CROWDSTRIKE

2025

LATIN AMERICA THREAT LANDSCAPE REPORT

Table of Contents

Executive Summary

The CrowdStrike 2025 Latin America Threat Landscape Report provides key insights into cyber activity across Central and South America, the Caribbean, and Mexico, offering intelligence on targeted intrusions, eCrime, and hacktivism. Designed to inform regional stakeholders, the report examines emerging threats and adversary tactics, equipping organizations with the intelligence needed to navigate Latin America's (LATAM's) evolving security landscape.

This report is produced by the CrowdStrike Counter Adversary Operations team, which integrates two closely aligned groups. The CrowdStrike Intelligence team delivers actionable reporting that identifies new adversaries, tracks their activities, and monitors emerging cyber threats in real time. Leveraging this intelligence, the CrowdStrike OverWatch team conducts proactive threat hunting across customer telemetry, detecting and addressing malicious activity before it escalates.

Throughout 2024, CrowdStrike Intelligence observed both macro and micro trends shaping LATAM's cybersecurity posture. The macro cyber trends that transcended regional boundaries and nation-state borders include governments bolstering their domestic cybersecurity infrastructure as well as engaging in collaboration and knowledge sharing with foreign partners. On a micro level, trends include governments addressing politically sensitive policy questions regarding whether to include Chinese technology vendors in the bidding process for government contracts, effective stewardship of AI technology, and governments announcing investigations into the domestic weaponization of spyware to surveil political opponents.

LATAM remained a growing target for both regional and global eCrime adversaries. As of this writing, CrowdStrike Intelligence tracks six named adversaries — OCULAR SPIDER, BLIND SPIDER, ODYSSEY SPIDER, PLUMP SPIDER, SAMBA SPIDER, and SQUAB SPIDER — that are either based in or primarily targeting the region. These adversaries are further enabled by regional adversaries such as ROBOT SPIDER, which operates the *CryptersAndTools* (or *Fsociety*) crypter as a service (CaaS). To evade detection, LATAM-focused threat actors continue to prioritize defense evasion by adopting novel tactics, techniques, and procedures (TTPs), including using newer programming languages such as Rust; this activity highlights threat actors' interest in adapting to the current eCrime ecosystem.

Though state-nexus adversaries from China, Colombia, the Democratic People's Republic of Korea (DPRK), and Russia account for a small fraction of the global activity targeting LATAM, their targeting strategies are highly dependent on geopolitical factors, sectoral priorities, and external events; therefore, they typically align operations with national strategic objectives and emerging trends.

Geopolitical events and perceived country-specific domestic governance issues were the primary drivers for global hacktivist activity against LATAM countries, while regional government entities leveraged surveillance technology to quell unrest or dissent.

As LATAM's cyber threat landscape continues to evolve, organizations must stay vigilant against a diverse array of adversaries, from cybercriminal groups to state-backed actors and hacktivists. By leveraging intelligence-driven security strategies, regional stakeholders can strengthen their defenses, mitigate risks, and stay ahead of emerging threats in an increasingly complex threat landscape.

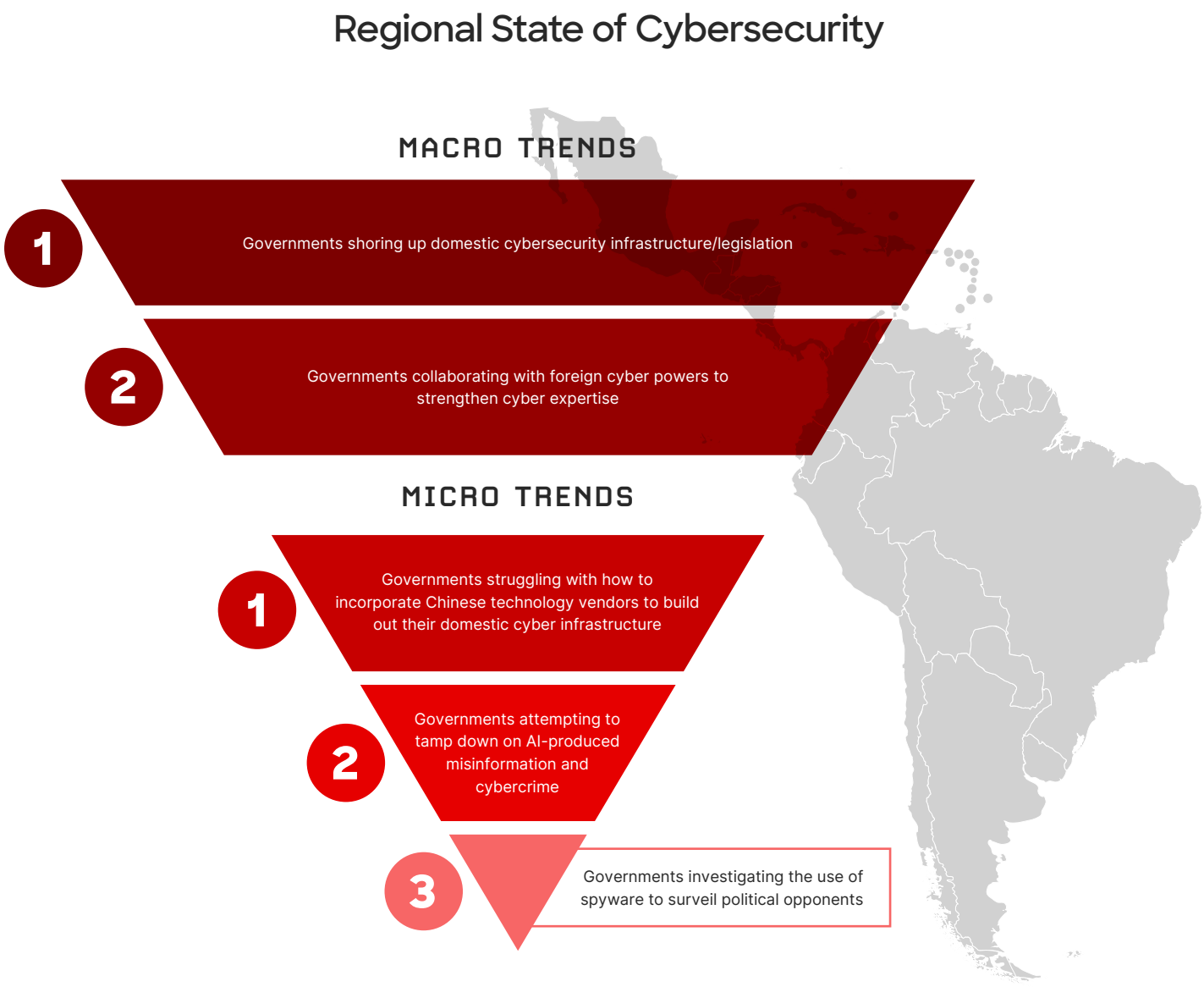

Figure 1. Cyber trends in Latin America

NAMING CONVENTIONS

ADVERSARY	NATION-STATE OR CATEGORY
BEAR	RUSSIA
BUFFALO	VIETNAM
CHOLLIMA	DPRK (NORTH KOREA)
CRANE	ROK (REPUBLIC OF KOREA)
HAWK	SYRIA
JACKAL	HACKTIVIST
KITTEN	IRAN
LEOPARD	PAKISTAN
LYNX	GEORGIA
OCELOT	COLOMBIA
PANDA	PEOPLE'S REPUBLIC OF CHINA
SAIGA	KAZAKHSTAN
SPHINX	EGYPT
SPIDER	eCRIME
TIGER	INDIA
WOLF	TURKEY

Overview of Cyber Trends

Central America

MACRO TRENDS

Throughout 2024, Central American governments took steps to pass cyber legislation to strengthen their domestic cybersecurity infrastructure, including establishing legal frameworks and attempting to align their domestic cyber legislation with international cyber conventions. This cyber legislation resulted in some governments — such as the government of El Salvador — creating national cybersecurity agencies. In other countries, such as Nicaragua, these laws spurred serious concerns about potential data privacy violations (Figure 2).

In 2024, Central American governments either organized or attended forums with foreign partners, including bilateral meetings with the U.S. and European Union (EU), almost certainly in an effort to share cybersecurity best practices to strengthen their domestic cyber posture.

Figure 2. Cyber trends in Central America

The most prominent example of a Central American government leveraging bilateral engagement with the U.S. and EU is Costa Rica. Since a 2022 WIZARD SPIDER ransomware attack affected the Costa Rican government, Costa Rica has received an influx of international support, including the U.S. providing $25 million USD for the construction of the country's national cybersecurity SOC.[1]

In October 2024, the Costa Rican government announced a new cyber intelligence laboratory, a forensic laboratory, and a secure information exchange network for public institutions, partly funded by the EU.[2]

1 http://wired.com/story/costa-rica-ransomware-conti/
https://weforum.org/stories/2024/05/latin-america-cybersecurity-report-ransomware-attacks/
https://cr.usembassy.gov/united-states-announces-25-million-to-strengthen-costa-ricas-cybersecurity/

2 https://elpais.cr/2024/10/22/costa-rica-tendra-laboratorio-forense-para-enfrentar-la-ciberdelincuencia/

MICRO TRENDS

Adoption of Chinese information and communications technology (ICT) and surveillance technology in Central America has been uneven; some countries diplomatically closer to the U.S. remain wary of additional Chinese infrastructure investment while other countries have welcomed Chinese technology companies.

In 2023, the Costa Rican government attempted to impose cybersecurity regulations that served as a de facto ban on Huawei as a domestic 5G technology provider; however, in February 2024, a Costa Rican court temporarily suspended this ban while reviewing its legal validity.[3] Then, in late 2024, the Costa Rican president issued a decree upholding the Huawei ban, citing national security concerns.[4]

Additionally, Costa Rican government officials filed a complaint against Huawei with accusations including bribery, fraud, and influence peddling.[5] In a separate but related event, U.S. and Costa Rica officials released a December 2024 joint statement claiming that a "comprehensive cybersecurity review of Costa Rica's critical infrastructure … revealed that China-based malicious actors had infiltrated the Central American country's networks."[6]

In contrast, Panama has been more welcoming to Chinese ICT investment. In May 2024, Huawei announced it had chosen Panama as the site of its first Cybersecurity and Transparency Center for Latin America, claiming to have chosen Panama because of its geographic location and emphasizing that this center's creation was to exchange information on cybersecurity and display the company's willingness to "show its transparency."[7]

Over the past year, concerns over AI-enabled cybercrime have increased in Central America. In February 2024, the Costa Rican government issued a warning over a surge of victims falling prey to fraudulent schemes employing fake AI-generated videos featuring the faces of public figures.[8] In July 2024, the Belize government warned about a fake AI-generated message from the Minister of Health that was "not sanctioned or produced by the government."[9]

There was limited publicly available information regarding Central American governments leveraging commercial spyware to monitor political opponents or conduct domestic surveillance.

MEXICO[10]

On October 1, 2024, Claudia Sheinbaum Pardo was inaugurated as the President of Mexico. As an ally to her predecessor, Andrés Manuel López Obrador (AMLO), Sheinbaum is almost certain to advance a similar agenda. At the end of AMLO's tenure, the Mexican government's cybersecurity posture remained a work in progress and was largely reactionary in response to widely publicized cyber incidents.

---

3 https://www.rcrwireless.com/20240214/5g/costa-rican-court-suspends-exclusion-huawei-5g-provider
https://www.bnamericas.com/en/news/costa-rican-court-suspends-5g-cybersecurity-regulations

4 https://ticotimes.net/2024/12/18/costa-rica-and-u-s-jointly-identify-alleged-cyber-intrusions-from-china

5 https://observador.cr/gobierno-denuncia-penalmente-a-huawei-y-a-5-funcionarios-del-ice-por-contratos-otorgados-durante-la-ultima-decada

6 https://dialogo-americas.com/articles/costa-rica-us-cybersecurity-collaboration-uncovers-chinese-espionage/
https://x.com/usembassysjo/status/1869047401224290614

7 https://prensa.com/economia/huawei-elige-a-panama-para-crear-su-primer-centro-regional-de-ciberseguridad-y-transparencia

8 https://ticotimes.net/2024/02/28/costa-rica-issues-warning-over-surge-in-deep-fake-video-scams

9 https://lovefm.com/belize-battles-rising-cybercrime-with-advanced-ai-amidst-misinformation-concerns/

10 Note: Mexico is geographically on the North American continent. However, the country is also considered LATAM for sociocultural factors (e.g., the official use of the Spanish language), historical ties to Central America (e.g., indigenous populations), and social connections to the region.

Since taking office, Sheinbaum has centered technological innovation in her economic development plans, pledging to create a Cybersecurity and AI center as well as domestically and autonomously produce low-cost drones and encrypted telecommunications and diagnostic technologies.[11]In mid-November 2024, the Mexican government announced plans for a National Digital Transformation and Telecommunications Agency that would be responsible for the rollout of national digital identity, cloud computing, and satellite technology projects.[12] Additionally, a draft cybersecurity law remains pending, largely due to a lack of cohesion among legislators and stakeholders. If passed, the legislation would mandate the creation of a National Cybersecurity Center, which would spearhead cybersecurity policies and implementation.[13]

South America

MACRO TRENDS

In 2024, South American governments focused on drafting national digital strategies, authorizing the creation of national cybersecurity entities, and penalizing cybercrime. Most of the cyber legislation prioritized drafting national cyber or digital strategies, with some countries — such as Chile — additionally establishing National and Defense Computer Security Incident Response Teams (CSIRTs). Other countries, such as Uruguay, passed cyber legislation outlining their national cybersecurity strategy while implementing penalties for cybercrimes such as online harassment, data breaches, identity theft, and unauthorized access to computer systems (Figure 3).

South American governments strengthened their domestic cybersecurity posture via bilateral agreements with regional and global counterparts focusing on cyber defense cooperation and international cybercrime convention adherence. For example, in March 2024 and April 2024, respectively, the Argentine and Uruguayan governments signed Memorandums of Understanding (MOUs) with the U.S. to strengthen bilateral cyber defense cooperation and public-private technology partnerships.[14]

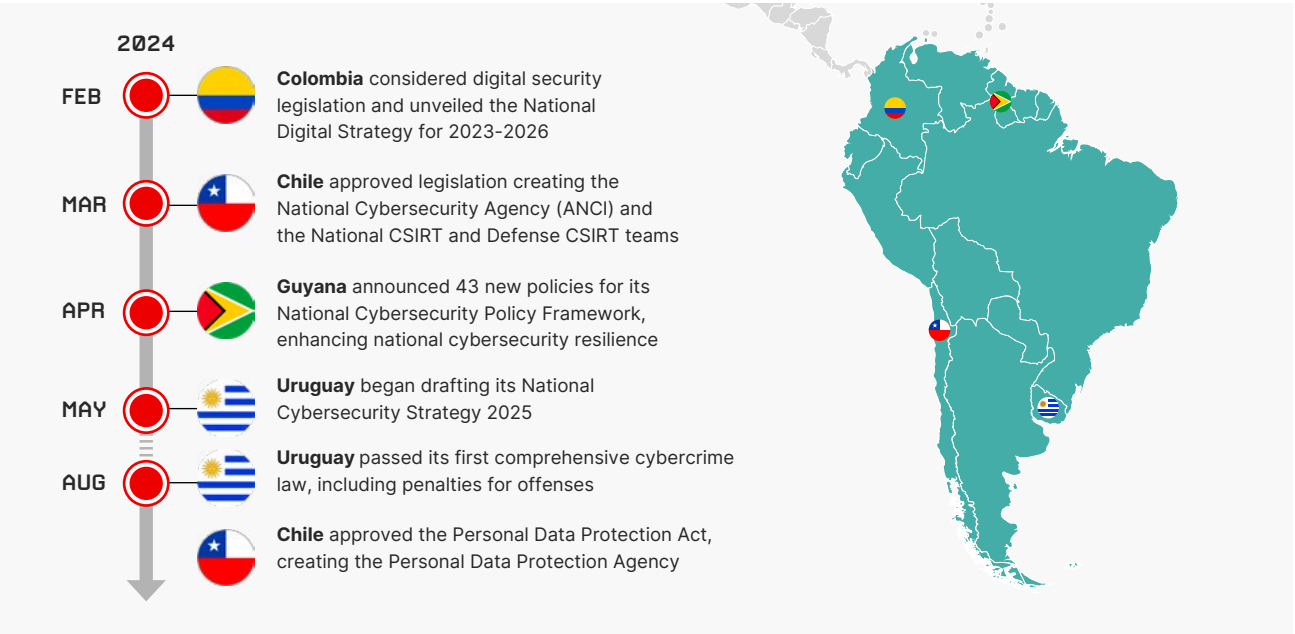

Figure 3. Cyber trends in South America

11 https://elpais.com/mexico/2024-10-02/estas-son-las-100-promesas-de-claudia-sheinbaum-como-presidenta-de-mexico.html

12 https://eleconomista.com.mx/politica/gobierno-presenta-agencia-transformacion-digital-y-telecomunicaciones-20241114-734183.html

13 https://es.wired.com/articulos/presentan-nuevo-proyecto-de-ley-para-garantizar-la-ciberseguridad-en-mexico

14 https://www.zona-militar.com/en/2024/03/26/argentina-signs-a-memorandum-of-understanding-with-the-u-s-to-strengthen-collaboration-in-cyberdefense-issues/ https://en.mercopress.com/2024/04/11/key-cooperation-deal-between-the-us-and-uruguay-signed

In November 2024, the Chilean Interior Minister and several EU representatives signed an agreement to cooperate on cybersecurity and "increase the cyber resilience" of LATAM countries.[15] In September 2024, Paraguay became a signatory to an expanded version of an EU-driven cybercrime convention that updated provisions on data sharing between internet service providers (ISPs) based in signatory countries and government authorities.[16]

South American governments either organized or attended bilateral or multilateral military exercises that included cybersecurity simulations, highlighting the increasing need to address defensive cyber operations in military strategy. For example, in August 2024, Chile and Brazil held their first bilateral Cyber Shield exercise in Santiago, Chile, to develop military and civilian cyber defensive capabilities by having participants face several scenarios and incidents for which they had to quickly draft a response to a simulated cyber crisis.[17]

Separately, in September 2024, six South American naval units engaged in a cybersecurity exercise called UNITAS 24, which included practical exercises in cyber operations.[18] Lastly, in November 2024, CRUZEX, one of the largest multinational military exercises in Latin America, expanded its scope to include a cyber scenario.[19]

Iran Engages in "Technology Diplomacy" with Regional LATAM Partners

In 2024, Iran deepened its South American regional interests through what it has termed "technology diplomacy," investing in selective alliances with a small group of authoritarian governments hostile to U.S. influence in the region, particularly Venezuela and Cuba. In late 2024, Iran's Minister of Information and Communications Technology (MICT) visited Venezuela and Cuba to sign several MOUs on the cooperative development of advanced technology, including ICT, AI, electronic governance, cybersecurity, and information operations.[20] This latest Latin American state tour is indicative of sustained legacy initiatives from Iran's previous presidential administration, demonstrating the continuity of Iran-Latin America policy across political transitions and Iranian presidential administrations.

MICRO TRENDS

South American governments have taken varying approaches to incorporating Chinese technology into their domestic cyber infrastructure, with highly competitive pricing likely eroding security concerns.

In April 2024, while Colombia was building its 5G network, private sector experts warned about the risks associated with technology provided by Chinese companies.[21] These warnings followed the publication of a private sector report titled "The Footprint of Chinese Technology in Colombia," which described the trade-off of increased technical sophistication for privacy.[22]

---

15 https://infobae.com/america/agencias/2024/11/08/chile-y-la-ue-firman-un-acuerdo-de-cooperacion-en-ciberseguridad-para-latinoamerica/

16 https://coe.int/en/web/cybercrime/-/paraguay-becomes-the-47th-state-to-sign-the-second-additional-protocol-to-the-convention-on- cybercrime

17 https://dialogo-americas.com/articles/chile-brazil-strengthen-cyber-defense-through-binational-exercise/

18 https://www.defensa.com/centro-america/armada-republica-dominicana-primera-ejercicios-cyber-unitas-24

19 https://www.southcom.mil/MEDIA/NEWS-ARTICLES/Article/3970832/cyber-operations-takes-stage-at-cruzex-2024/

20 https://www.tehrantimes.com/news/505807/Tehran-Caracas-sign-MOUs-on-ICT

21 https://dialogo-americas.com/articles/experts-warn-about-risks-from-chinas-5g-technology-in-colombia/

22 https://dialogo-americas.com/articles/warning-risks-of-chinese-technology-in-colombia/
https://asiapowerwatch.com/colombia-is-unprepared-to-handle-the-risks-of-chinese-tech-investment/

Separately, in April 2024, Brazilian President Luiz Inácio Lula da Silva dismissed security concerns regarding agreements to establish a semiconductor working group with China and expand Chinese involvement in developing Brazil's cybersecurity technology and 5G mobile infrastructure.[23] As of January 2025, Argentina, Bolivia, Brazil, Chile, Colombia, Ecuador, Peru, Suriname, and Uruguay used or planned to use Huawei equipment in their 5G networks.[24]

South American governments took steps to address AI-generated electoral misinformation while also attempting to discover avenues to leverage AI for socioeconomic growth. For example, in February 2024, the Brazilian Superior Electoral Tribunal (TSE) adopted new rules to address the spread of online electoral disinformation and restrict the use of AI during the electoral campaign process ahead of October 2024 municipal elections.[25] The new regulations included stricter liability rules and other obligations for online platforms and required that campaign materials clearly disclose, watermark, or label AI-generated content.

In March 2024, the European Union-Latin America and the Caribbean (EU-LAC) Digital Alliance discussed how to identify and mitigate AI's risks while capitalizing on socioeconomic growth opportunities.[26] In August 2024, representatives from 17 South and Central Latin American countries met in Colombia and signed a declaration focused on AI governance, ecosystem building, and education.[27]

In 2024, South American governments pursued several public investigations that were tied to surveillance of political opponents or civil society members, one of which resulted in a law enforcement investigation and subsequent arrests.

In January 2024, Brazilian law enforcement investigated former Brazilian President Jair Bolsonaro's allies for allegedly conducting extrajudicial electronic surveillance on Bolsonaro's political opponents. The surveillance allegedly gathered information on at least 30,000 Brazilians — including two Federal Supreme Court (STF) justices and a key ally of current President Luiz Inácio Lula da Silva — as part of a scheme to systematically sow distrust in the electoral system.[28]

In December 2024, Brazilian Federal Police made their initial arrests stemming from this investigation and detained a former member of Bolsonaro's cabinet for alleged obstruction of the collection of evidence. Separately, in September 2024, Colombian President Gustavo Petro requested the attorney general's office investigate the Colombian Police Intelligence Directorate (DIPOL) for allegedly purchasing the NSO Group's *Pegasus* spyware in 2021, during former President Iván Duque's administration. In a televised broadcast, Petro speculated that he or other Colombian politicians, activists, and civilians had been targeted by the spyware.[29]

---

23 https://www.reuters.com/technology/brazil-paves-way-semiconductor-cooperation-with-china-2023-04-14/

24 https://www.cfr.org/backgrounder/china-influence-latin-america-argentina-brazil-venezuela-security-energy-bri

25 https://freedomhouse.org/country/brazil/freedom-net/2024

26 https://www.eeas.europa.eu/eeas/exploring-potential-artificial-intelligence-latin-america-caribbean_en

27 https://www.bnamericas.com/en/news/latin-american-countries-adopt-sweeping-ai-declaration

28 https://g1.globo.com/politica/blog/andreia-sadi/post/2024/01/25/espionagem-ilegal-da-abin-atingiu-30-mil-pessoas-e-dados-foram-guardados-dados-em-israel-diz-chefe-da-pf.ghtml
https://apnews.com/article/brazil-bolsonaro-coup-plot-braga-netto-eaa04eb1ded433addc1eee2167f8b8e0

29 https://elpais.com/america-colombia/2024-09-05/petro-revela-un-documento-que-vincula-a-la-inteligencia-policial-de-la-era-duque-con-la-compra-del-software-espia-pegasus.html

OUTLIERS

In 2024, the Venezuelan government's cybersecurity posture was anomalous to the region's momentum in bolstering its domestic cybersecurity practices, instead focusing on quashing dissent, spreading misinformation, criminalizing free speech, and weaponizing legislation to remain in power. For example, in August 2024, the Venezuelan government invoked unsubstantiated "cyberattacks" when providing an explanation for a delay in presidential electoral results. International organizations, such as the United Nations, rebuffed these claims, stating their investigations did not uncover any evidence to suggest Venezuela's electoral system was the victim of a cyberattack.[30] These efforts suggest the government is likely weaponizing cybersecurity incidents for political gain.

Over the past 12 months, Venezuelan President Nicolás Maduro's administration also censored online content. For example, ahead of the July 2024 presidential election, Maduro allegedly ordered ISPs to block access to at least 50 independent local media and nonprofit websites.[31]

In April 2024, the Venezuelan government considered legislation that could muzzle social media platforms, including a law criminalizing "prohibited messages" — likely referring to content critical of the government — and imposing harsh penalties; the Venezuelan legislature postponed the debate on the draft law in August 2024.[32]

Additionally, in November 2024, the Guyana government accused the Venezuelan government of orchestrating an offensive cyber operation that included ransomware attacks and phishing against Guyanese targets to undermine Guyana's sovereignty over the Essequibo region, an oil-rich area that Guyana and Venezuela have both claimed in a long-standing territorial dispute.

According to local press reporting, the Guyanese government identified organizations and individual operations comprising Venezuela's cyber program, including names and photographs.[33] CrowdStrike Intelligence cannot presently corroborate these claims; however, if the claims are true, this campaign would demonstrate unique insight into Venezuela's use of offensive cyber capabilities outside its own borders.

30 https://www.voanews.com/a/no-evidence-venezuela-vote-hacked-carter-center-election-monitor-says/7734334.html
https://www.washingtonpost.com/world/2024/08/13/venezuela-election-results-un-report/

31 https://freedomhouse.org/country/venezuela/freedom-net/2024

32 https://freedomhouse.org/country/venezuela/freedom-net/2024

33 https://dpi.gov.gy/national-defence-institute-hosts-groundbreaking-ceo-cybersecurity-workshop-in-guyana/

The Caribbean

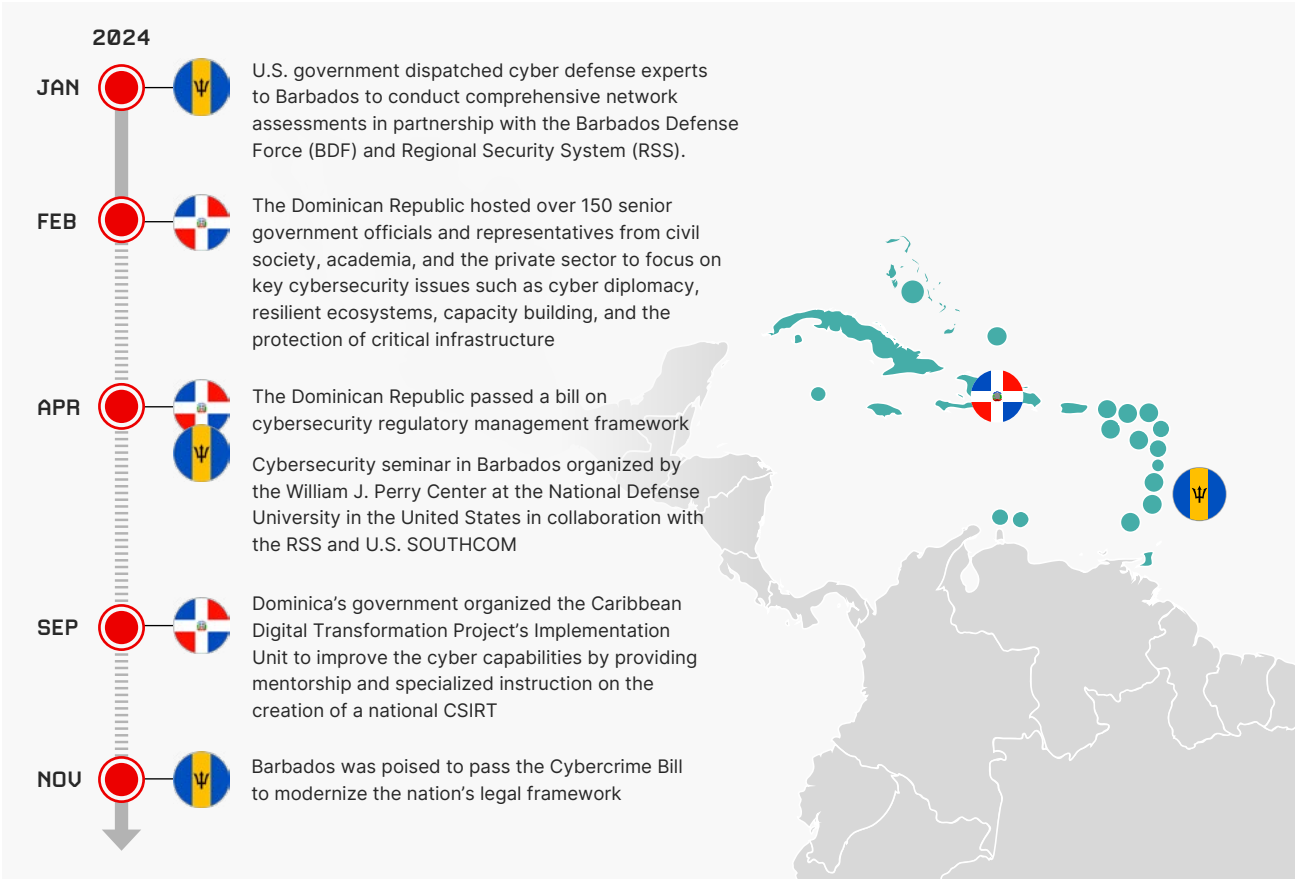

Figure 4. Cyber trends in the Caribbean

MACRO TRENDS

Throughout 2024, CrowdStrike Intelligence did not observe Caribbean governments passing numerous cyber laws. However, the Dominican Republic and Barbados drafted bills focused on cybersecurity regulatory management frameworks (Figure 4).[34] The Dominican Republic bill on cybersecurity management was passed by the Senate in April 2024, and the Barbados cybersecurity bill is awaiting a Senate vote.[35]

Numerous Caribbean governments either organized or attended bilateral or multilateral meetings focused on routine cybersecurity information sharing and capacity building; however, in late January 2024 and early February 2024, the Barbados government conducted outreach to the U.S. requesting network assessment assistance following a series of cyberattacks targeting public and private entities.[36]

Separately, in February 2024, the Dominican Republic hosted senior officials from South America, the Caribbean, and the EU to discuss cyber diplomacy and protection of critical infrastructure. Additionally, in September 2024, Dominica's government organized the Caribbean Digital Transformation Project's Implementation Unit, whose goal was to create a national CSIRT.[37]

---

34 https://dominicantoday.com/dr/local/2024/04/10/senate-approves-cybersecurity-bill-and-other-legislative-measures/ https://www.thestkittsnevisobserver.com/bad-news-for-cybercriminals-as-barbados-bill-almost-ready-for-vote/

35 https://www.barbadosparliament.com/bills/details/741

36 https://dialogo-americas.com/articles/us-and-barbados-collaborate-on-cybersecurity/

37 https://dominicanewsonline.com/news/homepage/news/caribbean-digital-transformation-project-provides-training-to-boost- national-cyber-security/

MICRO TRENDS

Caribbean governments seemingly began developing AI policies and frameworks, likely to develop a structured approach to incorporating AI into digital government strategies.

For example, in September 2024, the Economic Commission for Latin America and the Caribbean (ECLAC) discussed a study on AI readiness and digital government strategies for Caribbean countries, specifically focused on Small Island Developing States (SIDS).[38] In September 2024, Jamaica's AI Task Force — established in 2023 to provide an "evidence-based foundation for the development of a National AI Policy" — presented its findings to the Jamaican Prime Minister's office on how to incorporate AI into Jamaica's education, business, and government sectors.[39] In November 2024, Grenada's parliament announced it would introduce AI tools in 2025 for use by legislators, but it has not provided further information.[40]

There was limited publicly available information on Chinese technological inroads in the Caribbean region. As of January 2025, only two Caribbean countries — the Dominican Republic and Trinidad and Tobago — used or planned to use Huawei equipment in their 5G networks.[41]

There was limited publicly available information on Caribbean governments using commercial spyware for political gain or domestic surveillance.

OUTLIERS

Similar to Venezuela, Cuba was a 2024 outlier, as it did not bolster its domestic cybersecurity policy and posture, instead enacting policies subjugating its domestic population, including restricting internet service during public protests, allegedly planning to conduct information operations (IO) targeting the U.S. presidential election, and updating its electronic surveillance facilities.

In February 2024, the Cuban government repealed a planned five-fold increase in fuel prices due to an unspecified "cyberattack"; the Cuban Economy Vice Minister made an unsubstantiated claim blaming the increase on a "virus from abroad."[42] In March 2024, a nonprofit human rights organization identified at least one internet disruption in Santiago de Cuba following a public protest, which the organization judged may have been government-directed.[43] In June 2024, the U.S. intelligence community reportedly assessed that the Cuban government would likely conduct IO during the 2024 U.S. elections to influence voters' perceptions of candidates that the Cuban government views as hostile to Cuba.[44]

Cuba also sought to enhance its existing cooperation with the Chinese government. In July 2024, the Center for Strategic and International Studies (CSIS), a think tank based in Washington, D.C., released a report detailing four updated, active sites in Cuba conducting electronic surveillance operations likely linked to the Chinese government.

These sites are reportedly among the most likely locations in Cuba to support China's efforts to conduct signals intelligence (SIGINT) on the U.S. The report shows three surveillance sites around Havana and one in southeast Cuba approximately 70 miles from the U.S. naval base at Guantanamo Bay.[45]

---

38 https://www.cepal.org/en/events/virtual-expert-group-meeting-harnessing-artificial-intelligence-ai-and-digital-government
https://caribbean.eclac.org/information-resources/website/selected-publications-harnessing-ai-caribbean

39 https://jis.gov.jm/cabinet-to-receive-artificial-intelligence-task-force-report/

40 https://www.jamaicaobserver.com/2024/11/27/grenada-parliament-introduce-use-ai-2025/

41 https://www.cfr.org/backgrounder/china-influence-latin-america-argentina-brazil-venezuela-security-energy-bri

42 https://www.reuters.com/world/americas/cuba-delays-feb-1-fuel-price-hike-cites-cyberattack-2024-01-31/

43 https://freedomhouse.org/country/cuba/freedom-net/2024

44 https://www.miamiherald.com/news/nation-world/world/americas/cuba/article289243045.html
https://www.dni.gov/files/ODNI/documents/assessments/NIC-Declassified-ICA-Foreign-Threats-to-the-2022-US-Elections-Dec2023.pdf

45 https://features.csis.org/hiddenreach/china-cuba-spy-sigint/

eCrime Overview

The LATAM region faces several eCrime threats from regional and global eCrime adversaries. To date, CrowdStrike Intelligence has named six adversaries either based in or predominantly targeting LATAM: OCULAR SPIDER, BLIND SPIDER, ODYSSEY SPIDER, PLUMP SPIDER, SAMBA SPIDER, and SQUAB SPIDER. Though these adversaries almost exclusively target LATAM, big game hunting (BGH) adversaries and global eCrime adversaries are also increasingly targeting the region (Figure 5).

Additional adversaries like ROBOT SPIDER and OCULAR SPIDER played key roles in LATAM's cybercrime ecosystem in 2024 — ROBOT SPIDER through a dedicated crypter service website and OCULAR SPIDER as the operator behind the prominent *RansomHub* ransomware as a service (RaaS) offering.

Throughout 2024, CrowdStrike Intelligence observed Nigeria-based AVIATOR SPIDER, Russia-based RENAISSANCE SPIDER, and SOLAR SPIDER target entities in the LATAM region for the first time. While AVIATOR SPIDER and SOLAR SPIDER continued to exhibit their traditional aviation sector and financial sector target scopes, respectively, these adversaries have historically targeted other geographic regions.

Similarly, RENAISSANCE SPIDER primarily targets Eastern Europe-based entities. However, in separate January 2024 campaigns, the adversary targeted entities in the Colombian agriculture sector and Peruvian legal sector.

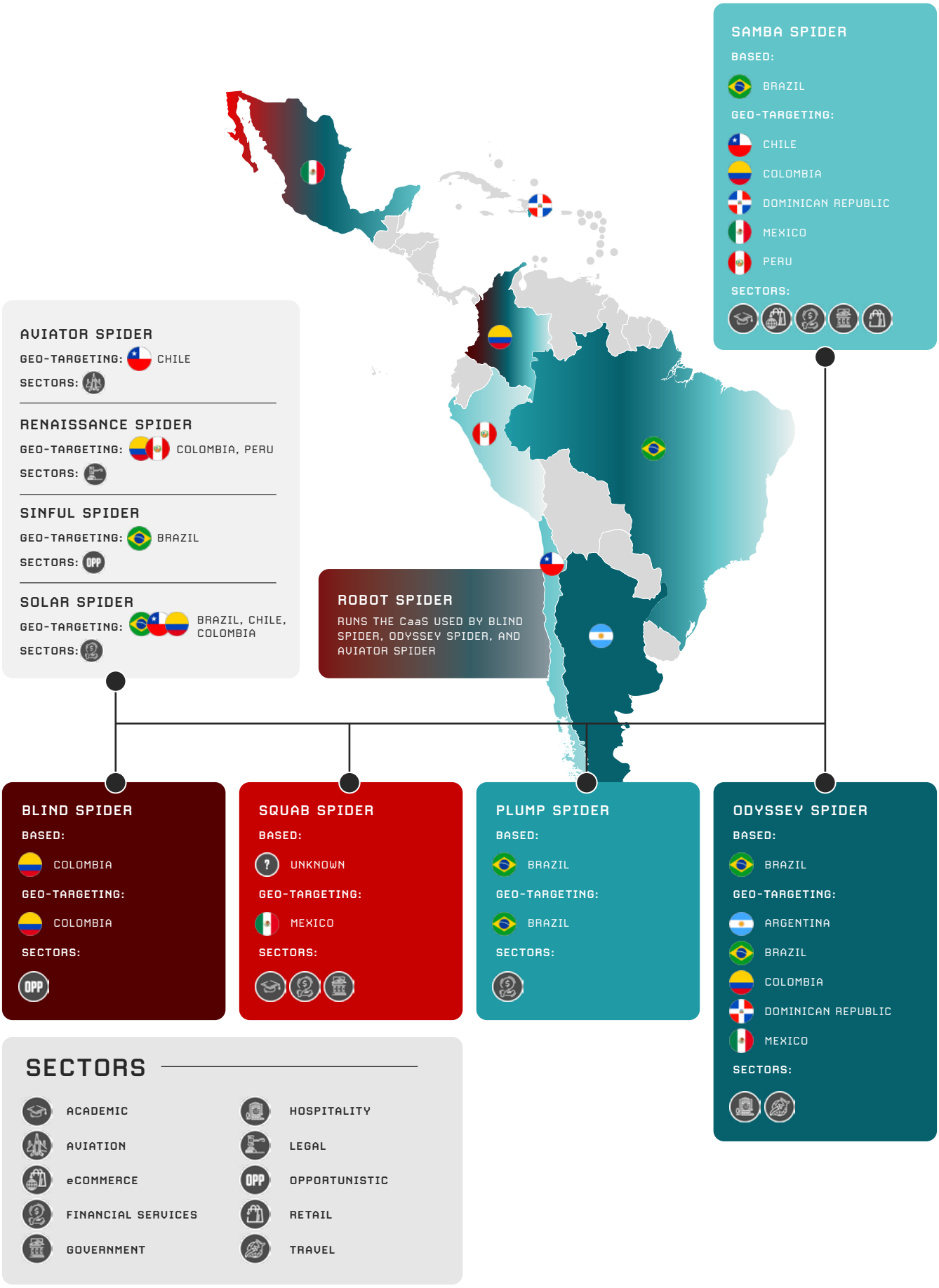

Figure 5. eCrime adversaries based in or targeting the LATAM region

LATAM-Based Adversaries

BLIND SPIDER

eCrime adversary BLIND SPIDER (aka *APT-C-36* and *Blind Eagle*) has actively targeted the Colombian public and private sectors since April 2018; however, the adversary has also intermittently targeted Chile and Ecuador. BLIND SPIDER conducts high-volume opportunistic malspam campaigns using financial- and legal-themed phishing content impersonating Colombian government authorities. BLIND SPIDER delivers PDF lure documents that contain malicious links leading to the download of password-protected archive files hosted on legitimate file-hosting services.

BLIND SPIDER has consistently used ROBOT SPIDER's *Fsociety* (or *CryptersAndTools*) crypter and other commodity crypters to protect and deliver commodity remote access tool (RAT) payloads (e.g., *AsyncRAT*, *njRAT Lime*, and *Remcos*). The adversary likely attempts to steal sensitive information relating to financial and email services.

From mid-2024 to January 2025, BLIND SPIDER continued targeting Colombia-based entities. While BLIND SPIDER maintained their overall financial- and legal-themed phishing content, the adversary regularly altered delivery methods, including using PDF lure documents, malicious links, and most recently Scalable Vector Graphics (SVG) files.

BLIND SPIDER continued using ROBOT SPIDER's crypters — which leverage steganography — as a BLIND SPIDER moniker was present in an October 2024 leaked ROBOT SPIDER customer list. BLIND SPIDER also employed *HijackLoader* and *Roda Crypter* to deliver their commodity RAT payloads.

ODYSSEY SPIDER

ODYSSEY SPIDER (aka *TA558*) is a Brazil-based eCrime adversary active since late 2018. The adversary has consistently targeted the hospitality and travel sectors, mainly in the LATAM region and less frequently in North America and Southwestern Europe. While ODYSSEY SPIDER regularly varies their TTPs, they typically use hotel reservation-themed phishing to deliver commodity RATs and the *CapturaTela* screencapturing tool. ODYSSEY SPIDER uses custom script downloaders, the *Alosh* multi-stage loader, and ROBOT SPIDER's crypter to protect their payloads.

ODYSSEY SPIDER likely monetizes their intrusions by stealing credit card information from hotels; this assessment is based on the adversary's *CapturaTela* screencapturing tool that takes and exfiltrates screenshots during an online booking process. CrowdStrike Intelligence also identified a PHP panel — designed to validate Brazilian credit card information — hosted on ODYSSEY SPIDER infrastructure.

In 2024, CrowdStrike Intelligence observed ODYSSEY SPIDER primarily targeting the hospitality and travel sectors in Argentina, Brazil, Colombia, and Mexico. The adversary leveraged hospitality-themed malicious infrastructure, including compromised domains belonging to LATAM-based hotels. Similarly, ODYSSEY SPIDER tailored their downloaders for hospitality sector targets by opening legitimate hotel reservation websites and displaying reservation-related decoy files. ODYSSEY SPIDER also targeted the U.S., leveraging the country's tax season in early 2024 and early 2025.

PLUMP SPIDER

Brazil-based eCrime adversary PLUMP SPIDER has targeted Brazil-based companies offering financial services since November 2023. The adversary impersonates IT support personnel during voice phishing (vishing) calls to entice targets to download remote monitoring and management (RMM) tools and SoftEther VPN. PLUMP SPIDER typically deploys custom Lightweight Directory Access Protocol (LDAP) reconnaissance tools to obtain user credentials and has used a custom tool to obtain user account balances for a payment platform. The adversary likely monetizes their intrusions by conducting fraudulent payments.

From January 2024 to January 2025, PLUMP SPIDER created and used several domains imitating IT support services, hosting their purported administrator tools Ammyy Admin, DWAgent, HopToDesk, RustDesk, Supremo, TeamViewer, and SoftEther VPN. While the adversary mainly used these domains to deceive victims in their vishing calls, they also used the domain `suporte[.]re` in a likely phishing campaign using a PDF lure document that was nearly identical to one used in a June 2023 ODYSSEY SPIDER campaign. The domain hosted a crypter sharing considerable overlaps with ROBOT SPIDER's *CryptersAndTools* (aka *Fsociety*) tooling.

SAMBA SPIDER

SAMBA SPIDER is a Brazil-based eCrime adversary that operates the *Mispadu* banking trojan, which first appeared in 2019. The adversary targets financial institutions and eCommerce entities in Spanish- and Portuguese-speaking countries, aiming to capture personally identifiable information (PII). In 2024, SAMBA SPIDER maintained a consistent operational tempo, leveraging regular updates to the infection chain used to distribute *Mispadu*. SAMBA SPIDER currently targets Spanish- and Portuguese-speaking entities in the Dominican Republic, Mexico, Chile, Colombia, Peru, Italy, Portugal, and Spain.

Throughout 2024, SAMBA SPIDER spread email spam campaigns using an updated infection chain, which includes updated and new scripting components. The campaigns delivered a first-stage payload with the filename prefix `*Factura*_`.

SQUAB SPIDER

SQUAB SPIDER (aka *FIN13*) is an eCrime adversary that has primarily targeted Mexico-based financial institutions. According to industry research, the adversary has been active since at least 2016.[46] SQUAB SPIDER uses a wide range of webshells to exploit vulnerable web servers to gain initial access and relies on *BLUEAGAVE* bind shells or simple listeners for lateral movement. Though SQUAB SPIDER's monetization methods are not confirmed, the adversary's narrow targeting of specific databases or log files is more consistent with targeted eCrime behavior than opportunistic data theft and extortion.

In May 2024 and August 2024, CrowdStrike Intelligence identified three SQUAB SPIDER intrusions at two Mexican government entities and a Mexico-based academic institution. The intrusions marked a departure from the adversary's historical targeting of financial institutions. Despite the adversary's expanded targeting scope, they maintained consistent TTPs, including compromising vulnerable web servers for initial access, deploying listeners — low-prevalence JSP webshells — and conducting their typical reconnaissance commands. The adversary was last observed in late January 2024 targeting a telecom company.

Big Game Hunting

In 2024, CrowdStrike Intelligence documented a total of 291 LATAM-based victims named on data extortion and ransomware leak sites.[47] Though this number only represents roughly 5% of the 5,276 globally documented incidents, it marks a 15% increase over the 254 documented incidents in the region in 2023. No evidence suggests that BGH adversaries target the LATAM region to the same extent as North America and Europe.

The most affected country in 2024 was Brazil with a total of 119 victims, followed by Mexico and Argentina with 45 and 29 victims, respectively (Figure 6). Peru, Colombia, and Chile each also represented over 10 victims on dedicated leak sites (DLSs).

The most targeted sectors were technology, financial services, consulting and professional services, retail, and healthcare.

46 https://cloud.google.com/blog/topics/threat-intelligence/fin13-cybercriminal-mexico

47 This number only represents the victims that did not pay a ransom.

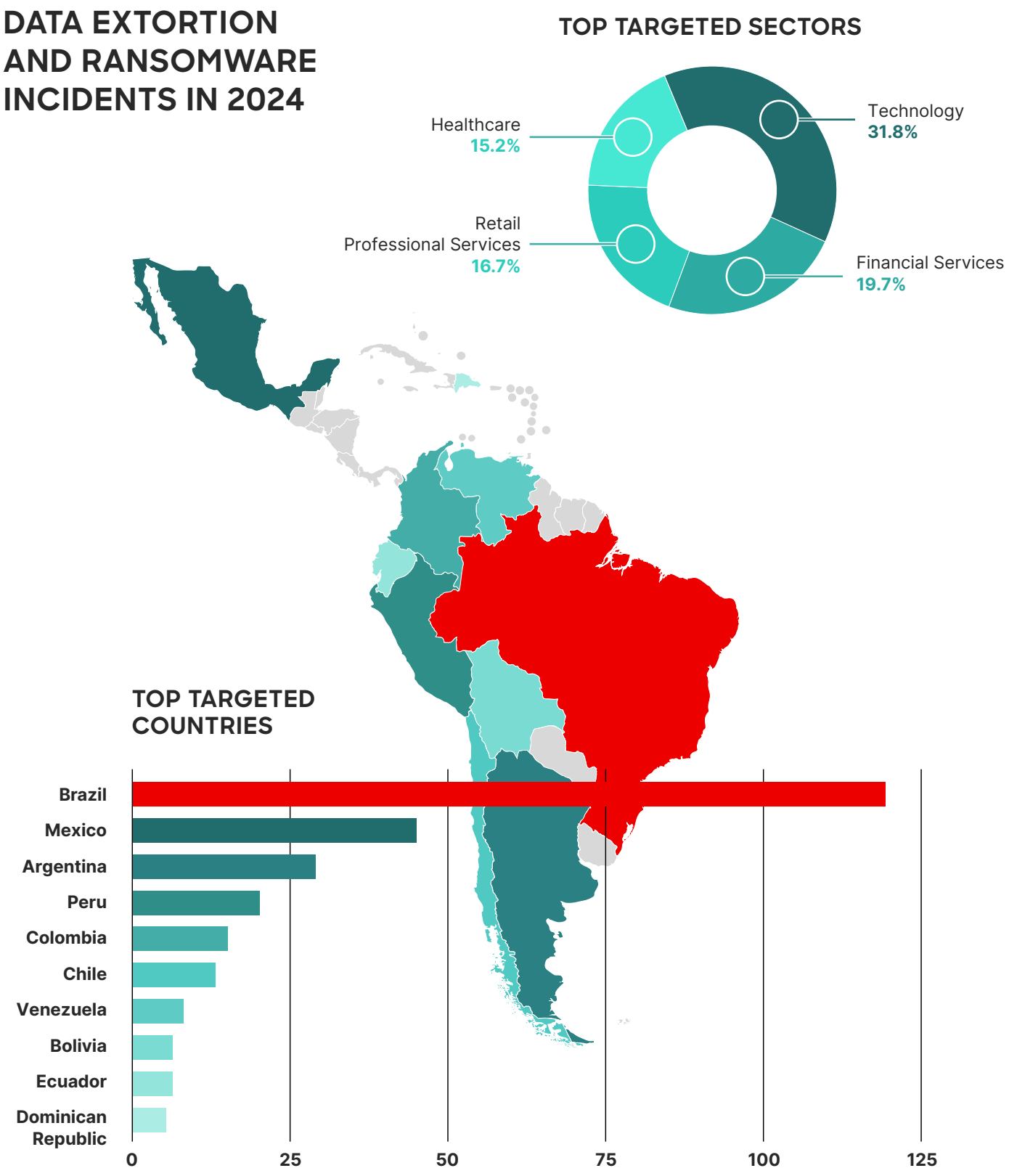

Figure 6. Data extortion and ransomware incidents by country and sector

OCULAR SPIDER's *RansomHub* RaaS and BITWISE SPIDER's *LockBit* RaaS were the dominant LATAM ransomwarethreats in 2024. Further ransomware threats included PUNK SPIDER's *Akira*, BRAIN SPIDER-associated *Dispossessor* and *EightBase*, FROZEN SPIDER's *Medusa*, and VICE SPIDER's *Rhysida*.

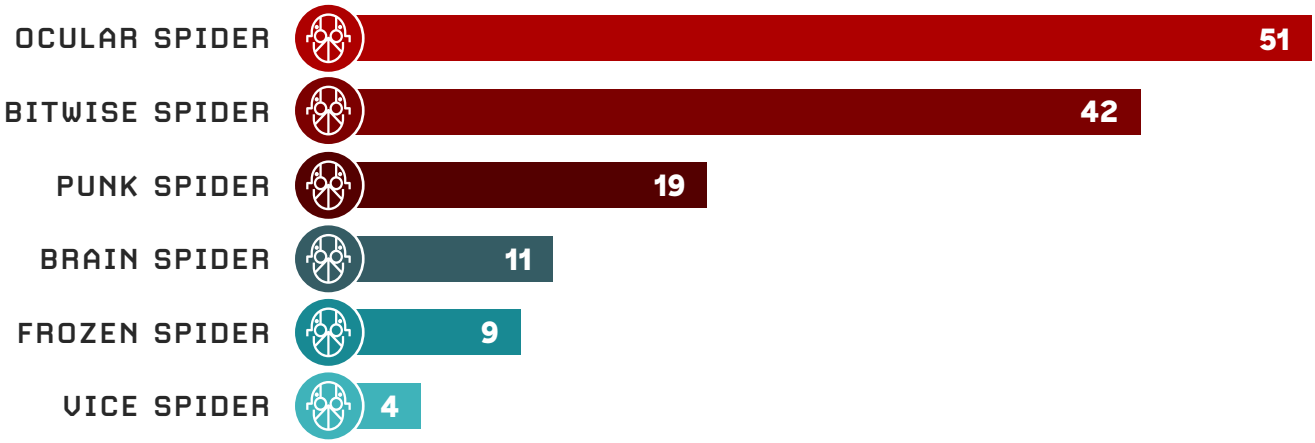

Figure 7. Dominant ransomware threats in 2024 and incident count

Though these BGH adversaries likely do not specifically target the LATAM region, they nonetheless present a major threat due to their high impact, as demonstrated by WIZARD SPIDER's April 2022 *Conti* ransomware attack against the Costa Rican government. The incident resulted in the suspension of several Costa Rican government and financial platforms and led to the declaration of a national state of emergency.

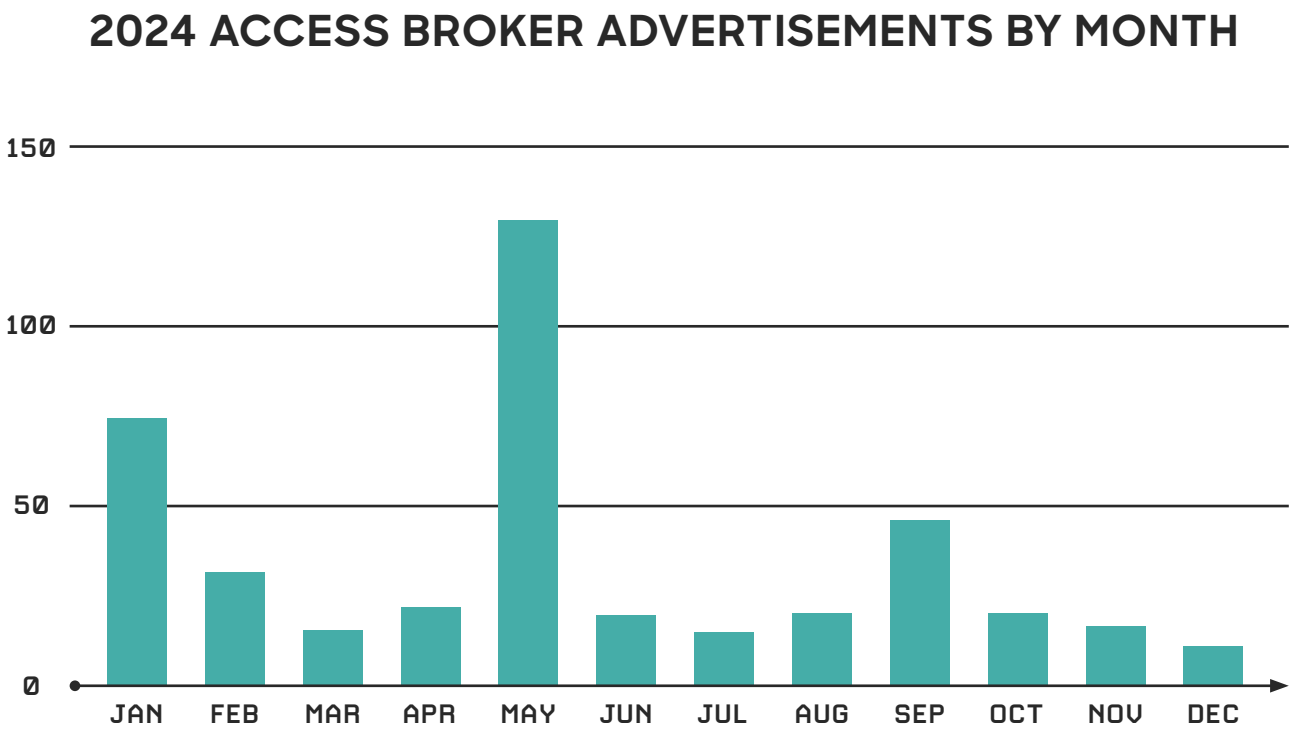

Figure 8. Access broker advertisements by month

Underground Ecosystem

LATAM-based eCrime threat actors benefit from an expansive underground ecosystem providing network access, leaked credentials, and various commodity malware or crypters. While these threat actors typically rely on English- and Russian-language eCrime forums used by global eCrime actors, CrowdStrike Intelligence identified several Telegram channels and forums catering to Spanish-speaking users.

LATAM eCrime adversaries have also operated their own forums and websites. In July 2024, a threat actor that advertises LATAM-based websites' vulnerabilities announced the creation of a new forum for English and Spanish speakers. In September 2024, Brazil-based ROBOT SPIDER launched a dedicated website to advertise their crypter service alongside their Telegram channel.

In September 2024, the international law enforcement operation Operation Kaerb took down the iServer website that targeted Spanish-speaking users in Argentina, Chile, Colombia, Ecuador, Peru, and Spain. The iServer service enabled eCrime actors to harvest user credentials to unlock stolen phones and bypass Lost Mode.

ACCESS BROKERS

BGH adversaries often collaborate with access brokers, who gain and sell access to target networks; understanding access brokers' TTPs can assist in mitigating the ransomware threat.

In 2024, 107 access brokers advertised network access to 428 LATAM-based entities (Figure 8). These entities were predominantly located in Brazil, Mexico, Colombia, Argentina, and Peru — the five most ransomware-affected LATAM countries.

The number of access broker advertisements marks a notable increase from 2023, when 93 access brokers advertised network access to 311 LATAM-based entities. This advertisement increase was also accompanied by a reduction in average network access price, from $3,385 USD in 2023 to $1,355 USD in 2024.

With 146 advertisements, one access broker — active on an English- and Russian-language eCrime forum — accounted for nearly 35% of the 2024 total and nearly 87% of advertisements in May 2024, an outlier month together with January 2024 (Figure 8). However, with 1,177 network access advertisements globally, the access broker is likely not specifically targeting the LATAM region, instead acquiring their access from high-volume information stealer campaigns, from leaked credentials, or by exploiting unpatched vulnerabilities.

Qualitor Zero-Day Vulnerability Affects Brazilian Entities

In September 2024, a threat actor opportunistically targeted a Brazil-based technology company to exploit CVE-2024-44849, which affects Qualitor 8.24, a Brazilian IT service management (ITSM) solution. The threat actor likely used a publicly available exploit released prior to the exploitation date.

Though CrowdStrike Intelligence did not observe other 2024 region-specific vulnerability exploitation, systems with internet-facing components remain susceptible to opportunistic exploitation via common exploits, brute-force attacks, and misconfigured systems.

LEAKED CREDENTIALS

Throughout 2024, CrowdStrike Intelligence recovered more than 1 billion credentials belonging to LATAM-based individuals and organizations related to data leaks and malware stealer logs. Figure 9 displays statistics on the stolen credentials across various LATAM countries, highlighting the scale of criminal operations in the region. The graph contains the total number of credentials leaked for each country and the proportion of credentials related to government institutions, which includes public services for citizens.

Brazil had the highest number of leaked credentials in 2024, likely reflecting its large population, increasing online activity, and rapid digitalization. Mexico, Argentina, Colombia, and Peru also had a high number of leaked credentials, indicating their growing digital economy and cyber threat exposure.
The stolen credentials can lead to financial fraud, identity theft, and further breaches, all of which can impact individuals and organizations.

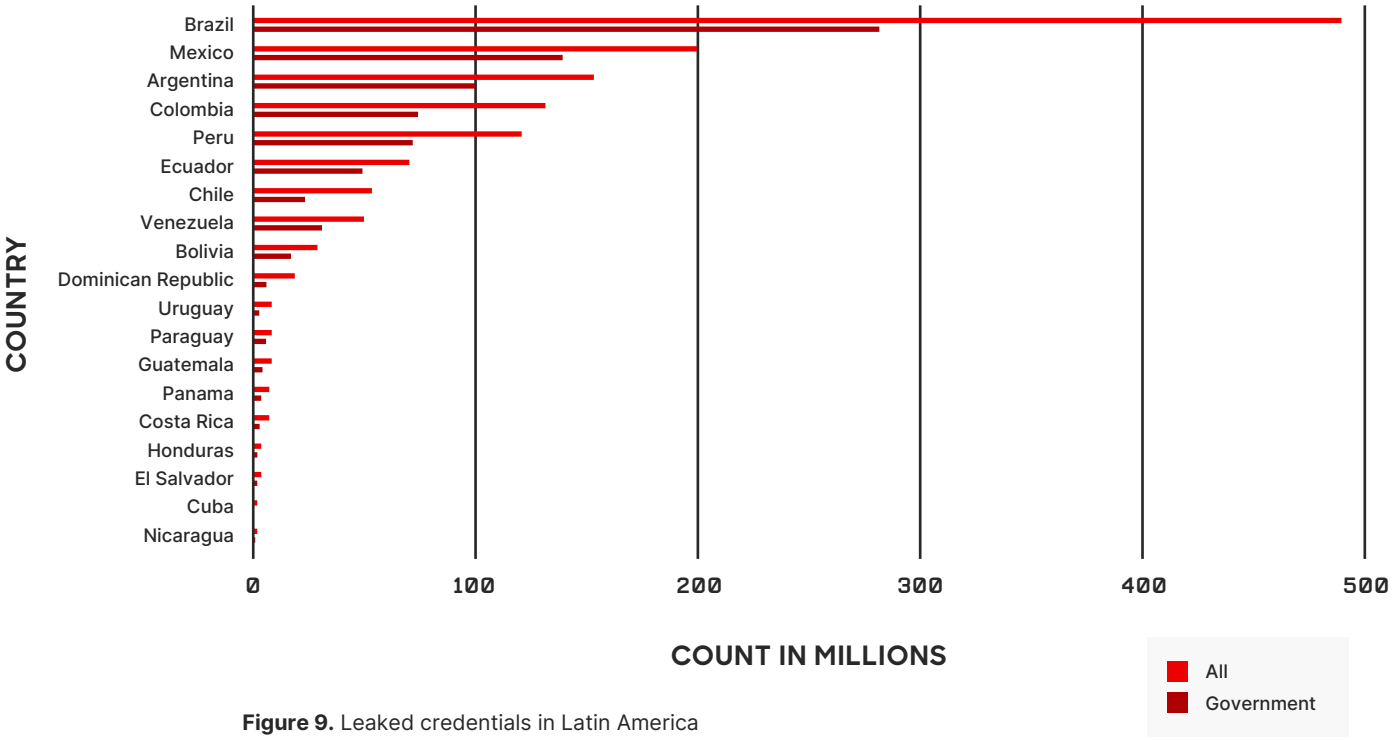

Figure 9. Leaked credentials in Latin America

ROBOT SPIDER CRYPTER AS A SERVICE

eCrime adversary ROBOT SPIDER uses their *CryptersAndTools* (*Fsociety*) CaaS to enable LATAM eCrime adversaries. Since 2017, *CryptersAndTools* has offered a multi-stage crypter, and CrowdStrike Intelligence has observed LATAM-based eCrime adversaries (BLIND SPIDER, ODYSSEY SPIDER, and PLUMP SPIDER) and the Nigeria-based AVIATOR SPIDER using this crypter.

ROBOT SPIDER has historically advertised *CryptersAndTools' Protector Crypter* via a Telegram channel; however, in September 2024, the adversary began using a website to advertise to a likely larger customer base. The adversary's English-language website offers semi-professional services that include 24-hour support and regular updates to accommodate multiple time zones (Figure 10).

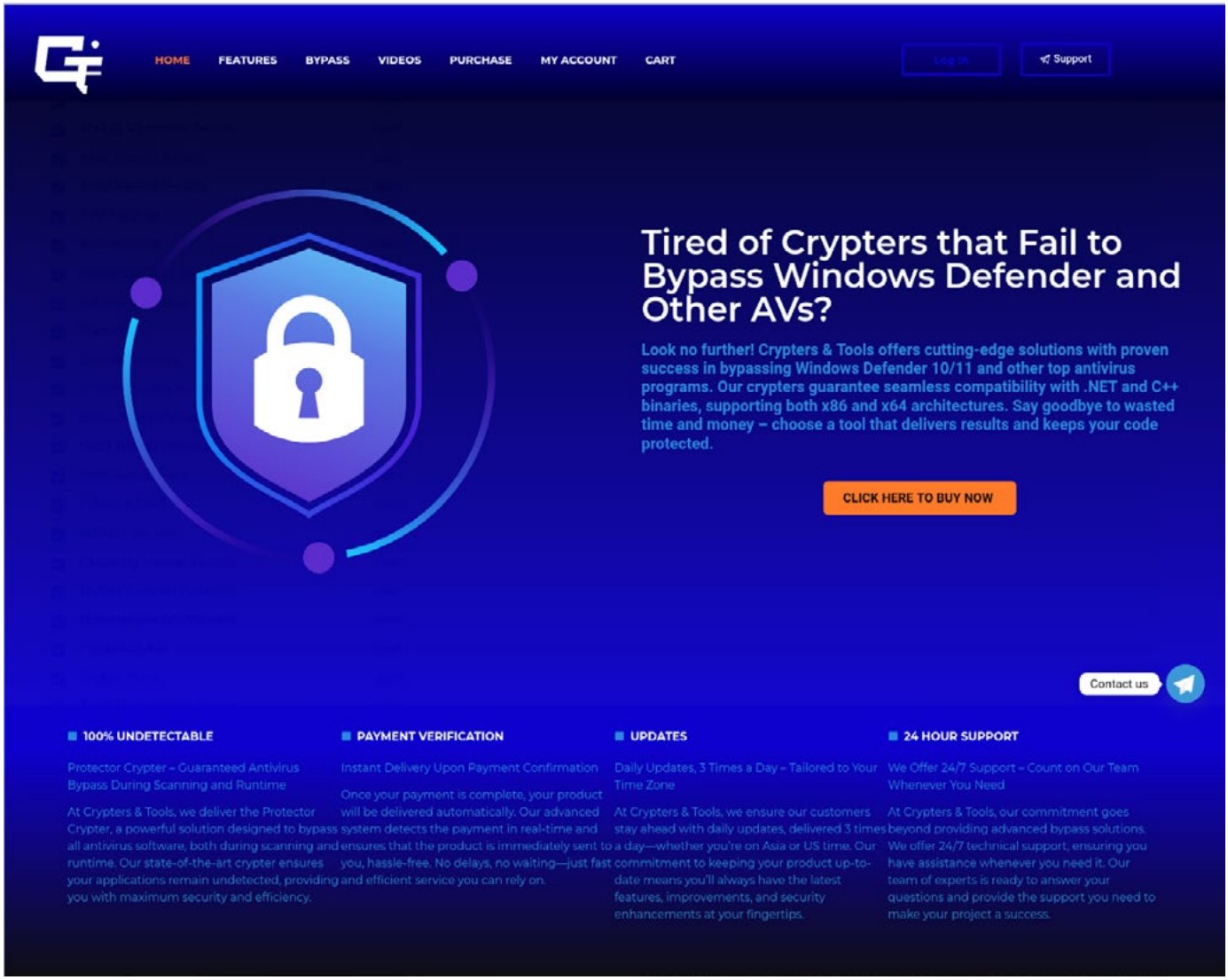

Figure 10. ROBOT SPIDER's *CryptersAndTools* website

In mid-2024, ROBOT SPIDER also began selling their crypter's source code for $6,000 USD. In December 2023, the adversary offered a crypter creation course likely providing customers with knowledge to build tools akin to their multi-stage crypter; this course has made incident attribution difficult. For instance, in September 2024, CrowdStrike Intelligence identified a *Makop* ransomware incident and a RENAISSANCE SPIDER campaign leveraging crypters likely based on ROBOT SPIDER's crypter.

ROBOT SPIDER's PowerShell script loader has consistently used the variable name `$codigo` and the same function call `$oWjuxd`; the use of the same name aids in attribution. This PowerShell script decodes a next-stage PowerShell script that downloads a ROBOT SPIDER .NET loader (aka *AndeLoader*) embedded within a JPG image between the markers `<<BASE64_START>>` and `<<BASE64_END>>`.

The PowerShell script invokes the export function `UAI` to execute the .NET loader. The adversary has consistently used the same JPG, often with variations of the name `deathnote.jpg`.

Dominant Malware Families

Throughout 2024, CrowdStrike Intelligence observed updates to well-known LATAM eCrime malware leveraging novel techniques focused on improving defense evasion, which were detailed in this 2024 CrowdStrike blog post.[48] Notably, LATAM-based malware family developers began adopting the Rust programming language leveraged exclusively in downloader components.

This adoption highlights the developers' interest in adapting to the current eCrime ecosystem by using new programming languages for malware development in an attempt to hinder analysis and evade host-based detections. CrowdStrike Intelligence observed the following updates:

- ***Mispadu* (aka *URSA*):** During April 2024 and June 2024, SAMBA SPIDER conducted campaigns leveraging new infection chains, which included new or updated components, to deliver *Mispadu*. *Mispadu* version 100 is the latest malware build observed during 2024.
- ***Kiron* (aka *Grandoreiro*):** In January 2024, law enforcement's Operation Grandoreiro resulted in infrastructure seizure and the arrest of Brazil-based individuals. Despite the seizure, the malware continued to leverage several updates in which developers tested new delivery methods, added a browser extension, and adopted Rust for a short period.
- ***Caiman* (aka *Grandoreiro*):** In June 2024, the developers updated the string obfuscation after a month-long *Caiman* hiatus that began in mid-May 2024.
- ***Astaroth* (aka *Guildma*):** During 2024, *Astaroth* developers did not release any significant updates, only adding a key derivation to decrypt strings and making minor adjustments in obfuscation and network protocol.
- ***Culebra* (aka *Mekotio*):** In late July 2024, *Culebra* developers updated the malware's downloader component — delivered as a PowerShell component — maintaining several techniques from the Delphi version used throughout 2023 and the first half of 2024.
- ***Salve* (aka *Casbaneiro*):** In mid-March 2024, *Salve* developers updated the infection chain to include a Rust-based downloader; this activity occurred after a likely hiatus that began in November 2023.

During 2024, other threat actors leveraged malware campaigns via phishing websites impersonating Mexico-based entities. Though the campaigns appear to be similar, different threat actors highly likely operated the activities leveraging *Doit* (aka *TimbreStealer*), *BotnetFenix*, and *Belero*. The use of similar TTPs highlights the knowledge sharing between LATAM-focused threat actors.

Threat actors primarily use *Doit* — an information stealer first observed in 2022 — to target Mexico. The malware developers updated *Doit* three times, leveraging a first AutoIt version, a C++ rewrite, and a final C++ modular version, which is the latest build in distribution (Figure 11).

48 Also see https://www.crowdstrike.com/en-us/blog/latin-america-malware-update/

Figure 11. Phishing websites for *Doit* distribution

BotnetFenix is a multi-stage LATAM stealer first identified in January 2023. The malware comprises a PowerShell downloader and the Rust-based loader *RustSimpleLoader*. In 2024, a threat actor distributed *BotnetFenix* using smishing and phishing websites, including fake CAPTCHA sites (Figure 12).

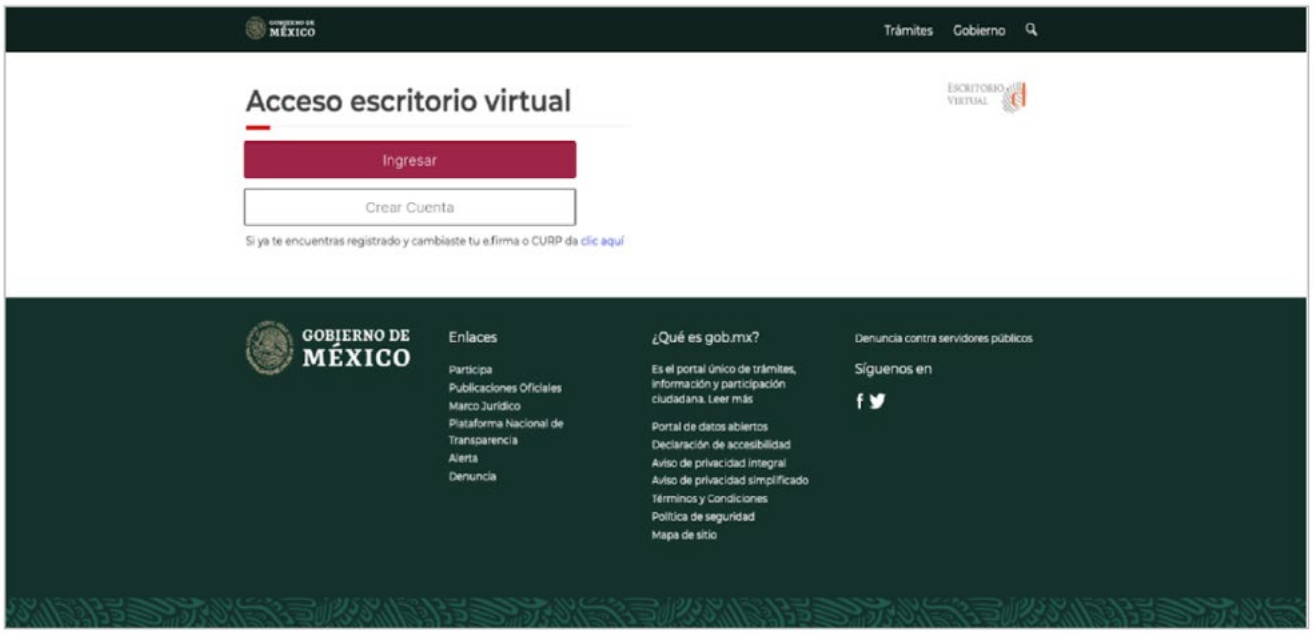

Figure 12. Phishing websites for *BotnetFenix* distribution

In mid-2023, a criminal actor opportunistically distributed an unidentified Visual Basic (VB)-based LATAM banking trojan — dubbed *Belero* — via phishing websites (Figure 13).

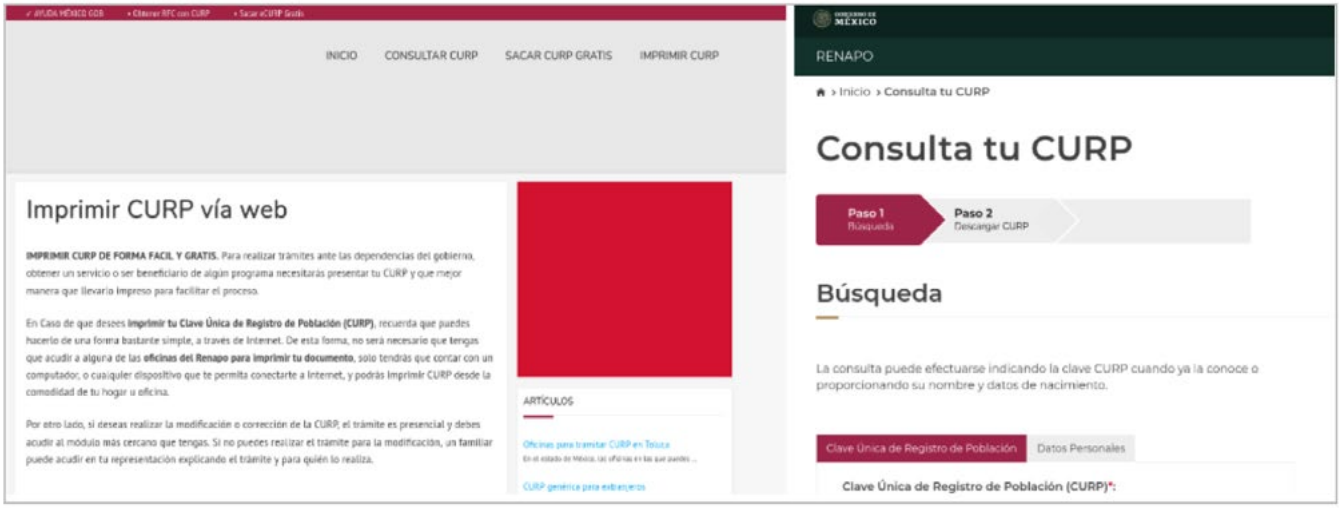

Figure 13. Phishing websites for *Belero* distribution

CrowdStrike Intelligence has observed other low-prevalence criminal operations in the region:

- In July 2024, a threat actor leveraged *HijackLoader* payloads containing *Remcos* using Spanish-language lures, which impersonated an inauthentic CrowdStrike fix.
- *EvolvedThief* (aka *Chaes* or *SolarSys*) is a modular LATAM banking trojan that was initially implemented in several programming and scripting languages. In late December 2023, the malware developers released a rewritten Python version targeting Portuguese-speaking users.
- *QuasarRAT* (aka *BlotchyQuasar*) is a *Quasar* variant with banking trojan capabilities. In May 2024, a threat actor leveraged an email spam campaign targeting Colombia-based users to spread the malware. This threat actor has conducted Colombia-focused campaigns since at least 2020. Though the activity TTPs are similar to BLIND SPIDER, the command-and-control (C2) infrastructure and the use of a *Quasar* variant indicate another threat actor likely conducted this activity.

Loan Shark Mobile Applications Distribute *SpyLoan* Malware

In November 2024, CrowdStrike Intelligence observed *SpyLoan* malware samples from predatory lending applications that purportedly originated in Mexico and were available via legitimate stores, including the Google Play store. In addition to their low transparency and high interest rates, these applications leverage spyware features to steal users' personal data, which are then leveraged to coerce users into repayment, often through harassment or threats of violence. According to Mexican press reporting, unregulated loan shark applications are popular in Mexico despite Mexican authorities' attempts to curb their prevalence.

State-Nexus Overview

In 2024, CrowdStrike Intelligence observed several China-, Colombia-, DPRK-, and Russia-nexus adversaries target the LATAM region (Figure 14). However, state-nexus adversaries represented a fraction of documented activity, likely due to their intelligence collection aims, related target prioritization, and generally greater focus on stealth. Thus, while these adversaries typically exhibit greater sophistication than their eCrime counterparts, the threat they pose depends on an entity's sector, their geographic location, and external events, such as elections.

China- and DPRK-nexus adversaries are responsible for a higher volume of activity targeting the LATAM region than Iran- and Russia-nexus adversaries.

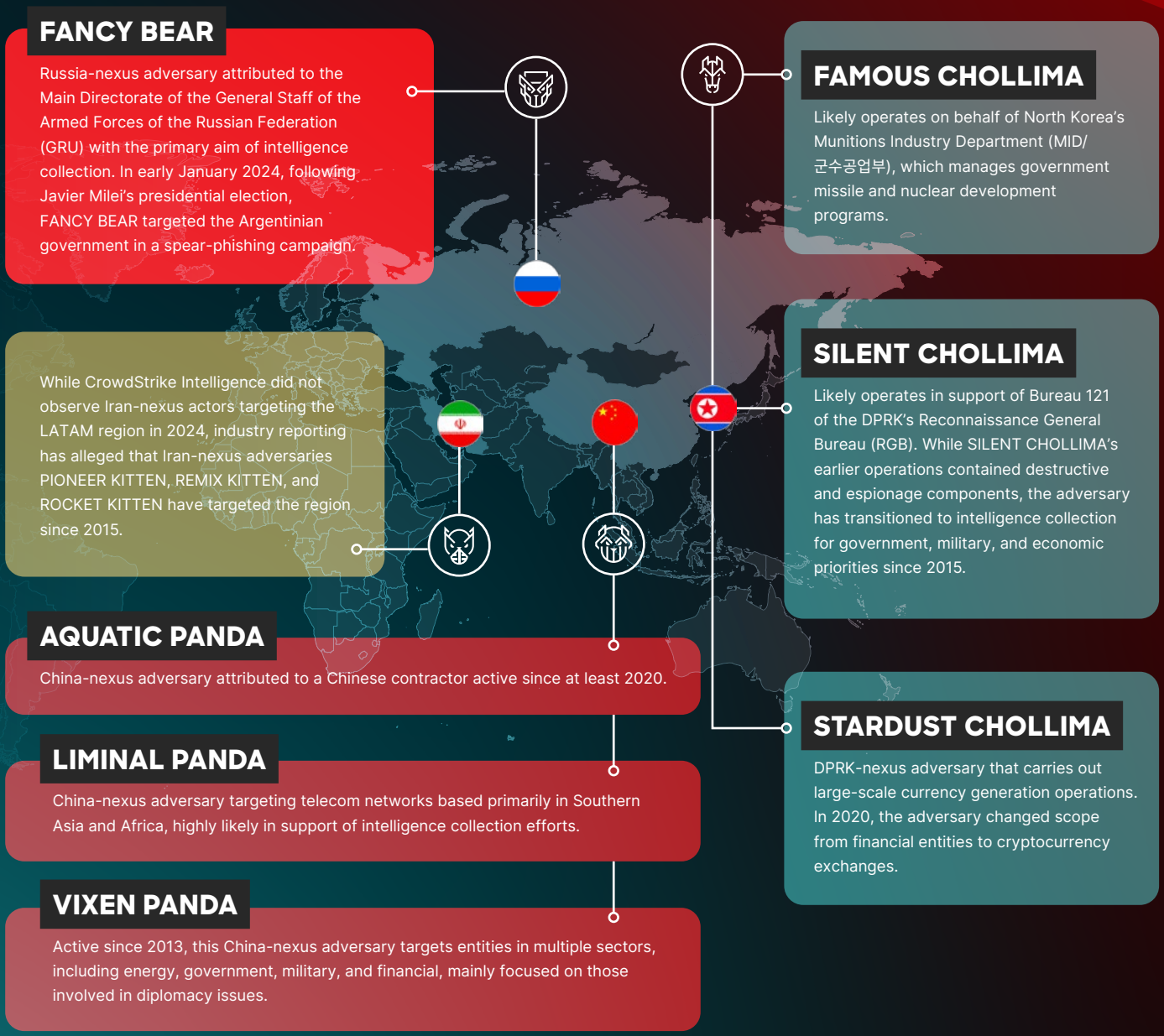

Figure 14. Map of nation-state adversaries targeting LATAM

China-Nexus Adversaries

Although not confined to 2024, CrowdStrike Intelligence has observed China-nexus adversaries AQUATIC PANDA, LIMINAL PANDA, and VIXEN PANDA target the LATAM region, primarily focusing on Central and South America. A joint press release between the Ministry of National Defense of the Republic of Paraguay and the U.S. Embassy in Paraguay also claimed that ETHEREAL PANDA — an adversary broadly aligning with a threat actor publicly tracked as *FLAX TYPHOON* — targeted Paraguay in late 2024.[49] However, CrowdStrike Intelligence cannot currently verify this claim.

In 2024, VIXEN PANDA used an operational relay box (ORB) tracked as ORB02 to likely conduct intrusions globally, including targeting entities in South America. Additionally, in 2022 and 2023, VIXEN PANDA used *Ketrican* to target ministries of foreign affairs in North and South America.

CrowdStrike Intelligence and broader industry reporting indicate that VIXEN PANDA — at least since 2019 — has targeted government organizations and non-governmental organizations (NGOs) in a range of countries in the LATAM region, including Argentina, Brazil, Chile, Colombia, the Dominican Republic, Ecuador, El Salvador, Guatemala, Honduras, Mexico, Panama, Peru, and Venezuela.

In November 2024, CrowdStrike Intelligence determined that LIMINAL PANDA — an adversary primarily targeting telecom networks highly likely in support of intelligence collection efforts — likely gained access to telecom providers located in Central and South America based on analysis of external DNS (eDNS) server logs. The adversary has likely used compromised telecom servers to also target providers in other geographic regions and exhibits expertise of telecom networks, including understanding interconnections between providers and mobile protocols.

AQUATIC PANDA — attributed to a Chinese contractor — has likely targeted South America-based entities from 2022 to 2024. In 2022, the adversary likely targeted email servers belonging to government and telecom entities in South America. In 2023, AQUATIC PANDA likely conducted reconnaissance against entities in Brazil. Evidence also indicates that the adversary has targeted military entities in Peru.

Unattributed China-Nexus Activities

In 2024, CrowdStrike Intelligence observed *SysloggerRAT* campaigns targeting South America-based retail, sporting, and logistics entities. *SysloggerRAT* is a Linux-based RAT written in Golang and primarily associated with China-nexus targeted intrusions.

In 2023, industry reporting claimed that an unknown China-nexus threat actor compromised South American government entities; though this activity remains unattributed to any known adversaries, CrowdStrike Intelligence assesses it is likely associated with an actor using TTPs consistent with China-nexus adversaries.

49 https://www.southcom.mil/MEDIA/NEWS-ARTICLES/Article/3979394/us-strengthens-cybersecurity-partnership-with-paraguay/

DPRK-Nexus Adversaries

Over the past year, CrowdStrike Intelligence has observed DPRK-nexus adversaries FAMOUS CHOLLIMA, SILENT CHOLLIMA, and STARDUST CHOLLIMA conduct likely opportunistic campaigns in the LATAM region for financial gain and, less frequently, cyber espionage.

In 2024, CrowdStrike observed FAMOUS CHOLLIMA activity in Argentina, Brazil, and Uruguay. The adversary illicitly obtains freelance or full-time equivalent work to earn a salary that can be funneled to North Korea. When employed, FAMOUS CHOLLIMA can also deploy malware to collect information that could likely be used for DPRK technological and defense-related development. This threat actor's campaigns in LATAM are opportunistic rather than targeted.

In late 2023, CrowdStrike Intelligence observed SILENT CHOLLIMA deploy *NineRAT* in a Colombian agricultural entity, likely to support North Korea's effort to solve its ongoing food shortage. In October 2024, CrowdStrike identified STARDUST CHOLLIMA deploying macOS malware *MinKit* at a Mexico-based cryptocurrency entity. The adversary used *MinKit* to deploy additional malware *StreamInjector*, *GillySocket*, and *ExtendedReach*.

Unattributed Targeted Activities

In 2024, CrowdStrike Intelligence observed unattributed incidents targeting telecom providers in South America. These activities included the *LightBasin* activity cluster and an unidentified adversary installing a modified *socat* version.

The *LightBasin* activity cluster is an unattributed adversary that has been observed targeting telecom providers and financial institutions worldwide since mid-2020, including ones based in Central and South America.

Non-State Overview

Throughout 2024, CrowdStrike Intelligence observed global hacktivists as well as likely Latin American hacktivists conducting various ideologically and politically motivated cyber operations in the Caribbean, Central and South America, and Mexico. A review of hacktivist incidents over the past year indicates hacktivists targeting the region are generally motivated by geopolitical events and perceived domestic governance issues.

Geopolitical events that spurred hacktivist campaigns include but are not limited to Venezuela's July 2024 presidential election, deteriorating living conditions and human rights violations in Cuba, perceived government graft in Guatemala, and the ongoing Israel-Hamas war.

Hacktivism to Expose Transnational Criminal Organizations (TCOs)

While hacktivists have historically rarely targeted TCOs (likely due to the threat of violent reprisals), throughout 2024, CrowdStrike Intelligence observed limited cyber operations purportedly aimed at exposing or undermining TCOs. In April 2024, hacktivist entity *AFS_Nemesis* (AFS is an acronym for AntiFentySec) announced they were developing software to expose Mexican cartels for their role in fentanyl supply chains.

In May 2024, *GhostSec* leaked data and published a dossier allegedly revealing ties between Mexican public and private sector entities and Mexico-based TCOs. In July 2024, the group leaked purportedly stolen data that reportedly included locations of weapons and money caches and demonstrated further ties between a Mexican state government and TCOs. CrowdStrike Intelligence cannot verify the data's authenticity.

Given that hacktivists frequently target perceived corrupt or unjustly violent government-affiliated organizations, hacktivist entities will likely continue to expose TCOs, especially those with perceived government ties.

Hacktivism Adjacent to Geopolitical Events Mirrors Historical Targeting Trends

Consistent with activity predating 2024, hacktivist entities continued to claim cyber operations predominantly targeting government or government-affiliated entities in response to perceived injustices against civilians or human rights violations.

Global hacktivists claimed many cyber operations targeting the July 2024 Venezuelan presidential election almost certainly due to widespread international claims of election fraud and the perceived illegitimacy of President Nicolás Maduro's government. The operations were likely intended to protest Maduro's government and demonstrate solidarity with domestic protestors.

For example, *Anonymous* affiliates claimed to have targeted a state-run mobile application reportedly enabling vigilantism against protestors as well as dozens of government-associated websites, likely via distributed denial-of-service (DDoS) attacks. Additionally, in early August 2024, hacktivist group *GlorySec* claimed to have breached Maduro's party website and leaked information purportedly related to Venezuelan government and media sector social media accounts as part of the group's campaign targeting Venezuela adjacent to the July 2024 election. From September 2024 to October 2024, *Anonymous* affiliates claimed to have conducted DDoS attacks[50] and hack-and-leak operations[51] targeting non-state or private sector entities the hacktivists perceived as supporting Maduro's regime.

---

50 https://x.com/White_Hunters/status/1837708682882379989

51 https://x.com/YourAnonHunters/status/1851363295963320823
https://x.com/YourAnonHunters/status/1851361153684779223
https://t.me/AnonHuntersLATAM/7463

Similarly, global hacktivists conducted cyber operations in purported support of domestic protests against the Cuban government and to raise awareness of the Cuban government's ties to China. In March 2024, an *Anonymous* affiliate conducted a series of likely cyber operations targeting various Cuban entities in solidarity with Cubans protesting ongoing power outages and widespread food shortages. In September 2024, *Anonymous*-affiliated hacktivist group *GhostSec*, which has consistently conducted cyber operations targeting the Cuban government, often in tandem with public protests, announced the revival of its Operation CubaLibra to expose Cuban and Chinese government ties.

Global hacktivists also targeted various government entities due to perceived corruption. In January 2024, *Anonymous* affiliates claimed to have conducted DDoS attacks targeting Guatemalan entities the hacktivists claimed had impeded the democratic transfer of power from former President Alejandro Giammattei to current President Bernardo Arévalo.

In April 2024, hacktivist entity *Cult of the Dead Cat* (*CoDC*) claimed a hack-and-leak operation targeting an Ecuadorian government ministry, likely related to the country's referendum vote on constitutional amendments to support counter-crime measures adopted under a state of emergency. In May 2024, an *Anonymous* affiliate claimed to have conducted a DDoS attack against a Nicaraguan law enforcement entity, citing unspecified violations of citizens' rights.[52]

Table 1 provides an overview of additional hacktivist entities targeting Latin American entities or based in Latin American countries.

HACKTIVIST ENTITY	DESCRIPTION OF HACKTIVIST ENTITY'S REGIONAL ACTIVITY
CiberInteligencia El Salvador	Active since at least July 2023, *CiberInteligencia El Salvador* claimed a series of alleged hack-and-leak operations targeting Salvadoran public entities. The group's targeting was likely prompted by grievances with the Salvadoran government, including displeasure at the government's purported cybersecurity posture and domestic insecurity issues. Despite May 2024 indications they were expanding targeting to private sector entities and potentially to other LATAM countries, the group has continued to target Salvadoran government entities as recently as late September 2024.[53]
GhostSec	*GhostSec* has engaged in various regional hack-and-leak campaigns targeting several Latin American countries, citing government corruption, mismanagement, or human rights violations, such as widely reported Venezuelan electoral fraud.
LulzSec Muslims	Throughout August 2024, pro-Palestinian and pro-Islam hacktivist group *LulzSec Muslims* claimed to have conducted various cyber operations targeting Argentina-based entities in response to the Argentine government's perceived support of Israel. The alleged activity was part of a broader campaign targeting multiple countries that *LulzSec Muslims* deemed supporters of Israel.
SiegedSec (disbanded)	*SiegedSec*, a hacktivist entity active since at least February 2022 until they announced their disbandment in July 2024, claimed one likely opportunistic breach of a Mexico-based electronic security solutions provider, citing entertainment and the victim entity's alleged lack of "basic security" as motives.
USDoD	Since at least 2020 and until August 2024, hacktivist entity *USDoD* focused on high-profile targeted intrusion campaigns primarily targeting the U.S. military, law enforcement, and defense contractors. Following an August 2024 CrowdStrike Intelligence attribution report, the Brazilian individual almost certainly behind the *USDoD* persona acknowledged the attribution. In mid-October 2024, Brazilian authorities arrested the individual.

Table 1. Latin American hacktivism coverage

52 https://x.com/YourAnonHunters/status/1792568293737250976
53 https://t.me/guacamayal/6068

Guacamaya's Impact on the Latin American Hacktivist Ecosystem

Throughout 2022, hacktivist entity *Guacamaya* — an indigenous-rooted Spanish word for "macaw" — claimed at least three major cyber campaigns targeting Latin American private and public sector oil and mining companies and Latin American government entities. *Guacamaya* has typically exploited publicly acknowledged vulnerabilities on unpatched systems to gain access to victim networks and then subsequently leaked the data via leak publishing platforms *Enlace Hacktivista* and *Distributed Denial of Secrets* (*DDoSecrets*).

Specifically, *Guacamaya* published a video that purports to show them exploiting CVE-2021-26855 in Microsoft Exchange — first disclosed in March 2021 — for initial access at a mining entity, harvesting credentials from the Local Security Authority (LSA) for lateral movement, and using living-off-the-land techniques to wipe data.

Although there has been no publicly reported *Guacamaya* activity in 2024, their past operations almost certainly spurred law enforcement action in Mexico in March 2023, a criminal investigation in Colombia in October 2022, and U.S. sanctions targeting a Guatemalan subsidiary of a Swiss-based mining conglomerate in November 2022.

Guacamaya likely emboldened nascent ideologically motivated hacktivist entities and encouraged copycat cyber campaigns. For example, in March 2022 *Guacamaya* published their "Mining Secrets" hack-and-leak campaign and published a video tutorial showing how they conducted the cyber operation, almost certainly as a knowledge sharing tool for emergent hacktivist entities. Fellow hacktivist entity *CiberInteligencia El Salvador* has invoked *Guacamaya*'s name in their cyber operations, almost certainly for reputational clout.

Conclusion

Throughout 2024, CrowdStrike observed several trends that defined the region's cybersecurity posture. These trends are likely to continue in 2025, as they are rooted in policy questions that have yet to be fully resolved or reconciled by regional governments.

CrowdStrike Intelligence observed several macro cyber trends that transcended regional boundaries and nation-state borders, including governments bolstering their domestic cybersecurity infrastructure as well as engaging in collaboration and knowledge sharing with foreign partners; the two notable exceptions were authoritarian regimes Cuba and Venezuela, both of which allegedly engaged in offensive cyber operations and in the online subjugation of their respective domestic populations. These trends will almost certainly continue in 2025, based on a review of planned cyber legislation and scheduled multilateral forums.

CrowdStrike Intelligence also observed several micro cyber trends, including governments wrestling with politically sensitive policy questions regarding whether to include Chinese technology vendors in the bidding process for government contracts, effective stewardship of AI technology, and governments announcing investigations into the domestic weaponization of spyware to surveil political opponents. These trends will likely persist in the near term, based on regional governments' mercurial policies toward Chinese technology vendors, nascent AI governance strategies, and fluctuating political will regarding the legality of spyware to surveil political opponents.

Throughout 2024, CrowdStrike Intelligence observed numerous predominant cyber threats targeting the region. CrowdStrike Intelligence observed that most cyberattacks targeting Latin America and the Caribbean were conducted by eCrime and BGH actors, followed by global and regional hacktivists and global and regional nation-state threats. In 2025, similar themes are likely, as threat actors have demonstrated resiliency and adaptability in their persistent evolution of their TTPs to continue targeting the region.

RansomHub RaaS and *LockBit* RaaS represented the dominant LATAM ransomware threats in 2024. Additionally, well-known LATAM eCrime malware continued to evolve due to operators leveraging novel techniques — such as adopting new obfuscation methods and new programming languages — to improve defensive evasion. This highlights developers adapting to the fluid eCrime ecosystem in an attempt to hinder analysis and evade host-based detections. This will likely continue in the future, based on threat actors' continued TTP adaptations.

Global hacktivists and likely LATAM-based hacktivists conducted varied ideologically and politically motivated cyber operations targeting public and private sector entities throughout 2024. The groups' claimed activity and purported motivations suggest hacktivists targeting LATAM and the Caribbean were typically motivated by geopolitical events and perceived domestic governance issues. In the near term, geopolitical events will likely continue serving as catalysts for hacktivist cyber campaigns, based on a review of geopolitical events over the past year that were punctuated or accompanied by subsequent hacktivist activity.

Lastly, CrowdStrike Intelligence did not observe a significant amount of Russia-, Iran-, or DPRK-nexus adversary activity targeting public and private sector entities in LATAM and the Caribbean during 2024. However, China-nexus threat actors represented the largest number of identified intrusions, with cyber operations predominantly targeting Central and South American entities.

China-nexus threat actors will likely remain at least a primary and the most consistent state-sponsored intrusion threat based on the country's continued goal of projecting economic and diplomatic influence in LATAM. Further, absent a shift in foreign policy objectives, limited information suggests Russia-, Iran-, and DPRK-nexus adversaries have prioritized cyber-enabled intelligence collection in the region, with little motive for these countries to conduct destructive or disruptive operations.

Recommendations

1 Secure the entire identity ecosystem

Adversaries increasingly target identities using credential theft, multifactor authentication (MFA) bypass, and social engineering while covertly moving laterally between on-premises, cloud, and software as a service (SaaS) environments via trusted relationships. This allows them to impersonate legitimate users, escalate access, and evade detection.

Organizations should adopt phishing-resistant MFA solutions, such as hardware security keys, to prevent unauthorized access. Strong identity and access policies are essential, including just-in-time access, regular account reviews, and conditional access controls. Identity threat detection tools must monitor behavior across endpoints and on-premises, cloud, and SaaS environments to flag privilege escalation, unauthorized access, and backdoor account creation. Integrating these tools with extended detection and response (XDR) platforms ensures comprehensive visibility and a unified defense against adversaries.

Additionally, organizations should educate users to recognize vishing and phishing attempts while maintaining proactive monitoring to detect and respond to identity-based threats.

2 Eliminate cross-domain visibility gaps

Adversaries' growing use of hands-on-keyboard techniques and legitimate tools makes detection and response more difficult. Unlike traditional malware, these methods allow attackers to bypass traditional security measures by executing commands and using legitimate software to mimic normal operations.

To counter this, organizations must modernize their detection and response strategies. XDR and next-generation security information and event management (SIEM) solutions provide unified visibility across endpoints, networks, cloud environments, and identity systems, enabling analysts to correlate suspicious behaviors and see the full attack path.

Proactive threat hunting and threat intelligence further enhance detection by identifying potential attack patterns and providing insights into adversary TTPs. With real-time intelligence, organizations can stay informed about emerging threats, anticipate attacks, and prioritize critical security efforts.

3 Defend the cloud as core infrastructure

Cloud-focused adversaries are exploiting misconfigurations, stolen credentials, and cloud management tools to infiltrate systems, move laterally, and maintain persistent access for malicious activities like data theft and ransomware deployment.

Cloud-native application protection platforms (CNAPPs) with cloud detection and response (CDR) capabilities are critical to counter these threats.

These solutions provide operators with a unified view of their cloud security posture, helping them rapidly detect, prioritize, and remediate misconfigurations, vulnerabilities, and adversary threats. Additionally, enforcing strict access controls — such as role-based access and conditional policies — limits exposure to critical systems and ensures continuous monitoring for anomalies, including logins from unexpected locations.

Regular audits are also critical to maintaining security. Automated tools can uncover overly permissive storage settings, exposed APIs, and unpatched vulnerabilities. Frequent reviews of cloud environments ensure unused permissions and outdated configurations are addressed promptly.

4 Prioritize vulnerabilities using an adversary-centric approach

Adversaries are increasingly exploiting publicly disclosed vulnerabilities and using exploit chaining, where they combine multiple vulnerabilities to gain rapid access, escalate privileges, and bypass defenses. These multi-stage attacks often rely on public resources like proof-of-concept exploits and technical blogs, enabling adversaries to craft effective and hard-to-detect payloads.

To counter these threats, organizations must prioritize regular patching or upgrading of critical systems, especially frequently targeted internet-facing services like web servers and VPN gateways. Monitoring for subtle signs of exploit chaining, such as unexpected crashes or privilege escalation attempts, can help detect attacks before they progress.

Tools like CrowdStrike Falcon® Exposure Management, built with native AI prioritization, enable teams to reduce noise and focus on the vulnerabilities that matter most, specifically those affecting critical and high-risk systems. By adopting proactive security approaches, discovering exposures across the attack surface, and leveraging automation, organizations can mitigate sophisticated threats and limit adversary opportunities.

5 Know your adversary and be prepared

When a cyberattack unfolds in minutes — or even seconds — being prepared can be the difference between containment and catastrophe. An intelligence-driven approach enables security teams to move beyond reactive defense by understanding which adversary is targeting them, how they operate, and what their objectives are. With threat intelligence, adversary profiling, and tradecraft analysis, security teams can prioritize resources, adapt defenses, and actively hunt for threats before they escalate. CrowdStrike's threat intelligence doesn't just detect known threats — it anticipates new and evolving tradecraft, ensuring defenders are always one step ahead. By seamlessly integrating intelligence into security workflows, organizations can accelerate response times, disrupt adversaries, and turn intelligence into action.

Though technology is critical to detect and stop intrusions, the end user remains a crucial link in the chain to stop breaches. Organizations should initiate user awareness programs to combat the continued threat of phishing and related social engineering techniques. For security teams, practice makes perfect. Encourage an environment that routinely performs tabletop exercises and red/blue teaming to identify gaps and eliminate weaknesses in your cybersecurity practices and response.

CrowdStrike Falcon Platform

AI and Cloud-Native

Leverages the network effect of crowdsourced security data while eliminating the management burden of cumbersome on-premises solutions

Single Lightweight Agent

Provides frictionless and scalable deployment and stops all types of attacks while eliminating agent bloat and scheduled scans

Charlotte AI

Powers the CrowdStrike portfolio of generative AI capabilities across the CrowdStrike Falcon® platform, tapping into the petabyte scale of CrowdStrike's automated intelligence — and further enriched by security experts — to accelerate analyst workflows

Falcon Fusion SOAR

Provides native security orchestration, automation, and response (SOAR) capabilities within the Falcon platform to allow you to collect contextually enriched data and automate security operations, threat intelligence, and incident response — all in a single platform and through the same console — to mitigate cyber threats and vulnerabilities

CrowdStrike Asset Graph

Solves one of the most complex customer problems today: identifying assets, identities, and configurations accurately across all systems — including cloud, on-premises, mobile, internet of things (IoT), and more — and connecting them together in a graph form

CrowdStrike Intel Graph

Enables security teams to proactively defend against emerging threats with intelligence-driven insights by mapping relationships between threat actors, tactics, vulnerabilities, and real-world attacks

CrowdStrike Threat Graph

Uses cloud-scale AI to correlate trillions of data points from multiple telemetry sources to identify shifts in adversarial tactics and map tradecraft to automatically predict and prevent threats in real time across CrowdStrike's global customer base

Falcon Foundry

Allows customers and partners to easily build custom, no-code applications that harness the data, automation, and cloud-scale infrastructure of the Falcon platform to solve your toughest cybersecurity challenges

CrowdStrike Marketplace

Offers an enterprise marketplace of technology partners where you can discover, try, buy, and deploy trusted CrowdStrike and partner applications that extend the CrowdStrike Falcon platform without adding agents or increasing complexity

CrowdStrike Products

Endpoint Security

FALCON PREVENT | NEXT-GENERATION ANTIVIRUS

Protects against all types of threats, from malware and ransomware to sophisticated attacks, and deploys in minutes, immediately protecting your endpoints

FALCON INSIGHT XDR | EXTENDED DETECTION AND RESPONSE

Offers industry-leading, unified endpoint detection and response (EDR) and XDR with enterprise-wide visibility to automatically detect adversary activity and respond across endpoints and all key attack surfaces

FALCON DATA PROTECTION | UNIFIED DATA PROTECTION

Provides deep real-time visibility into what is happening with sensitive data and stops data theft with policy enforcement that automatically follows content, not files

FALCON FIREWALL MANAGEMENT | HOST-BASED FIREWALL

Delivers simple, centralized host firewall management, making it easy to manage and control host firewall policies

FALCON DEVICE CONTROL | USB SECURITY

Provides the visibility and precise control required to enable safe usage of USB devices across your organization

FALCON FOR MOBILE | MOBILE THREAT DETECTION

Protects against threats to iOS and Android devices, extending XDR/EDR to your mobile devices, with advanced threat protection and real-time visibility into app and network activity

FALCON FORENSICS | FORENSIC CYBERSECURITY

Allows you to quickly respond and recover with automated forensic data collection, enrichment, and correlation

FALCON GO | SMB CYBER PROTECTION

Gives small businesses peace of mind against cyber threats with easy-to-install next-gen antivirus, device control, and mobile device protection

FALCON INSIGHT FOR XIoT | XIoT ASSET PROTECTION

Delivers industry-leading protection for extended internet of things (XIoT) devices — such as operational technology, IoT, and industrial control systems — by providing real-time visibility, threat detection, and prevention across connected environments

Counter Adversary Operations

FALCON ADVERSARY OVERWATCH | THREAT HUNTING

Provides 24/7 protection across endpoints, identities, cloud workloads, and next-gen SIEM delivered by AI-powered threat hunting experts and includes built-in threat intelligence to expose adversary tradecraft, vulnerabilities, and stolen credentials

FALCON ADVERSARY INTELLIGENCE | SOC AUTOMATION

Cuts response time from days to minutes across the entire SOC with end-to-end intelligence automation, enabling you to instantly submit potential threats to an advanced malware sandbox, extract indicators of compromise, and deploy countermeasures — all while continuously monitoring for fraud and safeguarding your brand, employees, and sensitive data

FALCON ADVERSARY INTELLIGENCE PREMIUM | ADVERSARY INTELLIGENCE

Delivers industry-leading intelligence reporting at your fingertips, along with prebuilt detections and one-click hunting, to cut the time and cost required to understand and defend against sophisticated nation-state, eCrime, and hacktivist adversaries

FALCON COUNTER ADVERSARY OPERATIONS ELITE | ON-DEMAND ANALYST

Provides an assigned analyst who leverages AI-powered investigative and threat hunting tools, enhanced by deep adversary intelligence, to detect and disrupt adversaries across your IT environment and beyond

Cloud Security

FALCON CLOUD SECURITY: PROACTIVE SECURITY

Provides unified security posture management (USPM) and business context across cloud layers, leveraging industry-leading threat intelligence, end-to-end attack paths, and ExPRT.AI so cloud teams can swiftly prioritize their work, neutralize critical risks, and leave adversaries no room to strike

FALCON CLOUD SECURITY: CLOUD RUNTIME PROTECTION

Delivers leading cloud workload protection (CWP) and cloud detection and response (CDR), allowing SOC teams to detect and respond to active threats across hybrid clouds so adversaries are stopped in their tracks

FALCON CLOUD SECURITY: CNAPP

Includes the features and capabilities of both Proactive Security and Cloud Runtime Protection for Falcon Cloud Security

FALCON ADVERSARY OVERWATCH: CLOUD | THREAT HUNTING

Offers both proactive and protective security as a managed service through Falcon Adversary OverWatch cross-domain threat hunting and Falcon Complete Next-Gen MDR, powered by integrated threat intelligence to protect the cloud control plane, host operating system, and data plane

SaaS Security

FALCON SHIELD | SAAS APPLICATION SECURITY

Enables security teams to secure their entire SaaS stack through threat prevention, detection, and response; proactively find and fix weaknesses across their SaaS stack; and maintain continuous security for all configurations, human and non-human users, data, and SaaS genAI

Identity Protection

FALCON IDENTITY THREAT DETECTION

Provides unified visibility across hybrid identities and AI-driven threat detection to expose identity-based threats before they escalate

FALCON IDENTITY THREAT PROTECTION

Secures hybrid identities with AI-driven threat detection and behavioral analytics, leveraging the unified Falcon platform to stop identity-based attacks in real time

FALCON ADVERSARY OVERWATCH: IDENTITY | THREAT HUNTING

Provides 24/7 managed identity threat hunting, proactively detecting identity-based attacks, monitoring criminal forums for stolen credentials, and enforcing MFA challenges to prevent unauthorized access

Next-Gen SIEM

FALCON NEXT-GEN SIEM | SIEM

Empowers you to stop breaches and streamline your SOC by unifying industry-best detection, world-class threat intelligence, blazing-fast search, and AI-led investigation in one platform

Security and IT Operations

FALCON EXPOSURE MANAGEMENT | EXPOSURE MANAGEMENT

Provides full attack surface visibility, prioritizes vulnerabilities with AI, and automates remediation to proactively reduce cyber risk and prevent breaches

FALCON EXPOSURE MANAGEMENT: CAASM

Allows you to discover and monitor managed and unmanaged assets in real time and visually map assets and their relationships, revealing deep host insights into applications, browsers, CVEs, and misconfigurations

FALCON FILEVANTAGE | FILE INTEGRITY MONITORING

Provides real-time, comprehensive, and centralized visibility that boosts compliance and offers relevant contextual data

FALCON ADVERSARY OVERWATCH: NEXT-GEN SIEM | THREAT HUNTING

Proactively hunts advanced threats across the enterprise by correlating first- and third-party CrowdStrike Falcon® Next-Gen SIEM data, disrupting attacks across edge devices, SaaS, email, operating systems, and more

CrowdStrike Services

Managed Services

FALCON COMPLETE NEXT-GEN MDR | MANAGED DETECTION AND RESPONSE

Provides 24/7 expert-driven protection across endpoints, identities, cloud workloads, and third-party data — combining elite security expertise, AI-powered technology, and proactive threat hunting to detect, disrupt, and remediate sophisticated threats in minutes

INCIDENT RESPONSE

Provides 24/7 elite incident response to contain threats, restore order, and mitigate breach impact

Incident Response Services | Provides comprehensive response and recovery in the event of a cyber breach — spanning investigation, remediation, and recovery — backed by world-class threat intelligence and delivered by a highly experienced incident response team

Active Defense Services | Provides cross-domain response to recover from a breach with speed and precision

Services Retainer | Provides on-demand access to CrowdStrike expertise, from rapid response to long-term resilience

STRATEGIC ADVISORY SERVICES

Develops and matures the security program to improve defenses

Tabletop Exercises | Simulates incident response scenarios that expose process gaps and improve coordination across the full team, from hands-on-keyboard analysts to executive stakeholders

Maturity Assessment | Comprehensively evaluates your organization's security posture, identifying gaps, benchmarking capabilities, and providing a prioritized roadmap to strengthen defenses against evolving threats

Regulation Readiness and CXO Advisory | Helps you understand and prepare for cyber-related regulation mandates, including the evolving risk and governance responsibilities of the board of executives

Insider Risk Program Review | Strengthens your insider risk strategy by assessing and optimizing your current detection, prevention, and response capabilities

RED TEAM SERVICES

Tests and validates defenses through emulated attacks that expose weaknesses

Penetration Testing | Provides attack emulations that test the detection and response capabilities of your people, processes, and technology to identify vulnerabilities

Red Team/Blue Team Exercise | Increases response readiness under expert guidance, as a red team attacks systems in a simulated exercise and a blue team mounts the defense

Adversary Emulation Exercise | Gauges readiness to defend against a sophisticated adversary infiltration that employs advanced tradecraft

AI Red Team Services | Exposes vulnerabilities in the genAI stack that could be exploited by testing LLM integrations for sensitive data exposure and adversarial manipulation

TECHNICAL ASSESSMENT SERVICES

Audits and addresses security gaps across endpoints, cloud, and SaaS applications to tangibly reduce risk

SaaS Security Assessment | Assesses SaaS environments for security gaps across configurations, access controls, data policies, and third-party integrations

Technical Risk Assessment | Highlights security vulnerabilities, weaknesses, and gaps in the IT environment across endpoint devices, applications, and user identities

Identity Security Assessment | Audits identity security practices and defense posture for weaknesses, including Active Directory domain configuration, account configuration, privilege delegation, and potential attack paths

Cloud Security Assessment | Identifies misconfigurations and vulnerabilities in the cloud estate that could be exploited by adversaries

Compromise Assessment | Exposes and addresses undetected threat activity through a one-time threat hunt available for endpoint, cloud, and SaaS applications

TRAINING AND SECURITY UPSKILLING

Builds security acumen and closes the skills gap through CrowdStrike University, offering on-demand training, personalized learning paths, and five certifications for deep Falcon module expertise

CROWDSTRIKE PULSE SERVICES

Provides continuous consulting via focused sessions on a recurring cadence — biweekly, monthly, or every two months — tailored to your evolving needs. These engagements align with your priorities and adapt as needed, enabling consistent progress, improved resilience, and strategic maturity that evolves at the speed of the adversary

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

Learn more: www.crowdstrike.com

Follow us: Blog | X | LinkedIn | Facebook | Instagram | YouTube

Start a free trial today: www.crowdstrike.com/free-trial-guide