CYBER
THREAT
ANALYSIS

Recorded Future®

Insikt Group®

April 2, 2026

Latin America and the Caribbean Cybercrime Landscape

Insikt Group assesses that DarkForums and Telegram are the primary special-access forums and communications platforms used by threat actors operating in or targeting Latin America and the Caribbean (LAC).

Threat actors operating in or targeting LAC are often financially motivated and leverage social engineering, ransomware, and various forms of mobile malware for initial access to critical sectors.

Insikt Group noted that in LAC, threat actors leveraged banking trojans in targeted WhatsApp smishing campaigns, and LummaC2 was the most-used infostealer in 2025, succeeded by Vidar following LummaC2's disruption.

Executive Summary

This report provides an overview of trends and developments in the cybercriminal ecosystem of Latin America and the Caribbean (LAC) in 2025. Insikt Group found that threat actors operating in or targeting the LAC region predominantly use client-server applications and end-to-end encrypted messaging platforms such as Telegram, as well as established English- or Russian-speaking dark web and special-access forums, to communicate and conduct activities. Threat actors demonstrate increased sophistication in their operations, adapting their tactics, techniques, and procedures (TTPs) over time, while still relying primarily on traditional methods such as phishing and social engineering, malware distribution, and ransomware. Based on our analysis, we have determined that Brazil, Mexico, and Argentina were the countries most targeted by financially motivated cybercriminals, likely because they are LAC's largest economies. Additionally, based on this research, Insikt Group found that threat actors often targeted critical industries such as healthcare, finance, and government because they hold high-value data, face operational urgency, and, at times, rely on legacy systems that may be vulnerable.

Key Findings

- Insikt Group assesses that criminal forum DarkForums and the messaging platform Telegram are the primary special-access forums and communications platforms used by threat actors operating in or targeting the LAC region.
- Threat actors operating in or targeting LAC are typically financially motivated and frequently leverage social engineering, ransomware, and various forms of mobile malware to gain initial access to government, healthcare, and financial institutions.
- In 2025, Insikt Group recorded 452 ransomware incidents impacting the LAC region. The top five industries affected were healthcare, manufacturing, government, information technology, and education, all of which observed a noticeable increase in attacks compared to the previous year.
- Insikt Group continued to identify banking trojans being leveraged by threat actors, with established variants being the most widely used. Specifically, threat actors used banking trojans in targeted smishing campaigns targeting WhatsApp users to gain access to financial data and steal credentials.
- Insikt Group identified LummaC2 as the most prolific information stealer (infostealer) affecting organizations in LAC in the first half of 2025 and Vidar in the second half, following law enforcement disruption of LummaC2.

Background

In the aftermath of the COVID-19 pandemic, the LAC region underwent rapid digital development that outpaced security maturity, leading to asymmetrical cloud adoption, reliance on legacy infrastructure, and the introduction of remote work across all verticals. Many organizations adopted software-as-a-service (SaaS) platforms without effectively implementing strong access controls or multi-factor authentication (MFA) methods, leaving them exposed to ransomware and data theft, among other cyberattacks. Economic instability (inflation and currency controls) in LAC countries has created incentives for cybercrime while weakening institutional defenses. Political volatility, social protests, and corruption have created new opportunities for financially and politically motivated threat actors. Compounded factors such as high youth unemployment, income inequality, and the influence of informal economies have driven individuals to seek alternative sources of income, which in turn fuels much of the cybercrime we see today.

According to a World Economic Forum report, 13% of respondents in the LAC region expressed low confidence in their country's preparedness to respond to significant cyber incidents. Despite significant progress in digital government, regulatory advancements, and investments in the region, many countries still lack the technical competence in their workforce and the resources to sustainably harden their environments. Many LAC government networks hold large amounts of sensitive data but are deficient in their security best practices, leaving their systems vulnerable to cyberattacks. Large breaches are routinely circulated, recycled, and resold on dark web marketplaces, enabling identity theft, synthetic identity fraud, SIM swaps, and account takeovers, among other types of cybercriminality to flourish at a larger scale.

Although the LAC region has made significant technological advancements, particularly in the financial services sector, innovations are creating new challenges. The financial technology industry has introduced mobile banking applications, digital wallets, and instant payment systems. LAC countries face rising levels of cyber-enabled fraud in the financial sector because real-time payment rails have weaker identity verification controls, rendering social engineering attempts more effective. Instant payment systems, such as Brazil's PIX and similar mobile banking platforms, have often been targeted by threat actors. With faster transaction speeds at higher volumes, detection and recovery efforts have become increasingly complex, making scams significantly more profitable and scalable.

The LAC region has the world's fastest-growing rate of disclosed cyber incidents, though many remain unreported. Only seven LAC countries have plans to protect their critical infrastructure from cyberattacks, and only twenty have Computer Security Incident Response Teams (CSIRTs). Despite 31 LAC countries having some form of legislation addressing cybercrime, many face skills shortages, creating barriers to enforcement. Limited law enforcement resources and unreliable interstate cooperation further delay investigation and prosecution, enabling threat actors to operate across jurisdictions with relative ease. A cultural perception that cybercrime carries low risk and offers high reward undermines the deterrent effect that reliable law enforcement action would otherwise have. This

incentive structure, coupled with reduced stigma, encourages repeat offenses and recruitment, as reflected in the cybercriminal trends observed by Insikt Group in 2025.

Cybercriminal Activities in LAC

Throughout 2025, Insikt Group investigated and identified different types of cybercriminals operating on clearnet and dark web sources. Cybercriminals routinely leveraged phishing for initial access, and among the most common methods seen was the search and collection of sensitive information directly from a compromised host's file system or databases. This technique is often a critical pre-exfiltration step used to obtain financial records, passwords, and other forms of personally identifiable information (PII), likely to conduct account takeovers or fraud. Insikt Group research found that cybercriminals have also begun evolving their TTPs to exploit near-field communications (NFC) to commit financial fraud and are using malware to target cryptocurrency wallets. Insikt Group intelligence indicates that cybercriminals are primarily interested in selling compromised databases and access methods, as well as participating in hacktivist collectives. In some instances, advanced persistent threats (APTs) have also begun to overlap their activities with cybercrime when targeting the region.

Cybercriminal Sources

Threat actors operating in or targeting the LAC region continued to rely on the infrastructure of established English- and Russian-speaking forums throughout 2025 (see **Appendix A**). Insikt Group identified Spanish- and Portuguese-language postings on several established dark web and special-access forums. Even though these sources are predominantly English- and Russian-speaking, these posts likely indicate a preference among threat actors targeting LAC to seek more established, traditional platforms for conducting business. Research showed that low to moderate-tier forums are most commonly used by threat actors based in or targeting LAC countries, possibly suggesting lower levels of sophistication, as higher-tier forums often require vouching, payment, demonstration of knowledge or technical abilities, and sometimes private invitation to gain access.

Insikt Group assesses that most communications between threat actors likely occur on encrypted messaging platforms such as Telegram, WhatsApp, and Signal due to speed, ease of access, and higher levels of trust among group members. Given the privacy-enhancing features of many of these platforms, collection efforts can become significantly more constrained. Telegram is predominantly used because it offers larger channel and group capacities, account creation is simple, it enables threat actors to leverage bot automation and support for their malicious activities, and content moderation is typically less stringent than on other platforms. By offering a path of least resistance, threat actors enjoy the added privacy that end-to-end encrypted messaging platforms provide without delaying their operations.

Financially motivated threat actors often advertise a variety of data types, including PII, financial data, login credentials, system access credentials, exploits and vulnerabilities, malware, ransomware, and hacking tutorials. In some instances, Insikt Group observed threat actors selling customer relationship management (CRM) access, virtual private network (VPN) access with domain user privileges and local

administrator rights on a database server, and command-and-control (C2) access to LAC-based entities in 2025. Leveraging this access to information, cybercriminals may facilitate further crimes, including but not limited to extortion attempts, digital and social engineering scams, ransomware deployment, data theft, and account takeovers. Insikt Group research indicates that threat actors generally advertise breached databases and payment card data because they can be lucrative, require relatively low levels of sophistication, and are sought after by other cybercriminals.

Threat actors often target government systems because they contain highly sensitive data that can be profitable for scams, identity theft, or extortion. For instance, shortly after a tense general election, Ecuador's legislature, the National Assembly, reported it had suffered two cyberattacks aimed at accessing confidential data and disrupting the availability of information services. In another example, threat actors exposed sensitive data on millions of Paraguayan citizens on the dark web; among the alleged exfiltrated data are national ID numbers, dates of birth, physical addresses, and health service records.

DarkForums was the primary dark web and special-access forum where Insikt Group recorded the most posts relating to cybercrime-related events in Spanish and Portuguese in 2025. This forum is an English-language, low-tier forum operated by English-speaking administrators, launched in March 2023, and is accessible via a clearnet domain. Additionally, DarkForums was observed hosting leaked databases and data breaches involving Spanish-speaking countries, with posts describing the compromise of thousands of records and credentials. Other forums, such as XSS, Exploit, RehubcomPro, Cracked, BreachForums 2, ProCrd, and CrdPro, were also among the top forums to contain posts in Spanish and Portuguese. **Appendix A** presents a sample of Spanish and Portuguese forum threads from these sources.

Cybercriminal Tactics and Attack Vectors

The LAC region has a long history of financially motivated cybercrime; as a result, Insikt Group observed in this analysis that threat actors continue to heavily target the financial sector. Threat actors typically rely on traditional initial access methods, such as phishing via email, SMS, and WhatsApp messages, impersonating financial institutions, and requesting invoices or payments. Threat actors deliver lures via malicious links that redirect to fake login pages and contain malicious attachments with embedded links. Many of these techniques are effective when targeting entities in the LAC region due to an overwhelming reliance on email and messaging applications for business, as well as a general strong trust in branded communications. Artificial intelligence (AI) has introduced more sophisticated methods into the cybercriminal ecosystem in LAC, lowering the barrier to entry for threat actors and significantly increasing the scalability of attacks through automation. AI helps threat actors create more effective phishing messages that could be generated in native Spanish or Portuguese, rendering them more convincing to the local target audience. The advent of agentic AI also presents new opportunities and attack vectors for cybercriminal groups to exploit and greatly facilitates cybercrime-as-a-service. Organized criminal groups have integrated AI into their operations to assist with drug smuggling, money laundering, cyber-enabled fraud, and malware development.

Throughout 2025, Insikt Group observed threat actors targeting the LAC region by compromising remote desktop protocol (RDP), VPNs, and web admin panels, and obtaining credentials from prior infostealer infections, password reuse, brute-force attacks, and other initial access points. Based on data within the Recorded Future Intelligence Operations Platform, there are approximately 29,000 references to exposed LAC-related credentials on Russian Market. These exposed credentials are from domains belonging to the top organizations (by revenue) in the healthcare, government, and financial sectors across the five largest economies in LAC. Russian Market is one of the leading dark web marketplaces for the sale and distribution of infostealer logs. Most of these logs were from LummaC2 and then Acreed Stealer, consistent with what Insikt Group observed in its review of additional infostealer logs. It should be noted that many of the 29,000 exposed credentials are likely customers of these organizations and not necessarily employees, as Recorded Future does not have access to internal-facing employee domain addresses to search for exposed credentials; however, those can be added by an end user. Insikt Group assesses that these attack vectors were likely effective for infiltrating the systems of targets in the LAC region due to increased remote work adoption, legacy infrastructure in many public institutions, and limited monitoring and resources. Insikt Group observed threat actors advertising carding tools, bulk SMS/Email blasting, SIM swapping, hacking assistance, and other similar services on Telegram channels.

In 2025, Insikt Group observed a rise in novel types of malware that actively leverage and exploit NFC. First identified by Threat Fabric, PhantomCard is an Android trojan, notably a variant of China-origin NFC relay malware-as-a-service (MaaS), primarily targeting banking customers in Brazil. PhantomCard enables relay attacks by obtaining NFC data from a victim's banking card and transmitting it to a threat actor's device to perform transactions at point-of-sale (POS) systems or ATMs. PhantomCard is distributed via malicious webpages that impersonate legitimate applications, prompting victims to tap their cards and enter their personal identification numbers (PINs) for authentication. Once credentials are fraudulently obtained, they are relayed to attackers.
Similarly, in late 2025, threat actors deployed RelayNFC, a mobile malware that targets contactless payment cards, in a phishing campaign targeting Brazilian users. This evolution in TTPs parallels the shift by threat actors from skimming magnetic stripe data to “shimming” Europay, Mastercard, and Visa (EMV) chip data in the payment fraud ecosystem, since unique cybercriminal solutions typically follow new security innovations.

Per the 2025 Cybercriminal Cryptocurrency Annual Activity Report, Insikt Group consistently observed activity in which cryptocurrency wallets were targeted by various forms of malware, such as drainers, clippers, and miners, to steal funds. Given the persistent lag in cybersecurity measures in LAC and the rapid growth of the cryptocurrency market in the LAC region, its users may become attractive targets for cybercriminals. The top five countries in the LAC region that dominate the cryptocurrency ecosystem are Brazil, Argentina, Mexico, Venezuela, and Colombia. However, Brazil is the clear leader, accounting for a third of overall cryptocurrency activity. Insikt Group assesses that, as the mainstream adoption of cryptocurrency continues, threat actors will likely seek targets in these countries, as knowledge and security practices among the user base in these regions will likely be lacking. Additionally, as with threat actors in other regions of the world, those targeting LAC will almost certainly leverage this medium of exchange to transact and launder illicit funds. As countries continue to adopt

new regulations and introduce new forms of cryptocurrency, we expect threat actors to identify new vectors for exploitation. As of 2025, Argentina, Brazil, Colombia, Ecuador, Paraguay, Trinidad and Tobago, Uruguay, and Venezuela are participating in INTERPOL's inaugural pilot phase for the new Silver Notice, which will be published to "help trace and recover criminal assets, combat transnational organized crime and enhance international police cooperation," likely including cryptocurrency assets if linked to criminal proceeds.

Advanced Persistent Threats (APTs) and Cybercrime

Throughout 2025, Insikt Group observed a rise in APT activity targeting the LAC region using traditional cybercriminal methods, such as phishing and ransomware. This suggests some APT groups may also have financial motivations extending beyond seeking strategic geopolitical influence. Prominent APTs, such as Dark Caracal, conducted cyber espionage and delivered the Poco RAT via financial-themed phishing. TAG-144 (Blind Eagle) primarily targeted government entities in South American countries, notably Colombia, using TTPs such as spearphishing and remote access trojans (RATs) in campaigns blending espionage and financial motives.

Insikt Group assesses that some Chinese state-sponsored activity is likely aimed at protecting economic investments in the region, such as the Belt and Road Initiative (BRI), sovereign loans, and widespread commercial interests. In addition to the above APT groups, Chinese state-sponsored groups are also targeting entities in LAC countries. TAG-141 (FamousSparrow) leveraged SparrowDoor malware against entities in Mexico, Argentina, and Chile. Storm-2603 (Gold Salem) deployed ransomware, including Warlock, LockBit, and Babuk, targeting multiple sectors across agriculture, government, energy and natural resources, and telecommunications in the LAC and Asia-Pacific (APAC) regions. This activity may signal that China is seeking to retain influence in the LAC region through cybercriminal means or is interested in financial gain.

Hacktivism

The LAC region has repeatedly experienced periods of complex political and social unrest fueled by debates regarding economic reforms, corruption, and inequality. Unlike financially motivated cybercrime, hacktivism tends to be political or ideological, and these tense conditions can create an environment where hacktivism spikes. In late 2025, Insikt Group noticed increased activity from Chronus Team, a hacktivist group known for defacement attacks and data leaks aimed at exposing security vulnerabilities, primarily targeting organizations in Mexico. The threat group leverages Telegram channels for communication and propaganda. It has loosely aligned with other hacktivist and cybercriminals groups, such as Elite 6-27 and Sociedad Privada 157, to gain attention and increase its reputation. Insikt Group observed another trend where several hacktivist groups began transitioning to ransomware-as-a-service (RaaS) for financial gain. One such hacktivist group, "FiveFamilies", functions as a collective of several groups; some of their targeted entities included those located in Cuba and Brazil.

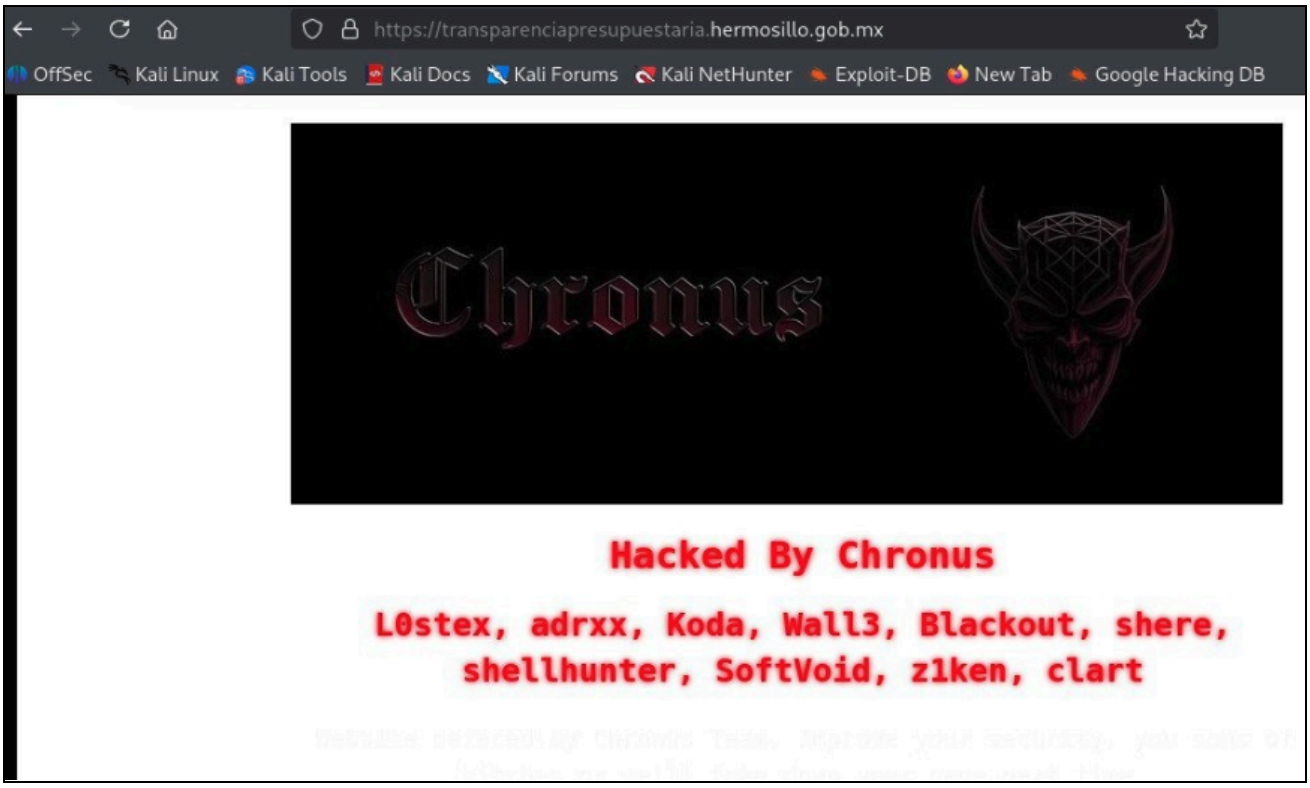


***Figure 1**: Chronus Team hack and web defacement of the website for the budget transparency for the municipality of Hermosillo, Sonora, Mexico (Source: Social Media)*

Malware Trends

In 2025, Insikt Group observed elevated ransomware activity targeting organizations in the LAC region. Additionally, banking trojans also remained a prominent issue affecting LAC countries, with Insikt Group noting an uptick in campaigns specifically leveraging WhatsApp for delivery. Infostealers remained a popular initial access enabler in the LAC region. Botnets have grown in the region largely due to small office/home office (SOHO) devices, such as routers and other internet-of-things (IoT) appliances with weak security, outdated firmware, and a reliance on default credentials. Botnet activity can contribute to credential theft, the propagation of phishing campaigns, the distribution of spam, the takeover and abuse of residential IP addresses, and the enabling of distributed denial-of-service (DDoS) attacks. Insikt Group also observed threat actors targeting payment terminals in 2025 with ATM and POS malware.

Ransomware

In 2025, Recorded Future's Global Ransomware Landscape Dashboard recorded 452 ransomware incidents impacting the LAC region out of 7,346 total globally, based on all publicly known ransomware victims listed on associated ransomware blogs. Attacks on entities in the LAC region constituted just over 6% of all global ransomware attacks in 2025. The top five industries most impacted by ransomware in the LAC region in 2025 were Healthcare (36 attacks), Manufacturing (49 attacks),

Government (28 attacks), Information Technology (21 attacks), and Education (20 attacks), as demonstrated in **Figure 3**. Insikt Group research on ransomware in the LAC region covers 27 of the 33 constituent countries. Insikt Group did not obtain ransomware data from Antigua and Barbuda, Belize, Cuba, Saint Kitts and Nevis, Saint Lucia, or Suriname in 2025.

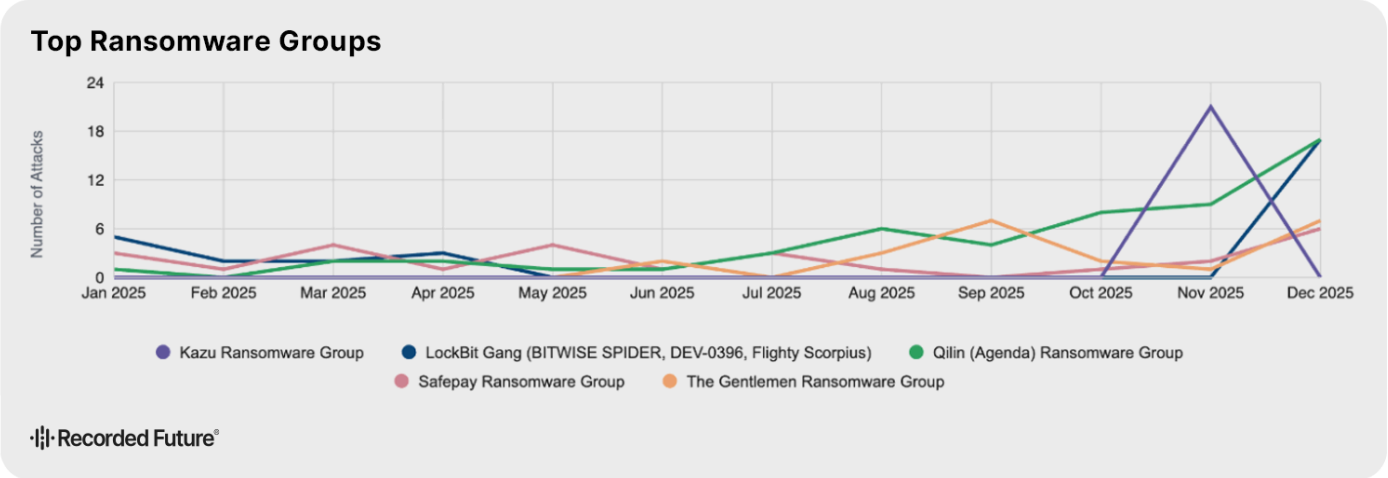
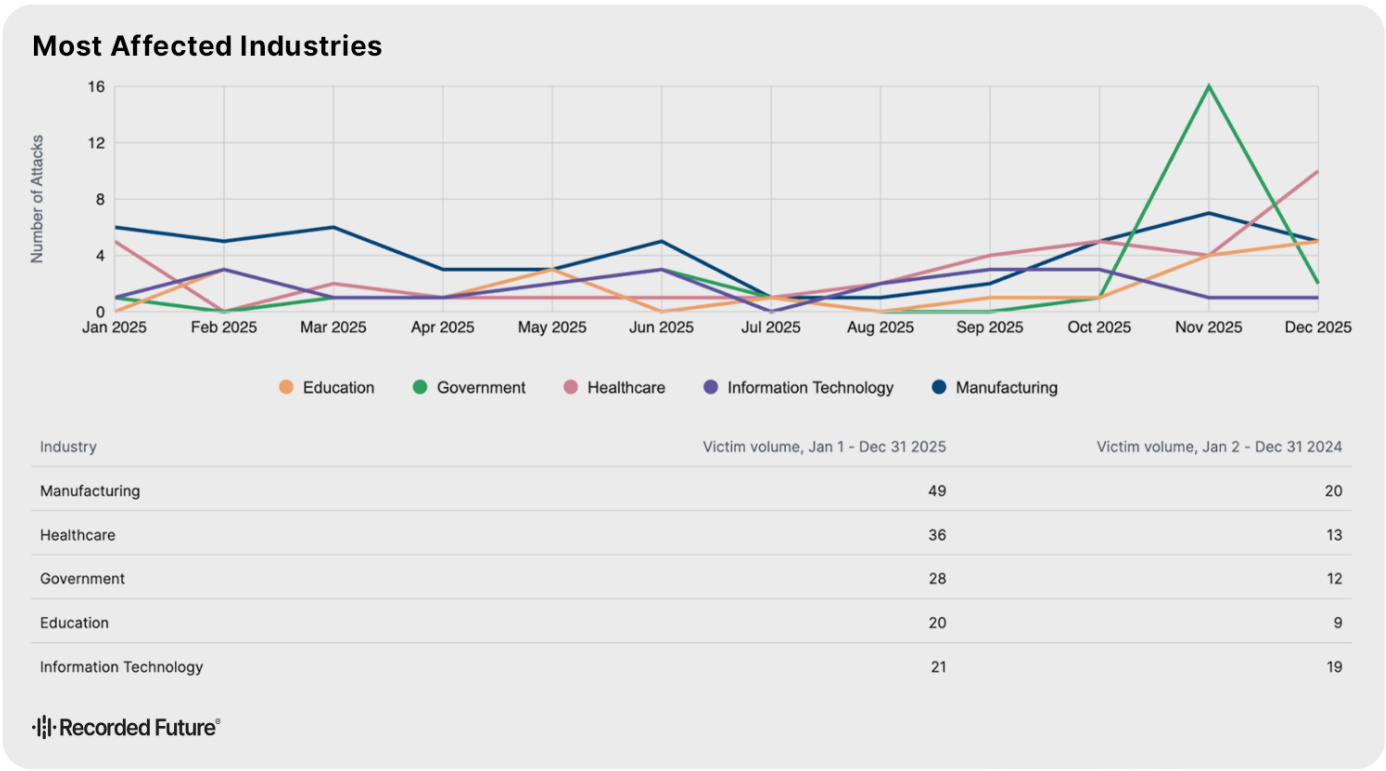


Figure 2: *Global Ransomware Landscape Dashboard view of attack metrics for the top five ransomware groups impacting LAC in 2025 (Source: Recorded Future)*



Industry	Victim volume, Jan 1 - Dec 31 2025	Victim volume, Jan 2 - Dec 31 2024
Manufacturing	49	20
Healthcare	36	13
Government	28	12
Education	20	9
Information Technology	21	19

Figure 3: *Global Ransomware Landscape Dashboard view of attack metrics for the top five most impacted industries in LAC in 2025 (Source: Recorded Future)*

Insikt Group observed an increase in ransomware activity across all major industries in LAC compared to the prior year. Insikt Group specifically examined ransomware attacks against financial, government, and healthcare entities across the LAC region and identified the following: 16 attacks targeting the finance sector, 28 attacks targeting the government sector, and 36 attacks targeting the healthcare sector. **Appendix C** highlights a sample of these ransomware attacks.

Regarding LAC countries, the top five countries most impacted by ransomware in the LAC region in 2025 were Brazil (128 attacks), Mexico (78 attacks), Argentina (63 attacks), Colombia (51 attacks), and Peru (27 attacks). These countries are among the largest economies in the region, which may lead to downstream spillover effects for enterprises that conduct business directly with them or with neighboring countries. Insikt Group found that the majority of ransomware groups leverage double extortion. This extortion technique involves encrypting a victim's data, exfiltrating the data, and then threatening to publicly leak the data on the ransomware group's name-and-shame blog if a ransom is not paid. Recorded Future assesses countries by network intrusion and ransomware targeting risk every quarter to provide awareness and help organizations assess risk exposure. Takeaways from the top five impacted countries based on metrics and analysis from Recorded Future include:

- Brazil's network intrusion risk score increased from Medium to Very High, and Brazil's ransomware targeting risk score remained Medium by the end of 2025. Brazil was the most targeted country in LAC and among the top ten countries worldwide impacted by ransomware in 2025, with a total of 130 victims.
- Mexico's network intrusion risk score increased from Very Low to Low, and Mexico's ransomware targeting risk score increased from Low to Medium at the end of 2025. Notably, data was leaked relating to a Mexican government entity on the dark web name-and-shame extortion website, Tekir Apt Data Leak Site.
- Argentina's network intrusion risk score increased from Very Low to Low, and Argentina's ransomware targeting risk score increased from Low to Medium at the end of 2025. Insikt Group observed that Argentina was targeted by a new rust-based ransomware "RALord".
- Colombia's network intrusion risk score increased from Low to High, and Colombia's ransomware targeting risk score remained low with no observed changes at the end of 2025. Colombia's financial sector was impacted by the ransomware group Crypto24, which posted victims' names on its blog.
- Peru's network intrusion risk score increased from Very Low to Low, and Peru's ransomware targeting risk score was low with no observed changes at the end of 2025. A pharmaceutical company headquartered in Peru was named as a victim on the Dire Wolf Blog.

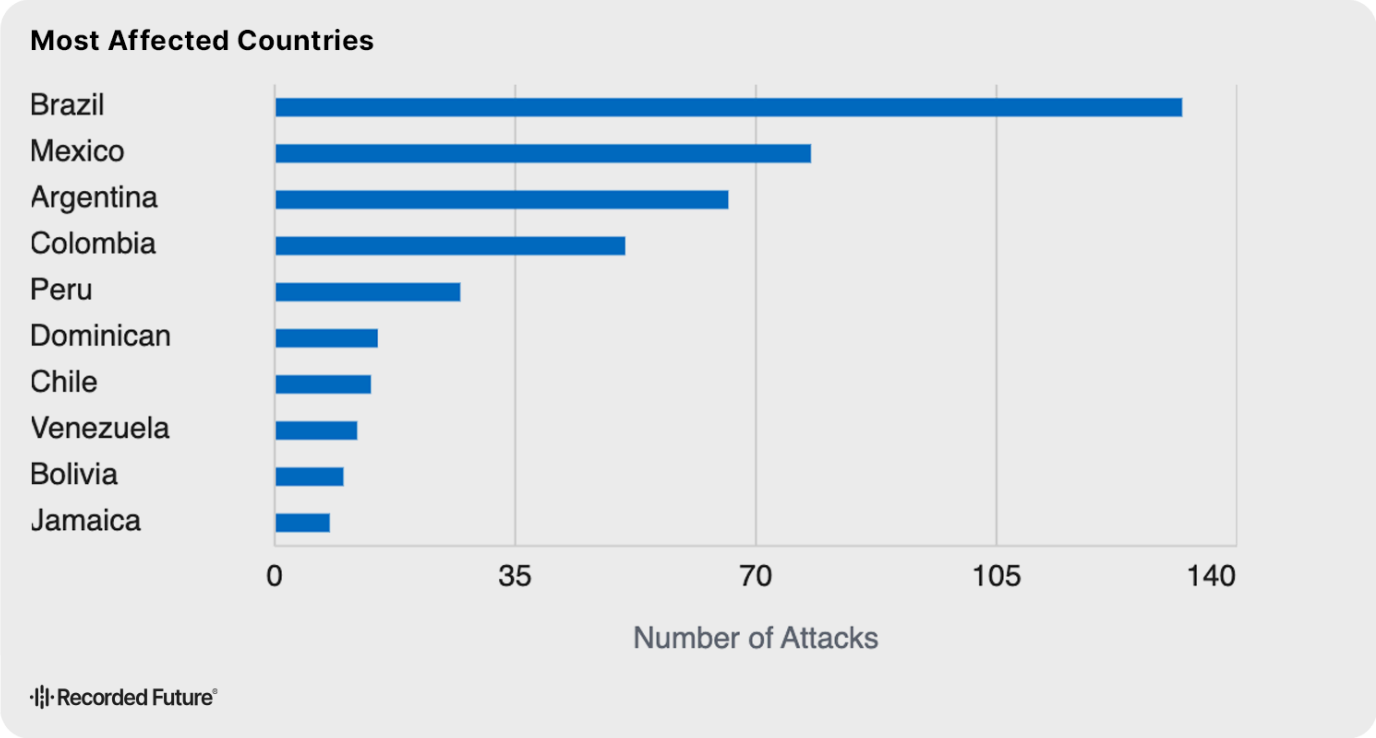


Figure 4: *Global Ransomware Landscape Dashboard view of the most affected countries in LAC in 2025 (Source: Recorded Future)*

Banking Trojans

According to the Global System for Mobile Communications Association (GSMA), in 2024, approximately 64% of the LAC population used mobile internet; it is projected that this will increase to nearly three-quarters by 2030. Increasing internet penetration and high cell phone subscription rates in LAC signify a rising reliance on mobile devices, likely making them more appealing targets for threat actors. Android remains the predominant operating system (OS) of mobile devices in South America with an 84.59% market share. Android devices may support more sideloaded applications (links and Android application packages [APKs] from social media or third-party stores) than Apple iOS, which typically has tighter ecosystem controls, and Android users may be running older OS versions, thereby making Android devices attractive targets for cybercriminals. The Android ecosystem grants developers more freedom to list apps within the Google Play Store, and the vetting and verification process is less stringent, allowing malicious APK domain mirrors to go undetected. In LAC, users may rely on mobile phones as their primary or only computing device, making them desirable initial access points for threat actors to deploy Android-based malware. According to the World Bank's Global Findex 2025 report, 37% of adults in the LAC region had a mobile money account as of 2024. Mobile banking, digital wallets, and QR payments are commonplace in the area. Based on the World Bank's findings, Insikt Group assesses that persistent mobile banking malware targeting LAC is likely driven by rapid digital banking integration that has outpaced security controls and the expansion of MaaS ecosystems. Sophisticated localized social engineering attacks and disproportionate regional enforcement capacity are further accelerating this trend within LAC's ever-evolving mobile financial landscape.

Insikt Group research reflected an increase in banking trojans targeting the WhatsApp platform in 2025. Brazilian authorities have, in recent years, focused their attention on disrupting banking trojans. A significant amount of crimeware in LAC consists of mobile banking trojans, though similar in many ways, they are not a monolith and differ in unique ways. Insikt Group analysis from 2025 reflects that, despite some law enforcement disruptions, banking trojans are still a prominent issue in the LAC region and will likely continue to be in 2026. **Appendix D** highlights the most active banking trojans across the LAC region in 2025.

Infostealers

Infostealers pose a persistent threat worldwide, and the LAC region is no exception. Insikt Group analyzed a small sample of the domains belonging to the top organizations (based on revenue) in the healthcare, government, and financial sectors across the top five largest economies in LAC. Analysis showed that the most prominent infostealer threats observed in 2025 were LummaC2, Vidar, Rhadamanthys, RedLine, and Nexus. This is despite multiple law enforcement operations under Operation Endgame conducting takedowns impacting Rhadamanthys and LummaC2.

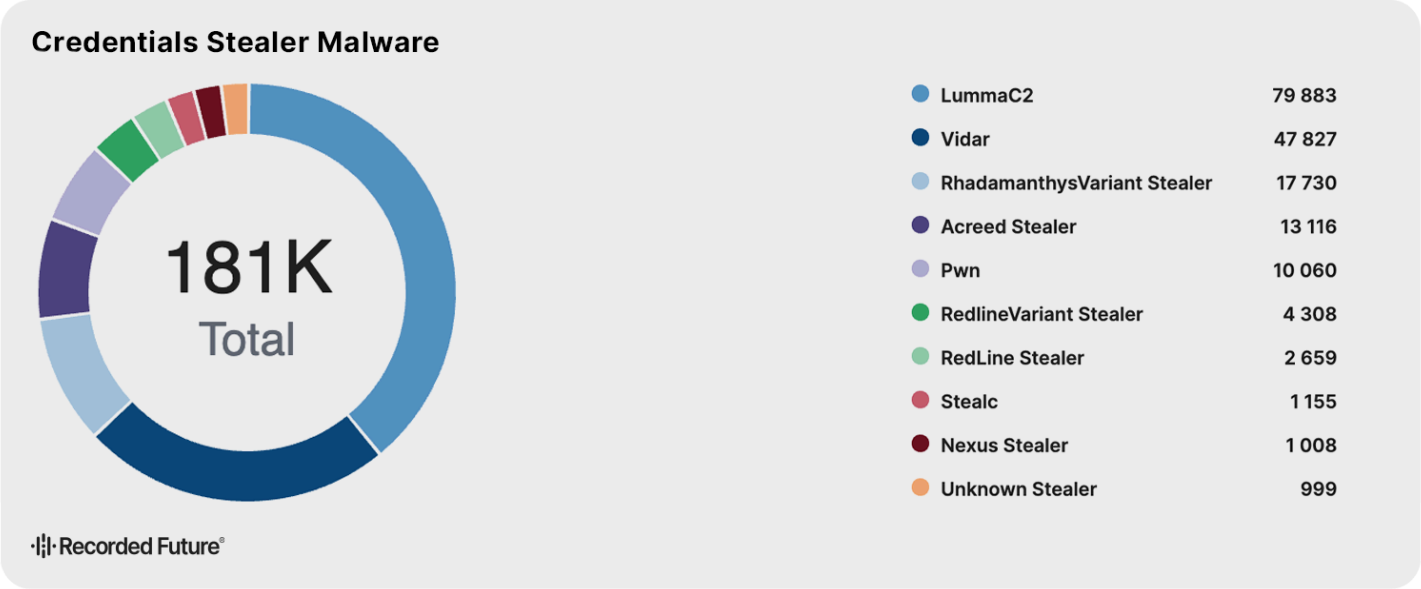


Figure 5: *Infostealers infection trends in 2025 for the domains belonging to the top organizations (based on revenue) in the healthcare, government, and financial sectors for countries with the top five largest economies in LAC (Source: Recorded Future data)*

LummaC2 was undoubtedly the most active infostealer targeting entities in the LAC region despite being targeted by law enforcement. LummaC2 has been discussed in several news sources and Telegram chatter as targeting users in Argentina, Paraguay, and Mexico. Cybercriminals deploy LummaC2 to obtain victim credentials to carry out financial fraud and cryptocurrency theft. Insikt Group conducted research into LummaC2 affiliates and identified a likely Mexico-based threat actor operating under multiple aliases linked to Lumma build ID “re0gvc”. In mid-2025, law enforcement took measures

to disrupt LummaC2; the operation effectively led to the takedown of approximately 2,300 malicious domains integral to LummaC2's infrastructure, Lumma's central command, and associated criminal marketplaces. Shortly after this operation, it appears LummaC2 still had infected victims in several countries, including Brazil and Colombia, likely because sinkholing requires some time to have a noticeable effect as it redirects traffic but does not automatically clean infected machines. More complete remediation would require patching and malware removal on affected systems, which is challenging to implement at scale when infected devices are spread across the world. However, Insikt Group observed a significant decrease in credentials exposed by LummaC2 in the second half of 2025, likely due to the success of the joint Microsoft and law enforcement operation, as well as the main threat actor being banned from Exploit.

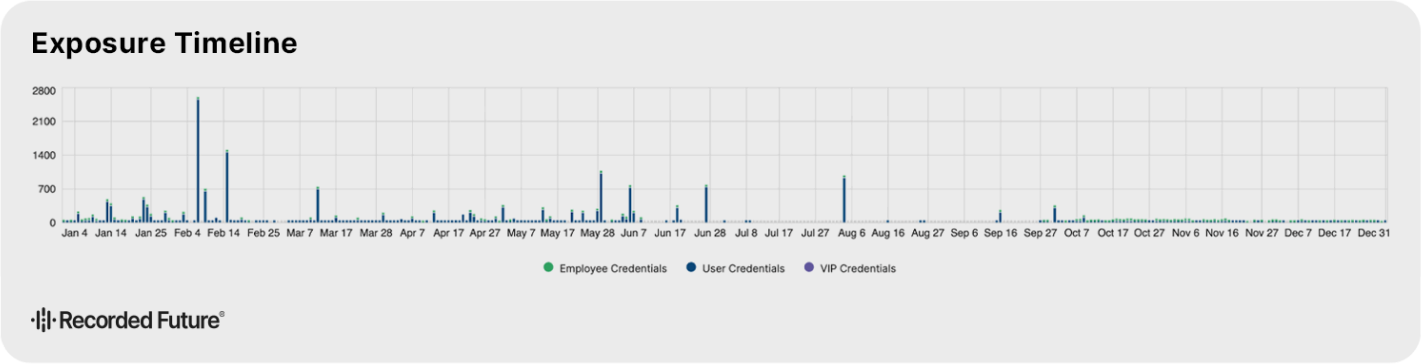


Figure 6: *LummaC2 infection trends in 2025 for the domains belonging to the top organizations (based on revenue) in the healthcare, government, and financial sectors for countries with the top five largest economies in LAC (Source: Recorded Future data)*

In the wake of the LummaC2 operation, Recorded Future detected an increase in Vidar infections during the latter half of 2025. This increase highlights threat actors' ability to migrate between infostealers to facilitate their criminality despite disruptions.

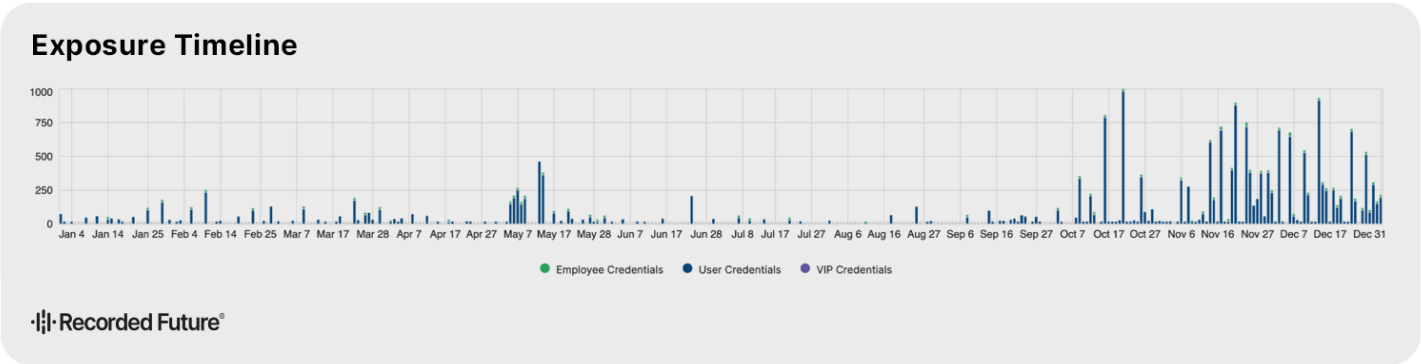


Figure 7: *Vidar Infection trends in 2025 for the domains belonging to the top organizations (based on revenue) in the healthcare, government, and financial sectors for countries with the top five largest economies in LAC (Source: Recorded Future data)*

Botnets

Botnet activity has grown steadily in the LAC region, enabling financial fraud, spam distribution, credential harvesting, initial access for ransomware and large-scale DDoS attacks targeting financial and government institutions. Botnets remained a priority for international law enforcement in 2025. For example, the ongoing Operation Endgame aims to hinder threat actors' remote-control capabilities by dismantling ransomware and other malware infrastructure. Emerging in late 2025, Kimwolf, also known as AISURU, is a botnet that targets compromised streaming devices. News reporting and dark web chatter indicate many of the devices infected with Kimwolf are based in Brazil, India, the US, and Argentina. Additional reporting suggests a threat actor involved with the AISURU botnet is likely based in Brazil. Horabot is a malware family and type of botnet first identified in June 2023, targeting Spanish-speaking users in six LAC countries: Mexico, Guatemala, Colombia, Peru, Chile, and Argentina. Horabot uses invoice-themed phishing emails to gain initial access to victims' systems.

Payment Terminal Malware

Threat actors also continued to target payment infrastructure for financial gain. ATM malware activity has continued to rise in LAC, with some experts noting ATM malware attacks have spiked by 46% across LAC in 2025. For instance, Ploutus is a sophisticated malware family first detected in Mexico in 2013, which compromises ATMs by issuing unauthorized commands to their cash dispensing modules. In December 2025, the US Department of Justice indicted 54 individuals associated with the Venezuelan gang Tren de Aragua (TDA) for participation in a massive ATM jackpotting scheme that exploited Ploutus malware. Moreover, the POS malware MajikPOS, designed to infiltrate systems connected to POS terminals and extract magnetic stripe payment data from bank cards, remained an active threat to companies operating in Brazil.

Mitigations

- **Use Recorded Future's Global Ransomware Landscape Dashboard:** Recorded Future customers can proactively mitigate this threat by operationalizing the Recorded Future Global Ransomware Landscape Dashboard and leveraging the victimology tab to filter based on ransomware group, country, and industry of interest. Recorded Future customers can customize their own ransomware risk profile and establish alerts that align with their risk priorities.
- **Use Recorded Future's Threat and Third-Party Risk Monitoring:** Configure alerts in the Recorded Future Intelligence Cloud to track activity across Telegram channels, darkweb forums, and other platforms for proactive awareness. Use the Third-Party Intelligence module to assess risk exposure for current and future partnerships.
- **Update Legacy Systems:** Threat actors, whether opportunistic or financially motivated, or both, often seek to exploit vulnerable systems. Organizations that rely on outdated technology stacks leave themselves exposed to preventable cyber threats and attacks.

- **Engage in Public-Private Information Sharing:** To bolster regional collaboration and establish standardized best practices, coordinate with law enforcement, and create intelligence-sharing channels to enhance investigations and decrease incident response times.
- **Generate Awareness through Education:** Advocating for digital literacy through university partnerships and scholarship in the LAC region will encourage good cyber hygiene and prepare for a stronger, more competent workforce. Enterprises can implement mandatory cybersecurity training during new hire onboarding and establish routine drills to ensure protocols are followed.

Outlook

Insikt Group has highlighted the most salient cybercriminal trends and methods observed throughout the LAC region in 2025. Threat actors conducted phishing and credential theft to gain and sell initial access to LAC organizations while often relying on dark web forums and end-to-end encrypted messaging platforms to communicate and monetize compromised data and access methods. Cybercriminals carried out elevated ransomware attacks against the healthcare, government, finance, and other critical sectors. Banking trojan and infostealer activity persisted throughout LAC despite law enforcement disruption attempts. Cybercriminals have proven to be adaptive and resilient, often capitalizing on immature or emerging businesses that lack the skills, tools, and personnel to prevent attacks. Small and medium-sized enterprises (SMEs) constitute over 95% of all businesses in LAC. SMEs are desirable targets for cybercriminals because they typically have limited resources and expertise, lack robust infrastructure, and have a high overreliance on third-party platforms. Insikt Group trend analysis supports these findings.

Absent regional harmonization of cybersecurity policies and best practices, LAC countries will likely continue to use fragmented incident response approaches, complicating cross-border cooperation and collaboration. For effective and sustainable protection of systems and information against cyber threats, LAC countries should focus on working together to establish standardized risk assessments and reporting mechanisms, protocols for information sharing to bolster timely remediation, and implement proactive “secure by design” principles. Possible approaches to accomplishing this may include increased investment in workforce development, participation in public-private partnerships, and the establishment of centralized cybersecurity management systems. Despite the lack of prominent Spanish- and Portuguese-language forums, it is likely that threat actors will continue to leverage traditional platforms and methods similar to those used by the English- and Russian-speaking cybercriminal underground. Based on current and historical data, we anticipate these trends will continue, and LAC will likely remain a popular target for ransomware groups and a hotspot for mobile malware in 2026.

Appendix A: Sample Listing of Posts Targeting Entities in LAC Countries on Dark Web and Special Access Forums

Alleged Access or Leak	Source	LAC Country and Sector Impacted
Access to a Brazilian banking entity	XSS Forum	Brazil/Finance
VPN access to a Colombian bank	Exploit Forum	Colombia/Finance
Access to a leaked government database	DarkForums	Mexico/Government
Database access to the official government portal	Exploit Forum	Argentina/Government
Web shell access with root privileges for a healthcare provider	XSS Forum	Chile/Healthcare
Global VPN access to a healthcare network	RehubcomPro Forum	Brazil/Healthcare

(Source: Recorded Future)

Appendix B: Sample Metrics of the Top Five Ransomware Groups Impacting LAC in 2025

Group Name	Total Attacks (All Sectors)	Healthcare	Manufacturing	Government	IT	Education
Qilin (Agenda)	54	4	6	0	2	2
LockBit Gang (BITWISE SPIDER, DEV-0396, Flighty Scorpius)	29	2	3	1	1	4
Safepay	27	2	4	0	0	0
The Gentlemen	22	3	1	0	0	1
Kazu	21	0	0	17	0	2

(Source: Recorded Future)

Appendix C: Sample Data of Ransomware Incidents Impacting Healthcare, Government, and Financial Sectors in LAC Countries in 2025

Ransomware Group	Country	Sector
Safepay	Argentina	Healthcare
The Gentlemen	Brazil	Healthcare
Kazu	Colombia	Government
Kazu	Mexico	Government
Qilin (Agenda)	Ecuador	Finance
Qilin (Agenda)	Argentina	Finance

(Source: Recorded Future)

Appendix D: Trends from the Most Active Banking Trojans in LAC in 2025

Banking Trojan	Attributes	Activity in 2026
Grandoreiro	Spreads through phishing emails with seemingly legitimate documents, such as PDFs. Once on a device, it performs anti-sandbox checks, logs keystrokes, and communicates with C2 servers to exfiltrate sensitive banking credentials	New variants emerged with advanced evasion techniques, rendering them more effective at bypassing modern security measures
Crocodilus	Employs sophisticated tactics such as remote control capabilities, keylogging, overlay attacks to capture user credentials, and the ability to harvest cryptocurrency wallet seed phrases	Expanded operational reach by targeting users in Poland, Spain, Brazil, Argentina, Indonesia, the US, and India
Mispadu (URSA)	Employs sophisticated infection methods, including spam emails containing malicious PDFs that trigger multi-stage download processes that deploy the Mispadu payload after performing anti-sandbox and anti-virtual machine checks	Insikt Group created a YARA rule to detect Mispadu after analysis indicated the trojan had targeted several LAC banks
Astaroth (Guildma)	Distribution methods include spearphishing attacks and the use of compromised cloud infrastructure for hosting malicious content. Insikt Group conducted technical static analysis and detection using sigma rules	Resurfaced with a multi-stage campaign, “STAC3150”, involving WhatsApp session hijacking, credential theft, and persistence on compromised systems
SORVEPOTEL	Targeted Brazil in several campaigns; Insikt Group assesses that at least some SORVEPOTEL operators are likely Portuguese-speaking, based on language artifacts in the panels analyzed and consistent targeting of Brazilian victims; analysis of a notable campaign dubbed “Water Saci” indicates WhatsApp Web was used for distribution	Analysis of the new infrastructure tied to the SORVEPOTEL loader demonstrates that it has distributed Coyote and Maverick

Banking Trojan	Attributes	Activity in 2026
Casabaneiro ("Mekotio" and "Metamorfo")	Primarily targets financial institutions in LAC, leverages phishing emails that typically contain malicious URLs, which lead to ZIP archives or ISO files with payloads that execute PowerShell scripts designed for obfuscation and evading detection	Water Saci campaign targeting Brazilian financial platforms via WhatsApp propagation linked to Casbaneiro malware family
BBTok	Distribution methods that trigger infections via LNK files and exhibit advanced capabilities for credential theft and data exfiltration, leveraging techniques such as dynamic-link library (DLL) embedding within downloaded files and the use of legitimate Windows utility commands for evasion	A new tactic emerged where the primary delivery method was WhatsApp
Coyote	Primarily targets Brazilian users, capable of executing keylogging, capturing screenshots, and displaying phishing overlays to steal sensitive credentials; Coyote's infrastructure is dynamic and hosted on various platforms, indicating robust evasion techniques by its operators	Coyote remained active in 2025 and was observed in a WhatsApp-based worm campaign that used self-propagating messages containing malicious ZIP archives that further distributed the malware
Herodotus	Distributed through smishing messages that lure victims into downloading malicious APKs; Herodotus has been observed primarily targeting users in countries like Brazil and Italy	Insikt Group analyzed a sample, where Herodotus impersonated a security application named "Modulo Seguranca Stone" in a campaign in Brazil

(Source: Recorded Future)

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for customers, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest intelligence company. The Recorded Future Intelligence Operations Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining precise, AI-driven analytics with the Intelligence Graph® populated by specialized threat data, Recorded Future enables cyber teams to see the complete picture, act with confidence, and get ahead of threats that matter before they impact your business. Headquartered in Boston with offices around the world, Recorded Future works with more than 1,900 businesses and government organizations across 80 countries.

Learn more at recordedfuture.com