



| Brief |

Continuity Likely After Mexico Elections

Classification: TLP:CLEAR

Criticality: HIGH

Intelligence Requirements: Government, Cybersecurity, Geopolitical

May 29, 2024

Scope Note

*ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 5:00 AM (EDT) on May 29, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

Brief | Continuity Likely After Mexico Elections

Executive Summary

Like the elections in India, South Africa, and now the United Kingdom (UK), there is a clear frontrunner in Mexico's June 2nd general election. Presidential candidate Claudia Sheinbaum of the ruling Movimiento de Regeneracion Nacional (Morena) Party has maintained a 15–30 percent polling lead over her main opponent, Xochitl Galvez, for months and is very likely to be Mexico's next president. Morena will also likely win most of the other 20,000 posts for governor, congress, and local representatives. What matters is the margin of victory; a narrower-than-expected victory will make it difficult for the Morena party to achieve its overarching political reforms and goal of dominating Mexico's political institutions and economy. As with most major elections around the world, orchestrated disinformation campaigns are likely to pose a threat to informed voter behavior. As is normal during Mexican campaigning, violence by criminal groups—towards voters, candidates, and even third-party entities such as election observers and journalists—remains a significant threat to the integrity of the elections.

Morena Dominance

Sheinbaum will very likely replace term-limited President Andres Manuel Lopez Obrador (AMLO), who founded the Morena party. With AMLO unable to run again, he has used his time in office to shape Morena in his image. Sheinbaum's large and stable lead is likely

tied to voter approval of AMLO, and his backing of her as the new leader of Morena indicates to supporters that she will continue his core policies over the next six-year term.

Morena's popularity very likely stems from the perception that AMLO is battling the corruption deeply embedded in Mexico's political institutions after decades of elite rule. At the time he assumed office in 2018, nearly 90 percent of voters believed the government served only the elite.¹ AMLO's approval rating throughout his tenure has been around 65 percent, and perceptions of state institutions have improved during his term.² The lack of credible opposition has likely also helped AMLO maintain his high approval ratings for the entirety of his presidency and allowed Morena candidates to win elections throughout his time in office.

- AMLO buttressed this support by using Morena to push labor law changes to increase the purchasing power of Mexico's large working class through higher minimum wages and infrastructure projects in southern Mexico, traditionally the poorest part of Mexico. He has also pushed a cash-transfer program to about 14 million of the poorest citizens and reportedly lifted 3.5 million out of poverty.³ While these cash handouts are likely unsustainable in the long term, Sheinbaum could suffer politically if she reduces them.
- During AMLO's term, Mexico's economy has performed relatively well, benefiting from growing trade ties with the United States. Mexico's economy has grown at a steady pace under him—over 3 percent in 2023 and even more in southern Mexico.⁴

AMLO's anti-elite rhetoric also likely protects him from opposition criticism mainly aimed at Mexico's worsening insecurity, lack of growth in certain economic sectors, and allegations of democratic backsliding. Critics suggest that, by making politics about Morena and AMLO rather than Sheinbaum, the party's leader can remain relatively unaffected if she performs poorly on certain issues, with voters knowing that the Morena party stands for the working class.

¹ [hXXps://www.latinobarometro\[.\]org/lat.jsp](https://www.latinobarometro.org/lat.jsp)

² [hXXps://www.as-coa.org/articles/approval-tracker-mexicos-president-amlo](https://www.as-coa.org/articles/approval-tracker-mexicos-president-amlo)

³ [hXXps://www.americasquarterly.org/article/the-real-reasons-for-amlos-popularity/](https://www.americasquarterly.org/article/the-real-reasons-for-amlos-popularity/)

⁴

[hXXps://www.banxico\[.\]org\[.\]mx/publicaciones-y-prensa/reportes-sobre-las-economías-regionales/reportes-economías-regionales.html](https://www.banxico[.]org[.]mx/publicaciones-y-prensa/reportes-sobre-las-economías-regionales/reportes-economías-regionales.html)

- AMLO has eliminated certain policing powers and given them to a new security force he created, the Guardia Nacional (GN).⁵ However, crime has continued to increase, with drug cartels controlling large swaths of the economy and GN in charge of certain economic and infrastructure projects that would normally fall to other institutions or the private sector.⁶
- While Mexico's economy has grown steadily under AMLO, it has not diversified well beyond exports or trade with the United States, leaving AMLO open to criticism that Mexico has not taken full advantage of the trade opportunities presented because of the Western trade war with China. Foreign investors are also critical of many of AMLO's economic policies, which prioritize Mexican companies or institutions over more efficient private sector or multinational corporations.
- AMLO has dedicated much of his tenure to pursuing projects without clear economic benefits. Mexico has given USD 90 billion to the indebted state oil company PEMEX during the AMLO administration at the expense of increasing renewable energy generation.⁷ Again, previous credible corruption allegations at PEMEX and across Mexico's political institutions have likely shielded him from criticism.

AMLO is very likely to maintain political influence beyond the election and will push Morena to exert greater influence across Mexico's institutions. Sheinbaum's support for GN and PEMEX will be key benchmarks when determining how much influence AMLO maintains once he leaves office. If Sheinbaum diminishes their influence, it could be a signal that she will attempt more significant changes; however, if she maintains financial support for PEMEX and continues to cede security power to GN, then it likely means a continuation of the AMLO government.

⁵ [hXXps://seguridad.nexos\[.\]com.mx/el-futuro-de-la-guardia-nacional-de-amlo-dos-escenarios/](https://seguridad.nexos[.]com.mx/el-futuro-de-la-guardia-nacional-de-amlo-dos-escenarios/)

⁶

[hXXps://www.bloomberg\[.\]com/news/features/2024-04-18/mexico-president-amlo-traded-security-for-infrastructure-during-his-term](https://www.bloomberg[.]com/news/features/2024-04-18/mexico-president-amlo-traded-security-for-infrastructure-during-his-term)

⁷

[hXXps://www.reuters\[.\]com/business/energy/fallout-mexican-presidents-pemex-rescue-set-greet-successor-2024-02-23/](https://www.reuters[.]com/business/energy/fallout-mexican-presidents-pemex-rescue-set-greet-successor-2024-02-23/)

Democratic Backsliding

AMLO's political opponents have attempted to tie Morena officials' efforts to exercise more control over Mexico's institutions to democratic backsliding, arguing these institutions will pursue Morena objectives rather than impartial ones.

In addition to exerting greater control of PEMEX, AMLO has pushed to have judges be popularly elected (giving them an incentive to be pro-Morena),⁸ attempted to gain more control of the electricity sector,⁹ nationalized the lithium industry, and attempted a series of electoral reforms that would benefit the Morena party.¹⁰

Critics argue that these institutions must remain independent and be improved but are having difficulty communicating this, likely because voters would rather have those institutions beholden to Morena than to parties that largely operated at the behest of elites.

During his tenure, AMLO has been accused of using the state to influence institutions that are hostile towards him, including by using spyware to influence journalists covering his administration.

- While AMLO was initially the victim of Pegasus spyware, a cyber espionage malware tool, he continued to use it.¹¹ This spyware infected the phones of activists from the Miguel Agustín Pro Juárez Human Rights Center, an organization known for exposing governmental abuses—including those by the Mexican Army. Under AMLO's administration, at least three human rights activists and two journalists have been illegally spied on using Pegasus. Press reports suggest the Mexican Army (currently the only government agency with access to Pegasus) is responsible for these surveillance activities.¹²¹³

⁸

[hXXps://elpais\[.\]com/mexico/2023-12-20/sheinbaum-se-aparta-del-plan-de-lopez-obrador-para-que-los-ministros-de-la-corte-sean-elegidos-por-voto-popular.html](https://elpais.com/mexico/2023-12-20/sheinbaum-se-aparta-del-plan-de-lopez-obrador-para-que-los-ministros-de-la-corte-sean-elegidos-por-voto-popular.html)

⁹ [hXXps://americasquarterly\[.\]org/article/blackout-politics-amlos-energy-plan-will-backfire/](https://americasquarterly[.]org/article/blackout-politics-amlos-energy-plan-will-backfire/)

¹⁰ [hXXps://www.americasquarterly\[.\]org/article/the-next-front-in-mexicos-battle-over-institutions/](https://www.americasquarterly[.]org/article/the-next-front-in-mexicos-battle-over-institutions/)

¹¹ [hXXps://thewire\[.\]in/world/mexico-election-spyware-pegasus-surveillance](https://thewire[.]in/world/mexico-election-spyware-pegasus-surveillance)

¹²

[hXXps://apnews\[.\]com/article/mexico-pegasus-spyware-activists-press-freedom-army-76477e1d4e3e09250e20aa4896b1f9e1](https://apnews[.]com/article/mexico-pegasus-spyware-activists-press-freedom-army-76477e1d4e3e09250e20aa4896b1f9e1)

¹³ [hXXps://www.nytimes\[.\]com/2023/04/18/world/americas/pegasus-spyware-mexico.html](https://www.nytimes[.]com/2023/04/18/world/americas/pegasus-spyware-mexico.html)

- Mexico's Attorney General reportedly ordered Mexico's largest telecom company to provide phone records, texts, and location data of over a dozen prominent Mexican officials and politicians, according to 14 reviewed orders.¹⁴

Insecurity

A crackdown on drug cartel activity would likely prompt a violent backlash from the cartels. Even under AMLO's tenure, there were frequent instances of mass violence whenever a key cartel member was targeted by security forces—including random killings, mass instances of vandalism, and sophisticated attacks on security forces designed to deter further actions.

- For example, August 2022 saw a wave of cartel-related violence across Mexico, led by the large border cities of Tijuana and Ciudad Juarez. There, cartels instigated highly publicized acts of violence—like torching dozens of cars at once in Tijuana or large-scale street and prison battles in Ciudad Juarez—after the arrest of key leaders.¹⁵ There were similar scenes of violence just weeks earlier in Jalisco and Guanajuato states, the bases for Mexico's two largest illicit economies in recent years: drug trafficking and oil smuggling (Huachicol).¹⁶

There have been relatively few instances of mass violence since, and critics suggest that Morena has reached an unspoken truce to allow cartels access to wide swaths of the economy in exchange for a certain level of peace—a policy that would continue under Sheinbaum.

- The homicide rate reached an all-time high in AMLO's first year in office and is 8 percent higher than under the previous administration,¹⁷ which did not have a good record on crime.
- Perhaps underscoring AMLO's popularity and the overall distrust of the old guard, Morena supporters point out that the homicide rate has improved under AMLO, decreasing from 28 per 100,000 after his first year in office to 25 per 100,000 since.¹⁸

¹⁴ [hXXps://www.nytimes\[.\]com/2023/11/09/world/americas/mexico-surveillance-attorney-general.html](https://www.nytimes.com/2023/11/09/world/americas/mexico-surveillance-attorney-general.html)

¹⁵ [hXXps://www.bbc\[.\]com/news/world-latin-america-62537830](https://www.bbc[.]com/news/world-latin-america-62537830)

¹⁶ [hXXps://politica.expansion.mx/mexico/2022/08/10/violencia-jalisco-guanajuato-detencion-de-lideres-criminales](https://politica.expansion.mx/mexico/2022/08/10/violencia-jalisco-guanajuato-detencion-de-lideres-criminales)

¹⁷ [hXXps://www.as-coa\[.\]org/articles/mexico-elects-whats-play-countrys-massive-elections](https://www.as-coa[.]org/articles/mexico-elects-whats-play-countrys-massive-elections)

¹⁸ [hXXps://delitosmexico.onc\[.\]org\[.\]mx/](https://delitosmexico.onc[.]org[.]mx/)

National polling on positive perceptions of safety from voters has notably increased as well.¹⁹

Collusion between security forces under Morena and cartels was reportedly exposed in a region-wide data breach by hacker group Guacamaya in 2023.

- The breach exposed incidents of corruption within Mexican security forces, including GN members allegedly accepting bribes from Huachicol thieves in August and a state police officer in Jalisco selling military-grade weapons to cartel members in June. The leaked classified material includes internal communications, personal information of soldiers, intelligence on drug traffickers and other criminals, and civil complaints about crimes. Disclosure of this sensitive information could have disastrous consequences if accessed by malicious actors, but it also underscored the military's influence over civilian affairs under Morena.²⁰

Contrasting with the Morena approach, Sheinbaum's main opponent, Galvez, is campaigning for a tougher crackdown on criminal activity.

- Multiple Mexican presidents have pursued a tougher-on-crime approach, including AMLO at the beginning of his tenure. These efforts have all been unsuccessful, as doing so requires rooting out corrupt officials while maintaining morale as violence escalates; meanwhile, foreign investment either departs or holds off as the security situation deteriorates.
- The potential positives of rooting out corruption and regaining control of institutions from criminal groups have never materialized.

During the campaign season, this has translated into a typical wave of violence against politicians.

- Over 270 political candidates have sought government protection ahead of the upcoming June general election. This security concern follows the assassination of at least 15 federal-level candidates and attacks on 28 others during the current

¹⁹[hXXps://www.inegi\[.\]org\[.\]mx/contenidos/programas/ensu/doc/ensu2023_septiembre_presentacion_ejecutiva.pdf](https://www.inegi.org.mx/contenidos/programas/ensu/doc/ensu2023_septiembre_presentacion_ejecutiva.pdf)²⁰ [hXXps://cyberscoop\[.\]com/guacamaya-hacktivist-group-latin-america-interview/](https://cyberscoop.com/guacamaya-hacktivist-group-latin-america-interview/)

campaign season.²¹ Additionally, in the lead-up to Mexico's June 2024 elections, two attacks on mayoral candidates in the southern state of Chiapas have resulted in nine deaths, as reported by the prosecutor's office in this crime-ridden region. Since September of the previous year, over two dozen politicians have been killed, including a mayoral candidate who was shot dead last month at the start of her campaign. This wave of violence highlights the severe dangers faced by political candidates in Mexico.²²

The high level of political violence during this campaign has had little influence on voter intentions, with Morena candidates holding steady leads throughout the last year.²³ However, the issue will likely be significant for the next administration. If these policies remain, they will likely slowly impact the Mexican economy. As criminal groups then move further into more formal sectors of the economy, it will likely decrease economic effectiveness and turn off foreign investors.

- Permitting cartel expansion would also likely weaken certain institutions, like security or entities responsible for regulating the economic sectors into which cartels move.
- However, Morena's approach likely avoids the large economic impact that a major security crackdown would bring. Mexico would then need to expend resources to combat the well-armed cartels, who would likely increase their violence in response. A wait-and-see approach will strengthen the cartels, and eventually, it will become politically impossible not to launch a military response.

| Political Cyber Influence Operations

Disinformation

Mexican elections have a recent history of utilizing disinformation campaigns to manipulate public opinion. ZeroFox anticipates a surge in fake news and disinformation

²¹

[hXXps://www.semafor\[.\]com/article/04/19/2024/mexican-election-campaign-marred-by-skyrocketing-political-violence](https://www.semafor.com/article/04/19/2024/mexican-election-campaign-marred-by-skyrocketing-political-violence)

²²

[hXXps://www.cbsnews\[.\]com/news/deadly-attacks-political-candidates-pre-election-death-toll-mounts-chiapas-mexico/](https://www.cbsnews.com/news/deadly-attacks-political-candidates-pre-election-death-toll-mounts-chiapas-mexico/)

²³ [hXXps://www.as-coa.org/articles/poll-tracker-mexicos-2024-presidential-vote](https://www.as-coa.org/articles/poll-tracker-mexicos-2024-presidential-vote)

(including via the wide use of generative AI technology to disseminate inaccurate information that includes manipulated images and messages). However, it is unclear if this will significantly influence the outcome of the upcoming presidential election, with voters likely already deciding on their preferred candidate well before June.

- In 2013, the Mexican government utilized Peñabots (automated social media accounts) to inflate support for candidate Enrique Peña Nieto, including deploying them to amplify his social media presence and artificially boost his follower count.²⁴ At the time, tactics such as automatic reposting of government officials' posts and purchasing fake social media followers were employed to create a false impression of widespread backing for Peña Nieto and his policies and were notably seen during instances like the promotion of energy reform.
- During Mexico's 2018 presidential election, social media activity saw a significant amount of misleading content, with bots and influencers contributing nearly one-fifth of some social media content in March 2018.²⁵
- A surge in fake news and disinformation online has raised concerns, as some falsehoods appear to originate from Morena. Since June, over 40 fake publications have been observed favoring or discrediting both political factions.²⁶

Hacktivism and Data Breaches

A Colombian hacker played a significant role in Enrique Peña Nieto's 2012 presidential election victory in Mexico. Employing malware, fake social media accounts, and bots, the hacker orchestrated a digital dark arts campaign to manipulate public opinion—demonstrating the potential of hacktivism to influence electoral outcomes. The hacker's tactics included backing Peña Nieto's policies and creating discord among rival supporters, demonstrating the influence of cyber operations in electoral outcomes.²⁷ This incident underscores the power of blackhat propaganda in shaping public opinion during the elections.

²⁴ [hXXps://medium\[.\]com/datasociety-points/rise-of-the-pe%C3%Blabots-d35f9fe12d67](https://medium.com/datasociety-points/rise-of-the-pe%C3%Blabots-d35f9fe12d67)

²⁵ [hXXps://www.codastory\[.\]com/rewriting-history/mexico-election-disinformation/](https://www.codastory.com/rewriting-history/mexico-election-disinformation/)

²⁶

[hXXps://apnews\[.\]com/article/mexico-fake-news-social-media-elections-2024-487943383b8f57f5eb0cc9ae1324fc1](https://apnews.com/article/mexico-fake-news-social-media-elections-2024-487943383b8f57f5eb0cc9ae1324fc1)

²⁷ [hXXps://www.theguardian\[.\]com/world/2016/mar/31/mexico-presidential-election-enrique-pena-nieto-hacking](https://www.theguardian.com/world/2016/mar/31/mexico-presidential-election-enrique-pena-nieto-hacking)

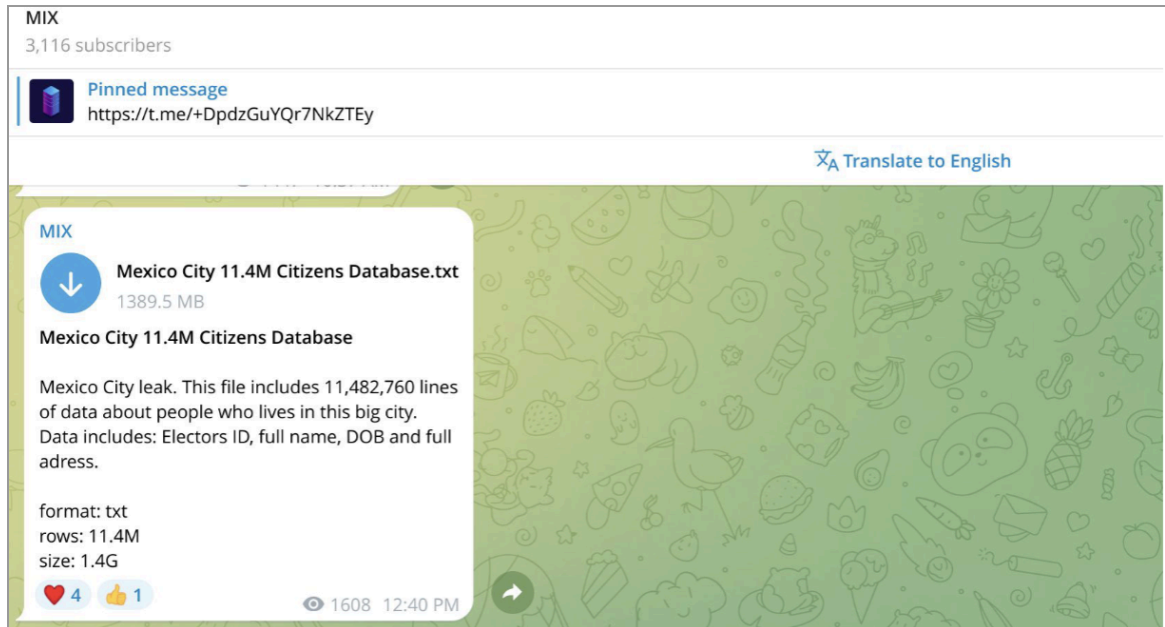
One of the key cybersecurity features of Latin American governments in recent years has been their increasing use of surveillance technologies that track movements, obtain secure communications, and build large databases of citizen data. These nascent technologies do not come with an increased focus on cyber and data protection, and data breaches are common across the region.

Data breaches have a roughly equal chance of interfering with the electoral process and often involve the compromise of specific individuals' personally identifiable information (PII). Sensitive security details to protect the electoral process could also be revealed by such acts, which could potentially weaken the election process. ZeroFox assesses there is a likely chance that threat actors will target the electoral body of Mexico, given various entities' capabilities to breach systems in the past and use this information to expose internal state machinations.²⁸²⁹

- On April 15, 2024, a database of Mexico City citizens was shared on the Telegram channel [t\[.\]me/mix_db](https://t.me/mix_db). The file includes 11,482,760 lines of data associated with citizens of the Mexican capital city and consists of electors' IDs, full names, dates of birth, and complete addresses. The size of the dataset is 1.4 GB. Threat actors may leverage this information for malicious campaigns during the upcoming elections.

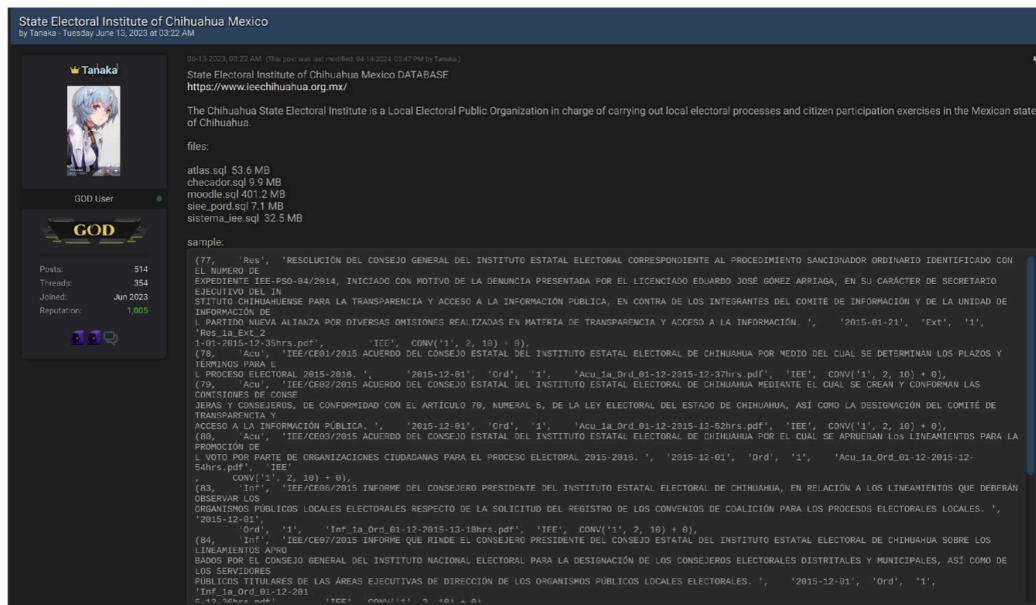
²⁸ [hXXps://www.reuters\[.\]com/world/americas/mexican-president-confirms-hack-government-files-2022-09-30/](https://www.reuters.com/world/americas/mexican-president-confirms-hack-government-files-2022-09-30/)

²⁹ [hXXps://www.washingtonexaminer\[.\]com/news/2144244/mexican-cartels-exploit-us-governments-cbp-one-app/](https://www.washingtonexaminer.com/news/2144244/mexican-cartels-exploit-us-governments-cbp-one-app/)

**Mexico City database shared on the Telegram channel MIX (t[.]me/mix_db**

Source: ZeroFox Internal Collections

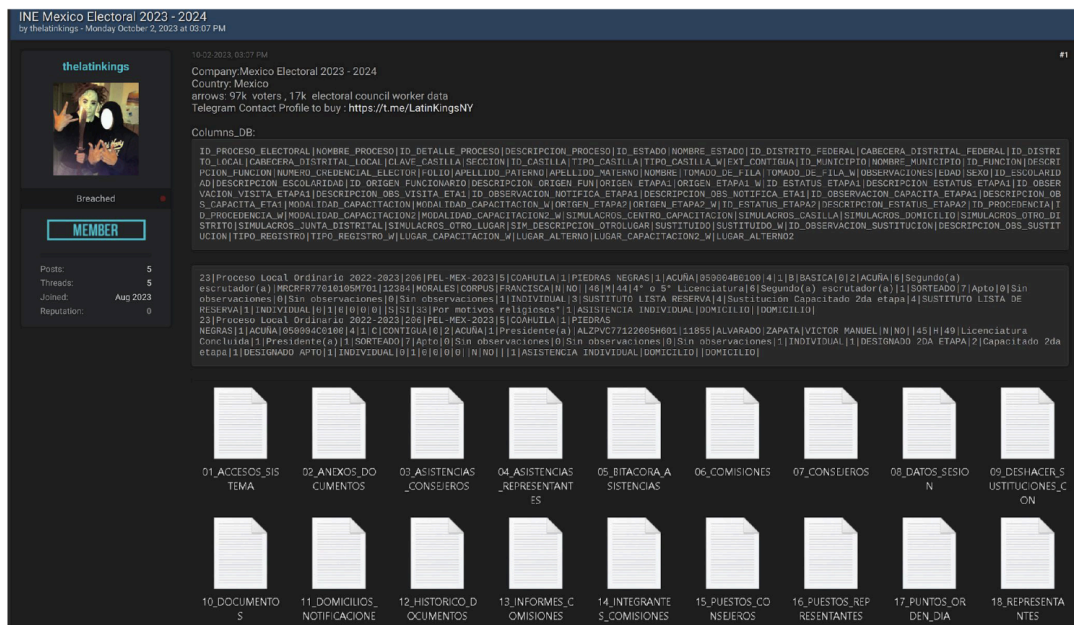
- On June 13, 2023, BreachForums user “Tanaka” shared leaked databases from the State Electoral Institute of Chihuahua, Mexico. The Chihuahua State Electoral Institute is in charge of carrying out local electoral processes and citizen participation exercises in the Mexican state of Chihuahua. Even though most of the records inside these files are from 2021, bad actors can still use such information for malicious campaigns during the elections and for social engineering.



Tanaka shares leaked databases of the Electoral Institute of Chihuahua, Mexico

Source: ZeroFox Collections

- On May 13, 2023, English-speaking member “MorphoSploit” shared a large Mexican electoral set related to the Coahuila State Elections on the LeakBase forum. According to the actor, the leaked files are associated with a former representative of the Congress of the State of Coahuila and other members of the Mexican Congress. All the leaked files were uploaded on the former web-based file-sharing service AnonFiles, and the full set is no longer accessible. However, ZeroFox is confident that this set was downloaded thousands of times before the decommissioning of the service. MorphoSploit mentioned that he was going to leverage these leaks for election complaints and election traps during the June 2023 elections.
- On November 2, 2023, a member of the data leaks forum Breach Forums, “thelatinkings” advertised a data set of the “Instituto Nacional Electoral, Mexico” (INE). The seller claims that the data set is relevant to 2023 and 2024 and consists of 97,000 lines with voter information and 17,000 records of electoral council worker data. The actor shared a data sample from the database:



Original post by a threat actor, “thelatinking” on Breach Forums

Source: ZeroFox Collections

Conclusion

Mexico’s political status quo is likely to remain after the June 2024 elections. Outgoing President AMLO has used his time in office to create a political party in his popular image, and members of the Morena Party can be expected to operate as an extension of him. Those concerned about data protection, worsening criminality, and government intervention in private-sector industries will likely remain frustrated. However, the trade, financial services, and infrastructure sectors will likely benefit from the continuity and can expect continued growth.

| Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

| Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%