheless, colloquially, indigeneity does tend to be associated with values of respect, conservation, and oneness with nature, see: "Indigenous people and nature: a tradition of conservation," UNEP, accessed April 14, 2023, https://www.unep.org/news-and-stories/story/indigenous-people-and-nature-tradition-conservation.
[9] Translated from Spanish into English. Enlace Hacktivista. "RESISTENCIA MILENARIA.," accessed April 13, 2023. https://enlacehacktivista.org/comunicado_guacamaya.txt.
[10] Catherine E. Walsh, "Pedagogías decoloniales caminando y preguntando: notas a Paulo Freire desde Abya Yala," *Revista Entramados - Educación Y Sociedad* N. 1 (October 17, 2014): pp 17-30, https://dialnet.unirioja.es/servlet/articulo?codigo=5251817.

region have a “heritage of dispossession of native people. They are not interested in the population, nor in maintaining a healthy respect for Mother Earth”[11].

Interestingly, explicit references to class were generally absent until the fourth statement. However, there are clear postmodern influences apparent in the linguistic choices of the authors. For instance, in the first statement, the authors make use of the feminine “nosotras” as opposed to the conventional choice of ‘nosotros’. In the second, the authors choose to use “nosotr@s”, the @ sign acting as a gender neutral suffix in place of the -o/-a ending. In the third statement, they use “nosotrxs” by the same rationale. Notably the fourth statement, where class-based analysis is more prevalent, uses conventional gendered Spanish form. These choices represent a challenge to the gendered nature of the Spanish language and indicate that these articles were likely written by young people, possibly with a university education; these language conventions predominantly emerged from and evolved in universities[12]. In an interview with the Click Here Podcast, Cecilia Farfán, the head of research at the Centre for U.S. Mexican Studies at the University of California, San Diego, suggests that Guacamaya draws upon feminist theory, as well as continuously highlighting the negative consequences of patriarchy. She suggests that women therefore likely make up a large part of the group[13]. In an interview with Guacamaya, the group rejects a western view that imposes a binary feminine and masculine division of people, and state that their actions were done by "all people"[14].

Despite these forward-looking, modern linguistic choices, the content of Guacamaya’s statements is notably backwards looking in many senses, often harking back to communal forms of existence and reparation for the losses of these communities. This is a rather different form of revolutionary rhetoric to that of the vanguardist Che Guevara for instance[15], arguably reflecting more of synthesis between indigenous tradition and anarchist philosophy. It is perhaps more in line with that of the non-hierarchical structure and ideology of the Zapatistas[16].

[11] Translated from Spanish into English. “GUACAMAYA NO SOMOS DEFENSORES DE LA VIDA, SOMOS VIDA!,” Enlace Hacktivista, accessed April 13, 2023, https://enlacehacktivista.org/comunicado_guacamaya4.txt.
[12] Cristobal Salinas and A. Lozano, “Mapping and Recontextualizing the Evolution of the Term *Latinx*: An Environmental Scanning in Higher Education,” *Journal of Latinos and Education* 18, no. 4 (January 14, 2019): 302–15, https://doi.org/10.1080/15348431.2017.1390464.
[13] See footnote 6.
[14] Dina Temple-Raston and Sean Powers, “A Q&A with the Hacktivists Rocking Latin America: Guacamaya,” *The Record,* March 28, 2023, https://therecord.media/interview-with-guacamaya-hacktivist-group-latin-america.
[15] Che Guevara, *Guerilla Warfare: A Method* (Peking: Foreign Language Press, 1964), 2.
[16] Mark Gelsomino, "The Zapatista Effect: Information Communication Technology Activism and Marginalized Communities," *Faculty of Information Quarterly* 2, no 3 (2010).

Questions of Authenticity

Despite their statements, questions regarding the group's authenticity began to circulate as soon as the leaks emerged. For example, the left-wing Mexican news outlet *Contralinea* claimed this was an attempt to discredit left-wing progressive governments in the region[17]. Mexican President Andrés Manuel López Obrador speculated that international agencies linked to a conservative group were behind Guacamaya[18]. For others, such as *Risky Biz* editor, Tom Uren, a few red flags such as interests initially aligning with another state, similarities with another case in Australia, as well as the group's use of ProxyLogon pointed at Chinese hackers as the potential perpetrators[19]

However, there are many indications that suggest Guacamaya is more likely to be an authentic hacktivist group. The statements they released contain specific references to historical events across the region that suggest at least some level of knowledge about the countries and organisations that were targeted. Furthermore, although their proficiency in Spanish is not an indication of authenticity, it can reduce the pool of actors that could be pretending to be a hacktivist group[20]. For example, spelling mistakes have been one way of identifying scammers and cybercriminals in the past[21]. This is often linked to carelessness and time constraints. But in the Guacamaya case, the statements are well written with no spelling mistakes, suggesting that time and care was taken when creating the statements. Furthermore, the group appears to have gone through great lengths to create what feels like an authentic aesthetic. The music and art used in the videos reflects historical events in the region as well as many of the themes they touch upon in their statements. Their vivid illustrations and the centring of their art in their pronouncements, has led some, such as anthropology professor Gabriella Coleman, to see the group as "authentic political activists"[22].

Across their statements, they also invite others to become involved in their movement through emulating their hack and leak practices. In their first statement, when citing their own video, they state that "hacking is not magic, nor does it require a lot of resources or advanced technical knowledge. It was all done with free open source tools that anyone can learn to master - just filter and sabotage with joyful rebellion"[23]. These

[17]Nancy Flores, "Con Pegasus, Guacamaya y 'El rey del cash', arrecia el golpe blando," *Contralínea*, October 20, 2022, https://contralinea.com.mx/interno/semana/con-pegasus-guacamaya-y-el-rey-del-cash-arrecia-el-golpe-blando/.
[18]Manuel Espino, "Cae mando militar por caso Guacamaya Leaks," *El Universal*, March 28, 2023, https://www.eluniversal.com.mx/nacion/cae-mando-militar-por-caso-guacamaya-leaks.
[19] Tom Uren, "Microsoft's Sociopathic Cybersecurity Pedantry," *Srslyriskybiz*, October 27, 2022, https://srslyriskybiz.substack.com/p/microsofts-sociopathic-cybersecurity.
[20] See footnote 6.
[21] Guardian Staff Reporter, "Spelling Mistake Prevented Hackers Taking $1bn in Bank Heist," *The Guardian*, May 25, 2017, https://www.theguardian.com/business/2016/mar/10/spelling-mistake-prevented-bank-heist.
[22] AJ Vicens, "The Politics and Power of Latin American Hacktivists Guacamaya," *CyberScoop*, January 23, 2023, https://cyberscoop.com/guacamaya-hacktivist-group-latin-america-interview/.
[23] Translated from Spanish into English. "RESISTENCIA MILENARIA."

were not particularly sophisticated hacks compared to the type of cyber operations conducted by major cyber powers who have greater resources available to them. Even in interviews with journalists Guacamaya have highlighted their limited hacking skills, stating that they "are learning"[24], as well explaining that for the SEDENA hacks, they found exploits on GitHub and downloaded them before employing them on the Mexican military's systems[25].

While the previous arguments are by no means proof that the group is authentic, public reporting[26] of the group's hacking activities, and the assessments of experts[27], suggest that the group's activities could credibly be conducted by a non-state actor. Finally, access to some of the more sensitive material of the leaked data requires an evaluation from the two host websites of this content (Enlace Hacktivista and DDoSecrets) of the intent and credibility of journalists and researchers[28]. This stands in contrast with other actors in cyberspace who either dump the data so that it can be accessed by anyone or sell it to the highest bidder. For now, Guacamaya appears to likely be an authentic hacktivist group.

2) What can we learn?

Many stories are yet to emerge as journalists and researchers continue to go through the leaked data. However, there are some general reflections that can be made around these incidents and the information that has emerged so far. Some of these reflections are relevant to hack and leak operations more broadly, whilst others are more specific to the Latin American context.

Guacamaya leaks reflect complexities of reporting on these types of stories

Coverage of this story has varied across the region. Whilst some countries saw the leaks dominating headlines for months, in others, the stories were more understated and limited. Moreover, what was deemed 'newsworthy' was very variable across countries and news media outlets. Such coverage therefore reflects the complexities of reporting on a case such as Guacamaya. For starters, not all

[24] Temple-Raston and Powers, "A Q&A with the Hacktivists Rocking Latin America: Guacamaya."
[25] Recorded Future, "58. Enemy of the State (Part 2): ¿Quién Es Guacamaya? (Who Is Guacamaya?),"; Nicolas Marin and Melissa Vida, "'Hacking Should Be Used to Wake up and Rebel,' Says Hacker Group Guacamaya," *Global Voices*, January 10, 2023 https://globalvoices.org/2023/01/10/hacking-should-be-used-to-wake-up-and-rebel-says-hacker-group-guacamaya/.
[26] Recorded Future, "58. Enemy of the State (Part 2): ¿Quién Es Guacamaya? (Who Is Guacamaya?),".
[27] Tom Uren, "Microsoft's Sociopathic Cybersecurity Pedantry,"; Vicens, "The Politics and Power of Latin American Hacktivists Guacamaya,"; Sc Staff, "LatAm Hacktivist Collective Guacamaya Examined," *SC Media*, January 25, 2023, https://www.scmagazine.com/brief/threat-intelligence/latam-hacktivist-collective-guacamaya-examined
[28] Vicens, "The Politics and Power of Latin American Hacktivists Guacamaya,".

researchers and journalists in the region have the technical know-how to access the many terabytes of leaked data and to "parse it for stories"[29]. Furthermore, Latin America is one of the deadliest regions for journalists[30], perhaps dissuading the reporting of certain topics.

The pattern of coverage reveals political interest and power. An example of this can be seen in the work of *Contralinea*, a left-wing news outlet in Mexico. Whilst in one article the leaks are seen as a way to discredit the current president, or a "soft-coup" as they call it[31], in another article they are willing to report on the actions exposed by the leaks of the previous government[32]. This is just one example of a broader tension that the Guacamaya leaks brings to the forefront. Their rhetoric and language is similar to what could have perhaps been identified in the past as leftist revolutionary ideology. Yet the leaks come out at a time where many of the countries targeted are now headed by leftist governments. This creates a dilemma for some who identify as being from the left, and would otherwise sympathise with Guacamaya's apparent views, but who do not want to criticise their current leaders.

Finally, the public's reaction to the stories across the region is also worth considering. The leaks received far more attention in some countries than in others. Most notably, following the Mexican government's confirmation on the 30th of September 2022[33] of the intrusion into SEDENA's systems and the subsequent data leak, mentions of 'SEDENA' in tweets peaked at 10th worldwide on Twitter[34]. In other countries, the relatively limited response could perhaps be understood against a backdrop of continuous scandal in the news cycle. Here, it is easy to see how one more story can be drowned out. This may explain why the reaction to the leaks was muted in Colombia. In a previous example, reports of a cyber incident affecting the networks of the Colombian armed forces in August 2021[35] received a limited response, despite being one the most serious cyber incidents to date in Colombia. The story was overshadowed by the ongoing scandal that had started a few days earlier when Haitian President Jovenel Moïse was assassinated by a group

[29] Vicens, "The Politics and Power of Latin American Hacktivists Guacamaya."
[30] Zoe Simbolon, "Latin America Was the Deadliest Region for Journalists in 2022," *Committee to Protect Journalists*, January 24, 2023, https://cpj.org/2023/01/latin-america-was-the-deadliest-region-for-journalists-in-2022/.
[31] Flores, "Con Pegasus, Guacamaya y 'El rey del cash', arrecia el golpe blando."
[32] Nancy Flores, "Con Peña, Sedena clasificaba a columnistas en 'positivos' y 'negativos,'" *Contralínea*, October 18, 2022, https://contralinea.com.mx/interno/semana/con-pena-sedena-clasificaba-a-columnistas-en-positivos-y-negativos/.
[33]Sarah Morland, "Mexican Government Suffers Major Data Hack, President's Health Issues Revealed," *Reuters*, September 30, 2022, https://www.reuters.com/world/americas/mexican-president-confirms-hack-government-files-2022-09-30/.
[34] For twitter trend see: "Sedena · Worldwide · Twitter Trending Topic," Getdaytrends, accessed April 14, 2023, https://getdaytrends.com/trend/Sedena/.
[35] Noticias Caracol, "La historia secreta del hackeo más grave contra las Fuerzas Militares de Colombia," *Noticias Caracol,* July 12, 2021, https://noticias.caracoltv.com/informes-especiales/historia-secreta-del-hackeo-mas-grave-contra-las-fuerzas-militares-de-colombia.

of mercenaries that included former Colombian soldiers[36]. Stories about the Guacamaya leaks have faced a similar dynamic, where they compete with the latest political scandal emerging as Colombia goes through a change of government. Interestingly, the inauguration of President Gustavo Petro in Colombia coincided with the release of the 'Fiscalía Leaks' (3rd leak) [37].

Leaks affected a wide scope of targets

The range of entities targeted by Guacamaya reflect the group's political motivations. Initially they focused on extractive companies and some associated ministries, highlighting abusive practices and revealing confidential information about agreements. The group later shifted their attention to law enforcement and military in the region. These stories have exposed issues of surveillance, corruption, lack of accountability, but have also revealed sensitive information concerning law enforcement and military operations.

Extractive Companies

Forbidden Stories, an organisation dedicated to publishing the findings of journalists working in contentious spaces, have published a series of articles from data leaked around the first set of hacks pertaining to Solway and the Fenix nickel project in Guatemala. In these, Forbidden Stories allege that Solway targeted journalists reporting on the mine, profiling, surveilling, and even following them with drones[38]. Further, they allege that Solway buried unfavourable scientific studies, bought support through generous donations, and engaged in numerous smear campaigns against opposition community leaders.

Law Enforcement and Militaries

This subsection largely centres on the SEDENA hacks in Mexico, reflecting how the majority of reporting concerning law enforcement and the military focuses on these particular leaks.

Concerning issues of surveillance, analysis of leaked documents by the *New York Times* substantiated claims that the Pegasus spyware operated by Israeli company NSO Group, had been used in Mexico to spy on journalists and activists who were attempting to expose corruption and misconduct, claims which the NSO group

[36] BBC News Mundo, "Jovenel Moïse: la vieja industria de mercenarios colombianos que presuntamente está detrás del asesinato del presidente de Haití," *BBC News Mundo,* July 9, 2021, https://www.bbc.com/mundo/noticias-america-latina-57784827.
[37] See Enlace page: "Fiscalia - Enlace Hacktivista," Enlace Hacktivista, accessed April 14, 2023, https://enlacehacktivista.org/index.php?title=Fiscalia.
[38]"'Mining Secrets': When There Is Strength in Numbers · Forbidden Stories," *Forbidden Stories*, March 6, 2022, https://forbiddenstories.org/about-mining-secrets/.

said it could not comment on due to confidentiality agreements with their clients[39]. This leak undermined President Andrés Manuel López Obrador's claims that his administration would never use such surveillance mechanisms, purportedly showing that such technology had grown to be even more important during his tenure.

The leaks have purported to expose cases of corruption. In one of the most notable cases, the daily Mexican newspaper, *El Financiero*, analysed an intelligence report from June 2019 which stated that an unidentified Mexican army officer was colluding with a drug trafficking cell operating in Atlacomulco, a town near Mexico City[40]. The officer was alleged to have offered the cell a range of tactical equipment, weapons, and the provision of information on the movements of a prosecutor in Mexico State, who the cartel was looking to assassinate[41].

The leaks have also highlighted issues around transparency and accountability. For instance, the National Security Archive draws on the leaks to show the inaction of the military surrounding the Ayotzinapa case. In 2014, a group of students from Ayotzinapa Rural Teachers College was allegedly attacked by local security forces and members of a criminal gang when travelling through Iguala, Guerrero. This attack resulted in the death of six people and the disappearance of 43. In the aftermath, there were major questions around the involvement of the military, and accusations of obfuscation around the investigation. The SEDENA leaks suggest the Mexican military had been surveilling the school for decades, considering its students 'subversives'[42]. Moreover, they found evidence that the Mexican Defence Secretary oversaw a campaign aimed at discrediting parents, lawyers and experts that had been assigned to the case by a commission from the United Nations.

Outside Mexico, the leaks also revealed sensitive information. For instance, from the hacks into the Peruvian military, the Chilean media outlet *CIPER* found files revealing a series of war plans that the country could implement in the event of an armed conflict on their southern border with Chile[43]. Arguably these leaks adversely impacted national security through potentially undermining these contingency plans.

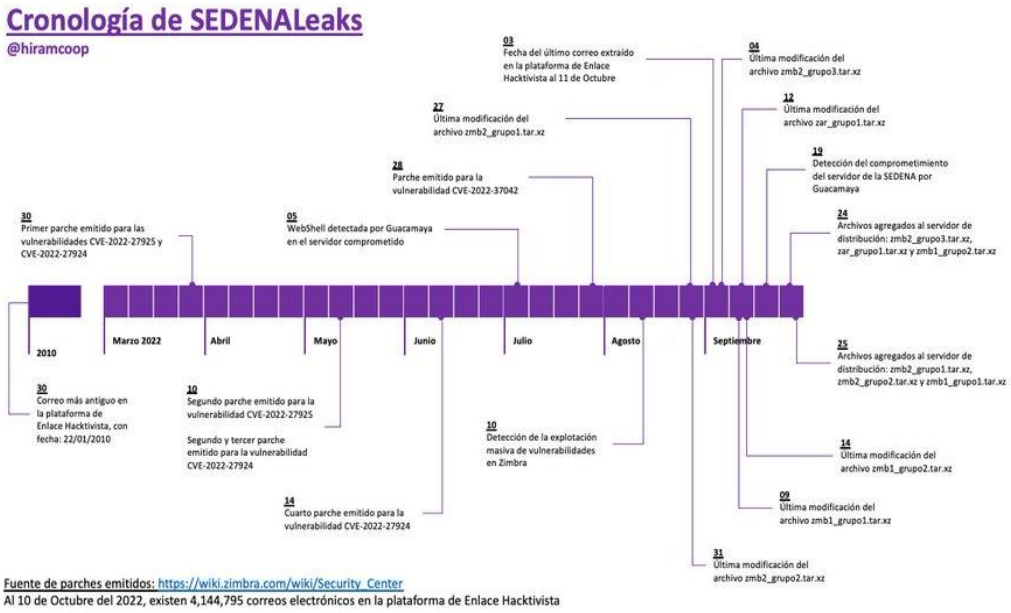
---

[39]Natalie Kitroeff and Ronen Bergman, "Spying by Mexico's Armed Forces Brings Fears of a 'Military State,'" *The New York Times*, March 7, 2023, accessed April 14, 2023, https://www.nytimes.com/2023/03/07/world/americas/mexico-military-surveillance.html.
[40]EFE, "Militar vendió armas a criminales, revela hackeo de 'Guacamaya Leaks,'" *El Financiero*, October 9, 2022, https://www.elfinanciero.com.mx/nacional/2022/10/09/sedena-vendio-armas-a-criminales-revela-hackeo-de-guacamaya-leaks/.
[41] Chris Dalby, "Three Criminal Revelations from Mexico's Defense Ministry Leaks," *InSight Crime*, October 12, 2022, https://insightcrime.org/news/three-criminal-revelations-from-mexico-defense-ministry-leaks/.
[42] "Guacamaya Leaks and the Ayotzinapa Case," *National Security Archive*, accessed April 14, 2023, https://nsarchive.gwu.edu/briefing-book/mexico-ayotzinapa/2023-03-10/guacamaya-leaks-and-ayotzinapa-case.
[43]Nicolás Massai D, "Perú-files: hackeo al Ejército peruano desnuda sus planes de guerra en caso de un ataque desde Chile," *CIPER Chile*, October 6, 2022, https://www.ciperchile.cl/2022/10/06/peru-files-hackeo-al-ejercito-peruano-desnuda-sus-planes-de-guerra-en-caso-de-un-ataque-desde-chile/.

Finally, recognising all the various allegations above, there has been little in the way of arrests and legal action. For instance, in Mexico President Obrador has openly defended Adán Augusto López[44] concerning allegations made by the Mexican magazine *Proceso*, that whilst serving as governor of Tabasco, he had appointed three men with suspected ties to the Jalisco Nueva Generación Cartel (CJNG) to senior security positions[45]. Of course, these are still the early stages of the leaks and juridical processes can take time. Thus far, the only arrests and resignations have related to the cyber security issues, as the next section shall explore.

Leaks speaks to the level of cyber (in)security in the region

Perhaps one of the less discussed aspects of the Guacamaya leaks is that it exposed the low levels of cyber security across a range of institutions in the region. Many of those institutions deal with highly sensitive documents. Some news outlets picked up on the relatively low level of technical skill and sophistication required for these hacks, calling into question the cyber security practices of these institutions. The group exploited a range of known vulnerabilities with available patches. For example, Guacamaya gained access to SEDENA's systems a few months after software patches for the collaborative software suite, Zimbra, were released. This can be seen on the timeline below shared by Threat Hunter, Hiram Alejandro, on twitter[46]:



[44] El Universal, "López Obrador Defiende a Adán Augusto Tras Guacamaya Leaks Por Supuestas Designaciones," *El Universal,* October 17, 2022, https://www.youtube.com/watch?v=6NtDFXQv8oU.
[45]Mathieu Tourliere, "Sedena Leaks: Adán Augusto López entregó la seguridad de Tabasco a presuntos líderes del CJNG," *Proceso*, October 5, 2022, https://www.proceso.com.mx/nacional/2022/10/5/sedena-leaks-adan-augusto-lopez-entrego-la-seguridad-de-tabasco-presuntos-lideres-del-cjng-294663.html.
[46] Hiram Alejandro, Twitter post, October 10, 2022, 6:30 p.m., https://twitter.com/hiramcoop/status/1579526972333383680.

In another example, the online magazine *CAMBIO*, detail how the group made use of Microsoft Exchange vulnerabilities to gain access to the systems of Colombia's Attorney General[47]. Even though updates were available, only six out of the eight servers of this entity were patched. Lax security practices when handling sensitive documents also appear to be an issue. *CAMBIO* highlights a document they encountered in the leaks containing the real identity of a European officer who had informed the Colombian police of the criminal plans of an organised crime group[48]. Despite containing highly sensitive information that could put an individual in serious danger, it appears the email was sent without any form of encryption.

Though the data leaked confirmed serious human rights abuses along with dubious practices, a discussion around the cyber security of government institutions should not be ignored. Amongst the many terabytes of information leaked, there was also sensitive personal information of individuals as well as information that could genuinely compromise national security (as was seen with the release of Peru's war plans). There have been some attempts of accountability in the face of cyber security failures, with the Chilean Chief of the General Staff resigning[49] and a SEDENA official in Mexico being charged for the loss of military information[50]. However, these actions are mostly political in nature, and it is unclear if they will address the underlying cyber security culture weaknesses. That a group with no sophisticated hacking skills gained access to so much information should be a major wake up call to governments in the region. This time a lot of that information has been mediated by the journalists and researchers who have tried to be cautious with what is published, but that is not to say that other criminal actors or nation states will do the same.

[47]Cambio Colombia, "#FiscalíaLeaks: La Mayor Fuga de Información de La Historia," *Cambio Colombia*, January 29, 2023, https://cambiocolombia.com/poder/fiscalialeaks-la-mayor-fuga-de-informacion-de-la-historia.
[48] Cambio Colombia, "#FiscalíaLeaks: La Mayor Fuga de Información de La Historia."
[49]Urgente 24, "Por hackeo cayó el Jefe del Estado Mayor Conjunto de Chile," *Urgente24 - Primer Diario Online Con Las Últimas Noticias De Argentina Y El Mundo En Tiempo Real*, September 23, 2022, https://urgente24.com/mundo/por-hackeo-cayo-el-jefe-del-estado-mayor-conjunto-chile-n544131.
[50]Manuel Espino, "Cae mando militar por caso Guacamaya Leaks," *El Universal*, March 28, 2023, https://www.eluniversal.com.mx/nacion/cae-mando-militar-por-caso-guacamaya-leaks/.

Questions to keep an eye on

What questions should we be asking?

- Are we yet to see the full impact of the revelations?

Many terabytes of information have been released, with journalists and researchers still making their way through the data to make sense of it. It is therefore likely that we will see further stories derived from these leaks.

- Will other groups follow the calls from Guacamaya?

One of the reasons for releasing a video detailing how the hack was conducted was to show others that this was possible. Guacamaya has consistently encouraged people to adopt its methods. It is therefore worth asking whether others will follow (or have followed) this call to action. Finally, as the vulnerabilities of certain institutions are made more public, it is also worth enquiring whether other actors see this as an opportunity to engage in further criminal activity.

- Will Guacamaya become more aggressive with their cyber operations?

For now, Guacamaya's actions have mostly followed the same steps: hack and leak. In some instances, they have also wiped computers and defaced websites[51]. However, as we read through their manifestos it becomes apparent that the group is demanding changes that are unlikely to occur by simply exposing information. It is therefore worth asking whether this is a reflection of the group's trust of information changing the world, or whether this is just the first step of a series of cyber operations. For instance, the use of ransomware and DDoS attacks.

[51] As seen in the CNG/Pronico case: "Pronico - Enlace Hacktivista," Enlace Hacktivista, accessed April 14, 2023, https://enlacehacktivista.org/index.php?title=Pronico.

References

Alejandro, Hiram. Twitter post. October 10, 2022, 6:39 p.m. https://twitter.com/hiramcoop/status/1579526972333383680.

BBC News Mundo. "Jovenel Moïse: la vieja industria de mercenarios colombianos que presuntamente está detrás del asesinato del presidente de Haití." *BBC News Mundo.* July 9, 2021. https://www.bbc.com/mundo/noticias-america-latina-57784827.

Cambio Colombia. "#FiscalíaLeaks: La Mayor Fuga de Información de La Historia." *Cambio Colombia*. January 29, 2023. https://cambiocolombia.com/poder/fiscalialeaks-la-mayor-fuga-de-informacion-de-la-historia.

D, Nicolás Massai. "Perú-files: hackeo al Ejército peruano desnuda sus planes de guerra en caso de un ataque desde Chile." *CIPER Chile*. October 6, 2022. https://www.ciperchile.cl/2022/10/06/peru-files-hackeo-al-ejercito-peruano-desnuda-sus-planes-de-guerra-en-caso-de-un-ataque-desde-chile/.

Dalby, Chris. "Three Criminal Revelations from Mexico's Defense Ministry Leaks." *InSight Crime*. October 12, 2022. https://insightcrime.org/news/three-criminal-revelations-from-mexico-defense-ministry-leaks/.

Dove, Michael. "Indigenous People and Environmental Politics." *Annual Review of Anthropology, 2006* 35, (2006): 191-208. https://www.jstor.org/stable/25064921.

EFE. "Militar vendió armas a criminales, revela hackeo de 'Guacamaya Leaks.'" *El Financiero*. October 9, 2022. https://www.elfinanciero.com.mx/nacional/2022/10/09/sedena-vendio-armas-a-criminales-revela-hackeo-de-guacamaya-leaks/.

El Universal. "López Obrador Defiende a Adán Augusto Tras Guacamaya Leaks Por Supuestas Designaciones," *El Universal*. October 17, 2022. https://www.youtube.com/watch?v=6NtDFXQv8oU.

Enlace Hacktivista. "Enlace Hacktivista," Accessed April 13, 2023. https://enlacehacktivista.org/.

———. "Fiscalia - Enlace Hacktivista," Accessed April 14, 2023. https://enlacehacktivista.org/index.php?title=Fiscalia.

———. "GUACAMAYA NO SOMOS DEFENSORES DE LA VIDA, SOMOS VIDA!,". Accessed April 13, 2023. https://enlacehacktivista.org/comunicado_guacamaya4.txt.

———. "Pronico - Enlace Hacktivista," Accessed April 14, 2023. https://enlacehacktivista.org/index.php?title=Pronico.

———. "RESISTENCIA MILENARIA.," Accessed April 13, 2023. https://enlacehacktivista.org/comunicado_guacamaya.txt.

Espino, Manuel. “Cae mando militar por caso Guacamaya Leaks.” *El Universal.* March 28, 2023. https://www.eluniversal.com.mx/nacion/cae-mando-militar-por-caso-guacamaya-leaks.

———. “Cae mando militar por caso Guacamaya Leaks.” *El Universal*. March 28, 2023. https://www.eluniversal.com.mx/nacion/cae-mando-militar-por-caso-guacamaya-leaks/.

Flores, Nancy. “Con Pegasus, Guacamaya y ‘El rey del cash’, arrecia el golpe blando.” *Contralínea*. October 20, 2022. https://contralinea.com.mx/interno/semana/con-pegasus-guacamaya-y-el-rey-del-cash-arrecia-el-golpe-blando/.

———. “Con Peña, Sedena clasificaba a columnistas en ‘positivos’ y ‘negativos.’” *Contralínea*. October 18, 2022. https://contralinea.com.mx/interno/semana/con-pena-sedena-clasificaba-a-columnistas-en-positivos-y-negativos/.

Forbidden Stories. “‘Mining Secrets’: When There Is Strength in Numbers • Forbidden Stories,” Accessed April 14, 2023. https://forbiddenstories.org/about-mining-secrets/.

Gelsomino, Mark. "The Zapatista Effect: Information Communication Technology Activism and Marginalized Communities". *Faculty of Information Quarterly* 2, no 3 (2010). https://web.archive.org/web/20110816101810/https://fiq.ischool.utoronto.ca/index.php/fiq/article/view/104/256.

Getdaytrends. “Sedena · Worldwide · Twitter Trending Topic.” Accessed April 14, 2023. https://getdaytrends.com/trend/Sedena/.

Guevara, Che. *Guerilla Warfare: A Method*. Peking: Foreign Language Press, 1964. https://www.marxists.org/history/erol/china/che.pdf.

Kitroeff, Natalie, and Ronen Bergman. “Spying by Mexico’s Armed Forces Brings Fears of a ‘Military State.’” *The New York Times*. March 7, 2023. https://www.nytimes.com/2023/03/07/world/americas/mexico-military-surveillance.html.

Richard, Laurent. “‘The Struggle of One Territory Must Be the Struggle of All’,” *Forbidden Stories*, March 6, 2022, https://forbiddenstories.org/about-mining-secrets/.

Marin, Nicolas and Melissa Vida. “‘Hacking Should Be Used to Wake up and Rebel,’ Says Hacker Group Guacamaya,” *Global Voices*. January 10, 2023. https://globalvoices.org/2023/01/10/hacking-should-be-used-to-wake-up-and-rebel-says-hacker-group-guacamaya/.

“Mining Secrets - Distributed Denial of Secrets.” Accessed April 13, 2023. https://ddosecrets.com/wiki/Mining_Secrets.

Morland, Sarah. “Mexican Government Suffers Major Data Hack, President’s Health Issues Revealed.” *Reuters*. September 30, 2022. https://www.reuters.com/world/americas/mexican-president-confirms-hack-government-files-2022-09-30/.

National Security Archive. "Guacamaya Leaks and the Ayotzinapa Case," Accessed April 14, 2023. https://nsarchive.gwu.edu/briefing-book/mexico-ayotzinapa/2023-03-10/guacamaya-leaks-and-ayotzinapa-case.

Noticias Caracol. "La historia secreta del hackeo más grave contra las Fuerzas Militares de Colombia," *Noticias Caracol*. July 12, 2021. https://noticias.caracoltv.com/informes-especiales/historia-secreta-del-hackeo-mas-grave-contra-las-fuerzas-militares-de-colombia.

Recorded Future. "58. Enemy of the State (Part 2): ¿Quién Es Guacamaya? (Who Is Guacamaya?)." Interview by Dina Temple-Raston. *Recorded Future*. March 14, 2023. https://open.spotify.com/episode/4HasAAokUKxeHGMEg71juY.

Reporter, Guardian Staff. "Guatemala Mine's Ex-Security Chief Convicted of Indigenous Leader's Murder." *The Guardian*. October 19, 2022. https://www.theguardian.com/global-development/2021/jan/07/guatemala-nickel-mine-death-adolfo-ich.

———. "Spelling Mistake Prevented Hackers Taking $1bn in Bank Heist." *The Guardian*. May 25, 2017. https://www.theguardian.com/business/2016/mar/10/spelling-mistake-prevented-bank-heist.

Salinas, Cristobal, and A. Lozano. "Mapping and Recontextualizing the Evolution of the Term *Latinx*: An Environmental Scanning in Higher Education." *Journal of Latinos and Education* 18, no. 4 (January 14, 2019): 302–15. https://doi.org/10.1080/15348431.2017.1390464.

Simbolon, Zoe. "Latin America Was the Deadliest Region for Journalists in 2022." *Committee to Protect Journalists*. January 24, 2023. https://cpj.org/2023/01/latin-america-was-the-deadliest-region-for-journalists-in-2022/.

Solway Investment Group. "FENIX PROJECT, GUATEMALA – Solway Investment Group." Accessed April 13, 2023. https://solwaygroup.com/our-business/fenix-project-guatemala/.

Staff, Sc. "LatAm Hacktivist Collective Guacamaya Examined." *SC Media*. January 25, 2023. https://www.scmagazine.com/brief/threat-intelligence/latam-hacktivist-collective-guacamaya-examined.

Temple-Raston, Dina, and Sean Powers. "A Q&A with the Hacktivists Rocking Latin America: Guacamaya," *The Record*. March 28, 2023. https://therecord.media/interview-with-guacamaya-hacktivist-group-latin-america.

Tourliere, Mathieu. "Sedena Leaks: Adán Augusto López entregó la seguridad de Tabasco a presuntos líderes del CJNG." *Proceso*. October 5, 2022. https://www.proceso.com.mx/nacional/2022/10/5/sedena-leaks-adan-augusto-lopez-entrego-la-seguridad-de-tabasco-presuntos-lideres-del-cjng-294663.html.

UNEP. "Indigenous people and nature: a tradition of conservation." Accessed April 14, 2023. https://www.unep.org/news-and-stories/story/indigenous-people-and-nature-tradition-conservation.

Uren, Tom. “Microsoft’s Sociopathic Cybersecurity Pedantry.” *Srslyriskybiz*. October 27, 2022. https://srslyriskybiz.substack.com/p/microsofts-sociopathic-cybersecurity.

Urgente 24. “Por hackeo cayó el Jefe del Estado Mayor Conjunto de Chile.” *Urgente24 - Primer Diario Online Con Las Últimas Noticias De Argentina Y El Mundo En Tiempo Real*. September 23, 2022. https://urgente24.com/mundo/por-hackeo-cayo-el-jefe-del-estado-mayor-conjunto-chile-n544131.

Vicens, Aj. “The Politics and Power of Latin American Hacktivists Guacamaya.” *CyberScoop*. January 23, 2023. https://cyberscoop.com/guacamaya-hacktivist-group-latin-america-interview/.

Walsh, Catherine E. “Pedagogías decoloniales caminando y preguntando: notas a Paulo Freire desde Abya Yala.” *Revista Entramados - Educación Y Sociedad* N. 1 (October 17, 2014): pp 17-30. https://dialnet.unirioja.es/servlet/articulo?codigo=5251817.

CONTACT DETAILS

Twitter: @DSLA_Research

Email: dsla.connect@gmail.com

Website: https://www.dslaresearch.org/