INTEL471

REPORT

LATIN AMERICA'S CYBER THREAT LANDSCAPE: RAPID DIGITAL GROWTH AND RISING RISK

TLP:CLEAR

Table of Contents

Key Findings

The following is a redacted version of a report released to Intel 471 customers on Jan. 01 2026. For full access, including links to related reporting on Verity471, Intel 471's cyber intelligence platform, and sensitive source-derived details, contact us at sales@intel471.com.

- According to an assessment conducted by the Organization of American States (OAS), states in Latin America have made measurable progress in cybersecurity maturity since 2020 but a significant variability remains across nations, particularly in areas such as software assurance, protection of critical infrastructure, innovation, market development and cyber insurance adoption.
- Common threats impacting Latin America relate to ransomware and extortion, compromised data vendors, compromised access vendors, hacktivism, financial fraud, banking trojans and phishing.
- We reported over 450 ransomware breach events pertaining to Latin America from January 2025 to December 2025, an increase of more than 78% compared to 2024.
- From January 2025 to December 2025, we observed over 200 initial access brokers (IABs) target entities in Latin America, with Brazil being the most targeted country in the region.
- Advanced persistent threat (APT) clusters impacting the region include those possibly operating from China, North Korea and even clusters within Latin America itself.
- We observed at least 119 hacktivist attacks across 15 countries of Latin America in 2025, with Brazil being the most targeted country.

Introduction

Figure 1: The image depicts key cyber incidents that impacted Latin America in 2025.

Latin America experienced an increasingly hostile cyber threat landscape in 2025 shaped by the convergence of well-resourced financially motivated actors, strategically driven state-sponsored adversaries and the usual fraud operators that constantly are seeking flaws in systems and business processes. Rapid digitalization across the region, often advancing faster than the adoption of mature security controls and governance frameworks, has expanded the attack surface and increased risk to governments, organizations and the population.

Cyber incidents observed throughout the year spanned a broad spectrum, ranging from large-scale financial fraud and banking trojan malware campaigns to ransomware operations with direct impact on business continuity, operational resilience and public trust.

Despite growing awareness of cyber risk, structural challenges persist across the region, including limited cross-sector collaboration, shortages of skilled cybersecurity professionals and inconsistent budget allocation. These constraints continue to impede the development of sustainable cybersecurity maturity. As governments and critical sectors further integrate digital services and infrastructure, cybersecurity has transitioned from a technical concern to a strategic priority for Latin America.

For security leaders and CTI teams, this report provides an overview of the cybersecurity governance models states across the region have adopted, as well as an overview of the adversaries and capabilities shaping the regional threat landscape. It is designed to help align detection and response planning to the most prevalent threats and inform risk decisions for those enterprises with operational or supply-chain exposure across the region.

Cybersecurity Maturity

In 2025, the OAS published the results of a comprehensive cybersecurity maturity assessment covering countries across Latin America. The assessment applied the Cybersecurity Capacity Maturity Model for Nations (CMM) to evaluate national capabilities across five core domains: policy and strategy, cyber culture and society, education and skills, legal and regulatory frameworks, and technology and standards. These domains examine factors such as the existence of national cybersecurity strategies, critical infrastructure protection measures, incident reporting mechanisms, workforce development, public awareness, legal enforcement capacity and alignment with international standards, among multiple others. Based on performance across these areas, countries are classified into one of five maturity stages: startup, formative, established, strategic or dynamic.

The image below compares assessments conducted in 2020 and 2025 and indicates that although only a limited number of countries progressed beyond the second maturity stage, a significant number demonstrated measurable improvements.[1]

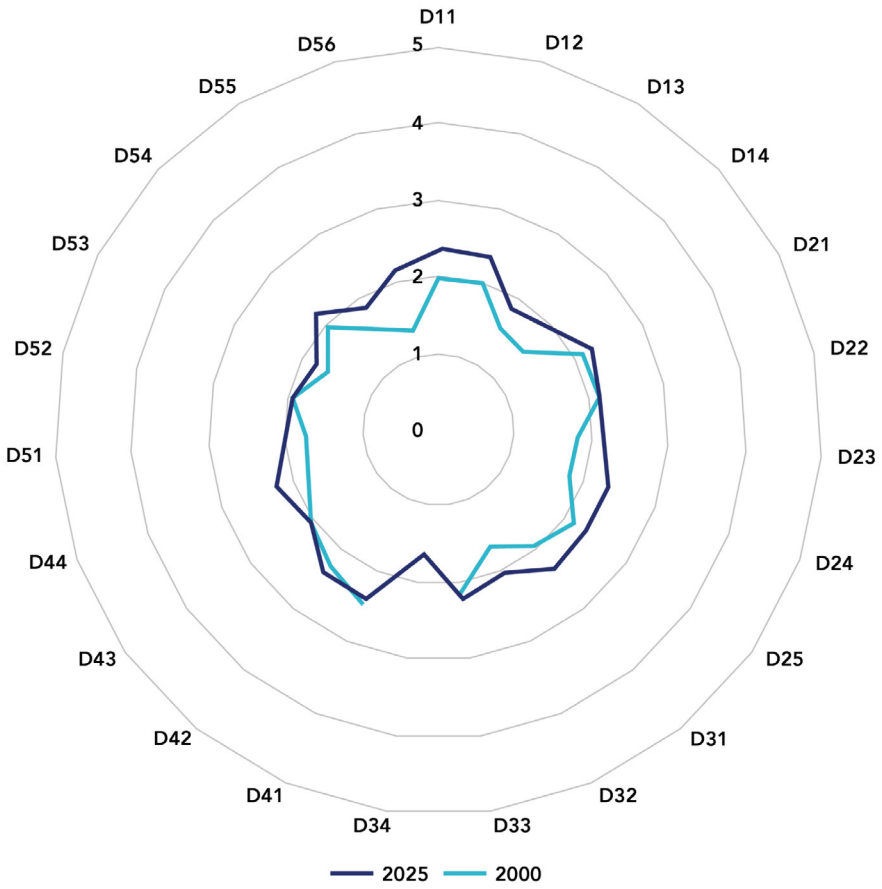

Figure 2: The image depicts the average cybersecurity maturity levels for the 30 OAS member states assessed in 2020 and 2025. The scale from 1 to 5 corresponds to the five maturity stages defined in the CMM. Each assessed element is represented by its corresponding numerical CMM code prefixed with the letter "D" rather than by its full descriptive title.

While the region has made measurable progress in cybersecurity maturity since 2020, significant variability remains among member states, particularly in areas such as software assurance, protection of critical infrastructure, innovation, market development and cyber insurance adoption.

National Cybersecurity Policy

The national privacy, security and data governance of each state in Latin America reflects the dynamics of their political doctrines, economic factors and geopolitical alliances. A study from the German Institute for Global and Area Studies (GIGA) categorizes states in the region into four primary models of cybersecurity policy.

Model	Characteristics	Key aspects	Example countries
Security-oriented	The state prioritizes the prevention of cyberattacks in its internet governance strategy while avoiding control of digital content and maintaining a relatively relaxed stance on digital privacy.	Presence of national cyber strategy (NCS) policies, national computer emergency response teams (CERTs), a dedicated cybersecurity authority and military cyber units. Aligns with the U.S. model.	Colombia, Ecuador, Paraguay and Dominican Republic.
Privacy-oriented	The state prioritizes data protection and citizen privacy through robust data protection laws and security protocols aimed at mitigating data theft and unauthorized access risks.	Presence of comprehensive data protection and digital privacy laws, broadly aligned with the European Union's (EU's) General Data Protection Regulation (GDPR), complemented by a dedicated national authority responsible for overseeing user data protection requirements. Aligns with the European model.	Costa Rica and Panama.
Control-oriented	The state emphasizes government control over data and cyberspace, including content regulation and censorship aligned with national objectives.	Presence of censorship affecting political content and social media, systematic monitoring and targeting of journalists, evidence of government surveillance of citizens in cyberspace and restrictions on the use of virtual private networks (VPNs). Aligns with the Chinese model.	Cuba, Nicaragua and Venezuela.

Model	Characteristics	Key aspects	Example countries
Hybrid security-private-oriented	The state follows a hybrid governance model that combines robust data and privacy protection frameworks, cybersecurity resilience and selective government control over digital content in support of national security and strategic objectives.	Presence of data protection and digital privacy laws, national data governance authorities, NCS policies, national CERTs, social media content monitoring and content regulation.	Argentina, Brazil, Chile, Mexico and Uruguay.

While security, privacy and control-oriented models have well-defined characteristics, hybrid cybersecurity models are expected to become more prevalent across nations. For example, the EU may be simultaneously categorized as both security and privacy-oriented. Similar trends are observed in Latin American countries where security considerations are increasingly combined with an emphasis on protecting user privacy and data governance.[2]

National Cybersecurity Strategies

Latin American countries exhibit uneven levels of maturity and differing priorities in their national cybersecurity strategies. In the absence of unified regional guidelines, states across the region have increasingly pursued the development of independent national contingency and cybersecurity frameworks to address evolving cyber threats. Brazil, Colombia, Chile and Uruguay currently maintain the most advanced strategies, while Argentina and Peru have also made notable progress in recent years.[3]

Across the region, national strategies commonly prioritize the protection of critical infrastructure, the establishment of data protection and cybersecurity legislation, the mitigation of cybercrime and enhanced public-private cooperation. This collaboration often materializes through joint incident response mechanisms, information sharing initiatives and public cybersecurity awareness campaigns. Examples of national cybersecurity strategies include:

Country	Cybersecurity strategy	Objectives
Argentina	Second National Cybersecurity Strategy[4]	• Protect critical infrastructure. • Strengthen the country's capacity to detect, prevent and investigate cybercrimes. • Promote digital sovereignty and the responsible use of emerging technologies. • Foster transparency and accountability in government and the digital space.

Country	Cybersecurity strategy	Objectives
Brazil	Estratégia Nacional de Segurança Cibernética (E-Ciber)[5]	• Enhance incident response and recovery mechanisms to detect, respond to and mitigate cyber threats. • Establish a centralized governance model at the national level through the creation of a national cybersecurity system. • Improve the legal framework on cybersecurity by reviewing and updating existing regulations, addressing new topics and developing new instruments. • Strengthen collaboration with international partners to address global cybersecurity challenges. • Enhance coordination between public and private sectors, including academic institutions and society, through continuous and proactive monitoring of cyber threats and attacks. • Promote cybersecurity awareness across society and invest in education and training programs.
Chile	Política Nacional de Ciberseguridad (PNCS) 2023-2028[6]	• Strengthen digital infrastructure security and resilience. • Protect citizens' fundamental rights, including personal data and privacy. • Promote cybersecurity education and the adoption of best practices among all citizens. • Facilitate coordination and collaboration between national institutions and their international counterparts. • Encourage research and development (R&D) and industrial growth by building local capacities to stimulate innovation in the cybersecurity sector.
Colombia	National Cyber Security and Cyber Defense Strategy[7]	• Implement the appropriate institutions. • Promote specialized training programs for civil servants. • Strengthen legislation and international cooperation.

Country	Cybersecurity strategy	Objectives
Peru	Estrategia Nacional de Ciberseguridad del Perú (ESNACIB) 2026-2028[8]	• Strengthen the state's capabilities to combat cybersecurity threats. • Adopt a holistic approach to safeguard digital information and promote digital trust. • Align Peru's cybersecurity standards with international best practices. • Enhance national protection and response capabilities against cyberattacks.

Cyber Underground Landscape

Overview

The cyber threat landscape in Latin America intensified significantly in 2025, driven by the combined activity of financially motivated and state-sponsored actors. The region has recorded the fastest global growth in disclosed cyber incidents, with reported activity increasing at an average annual rate of about 25% over the past decade. This trend accelerated sharply in early 2025, when the first quarter alone registered a 108% year-over-year increase, indicating a critical inflection point in the regional threat environment.

Organizations in Latin America face an average of 2,640 cyberattacks per week, which is 35% above the global average of 1,955, with associated annual costs exceeding US $90 million. This escalation is largely attributed to rapid digitalization, persistent security gaps in cloud environments and the increasing use of artificial intelligence (AI) to scale, automate and enhance cyberattacks.[9,10,11,12]

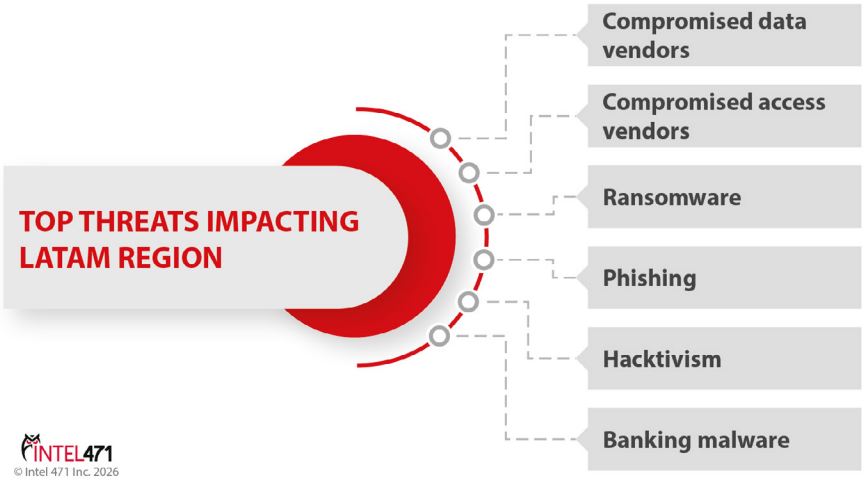

Figure 3: The image depicts the most common threats impacting Latin America.

Incidents in Focus

Below we provide an overview of significant cyberattacks and data breaches that affected countries across Latin America during 2025.

- In January 2025, the personal and financial data of both officers and civilian staff of an Argentina-based airport security force was reportedly compromised following a cyberattack. The breach occurred via a vulnerability in the systems of the institution responsible for processing the organization's payroll. Cybercriminals exploited this access to deduct small sums from employees' salaries, with amounts ranging from US $100 to US $245.[13]
- In June 2025, the **Brigada Cyber PMC** data extortion group claimed to have stolen more than 7 million records containing personally identifiable information (PII) of Paraguayan citizens from three Paraguayan government systems. The group criticized the country's leadership for corruption and neglecting citizens' data protection and demanded a ransom equivalent to about US $7.4 million — US $1 for each of the country's citizens.[14,15]

The Brigada Cyber PMC group demanded a ransom equivalent to about US $7.4 million

- In June 2025, Brazil suffered the largest cyberattack on the country's financial system. The Central Bank of Brazil revealed the Brazil-based financial technology provider C&M Software, which connects the country's financial institutions to the Central Bank's Pix instant payment system, was compromised. According to local authorities, the incident stemmed from insider access credentials and resulted in the diversion of about 800 million Brazilian reals (about US $148 million) from accounts of eight financial institutions through the Pix system. In November 2025, the DragonForce ransomware-as-a-service (RaaS) affiliate program operator or operators claimed to compromise C&M Software in a different cyberattack.[16]
- In September 2025, the operator or operators running the Inc. RaaS affiliate program claimed to compromise a Panama-based government entity. The gang allegedly stole more than 1.5 TB of data that included budgeting details, emails and financial data. The entity confirmed the breach — disclosing that one of its computers may have been compromised in a cyberattack — and asserted the incident was contained and did not impact central systems vital for its operations.[17,18]
- In December 2025, a Venezuelan state-owned oil company revealed its systems were subjected to a cyberattack it believed was "orchestrated by the U.S. and domestic conspirators" for the purpose of destroying Venezuela's right to sovereign energy development through "force and piracy." Although the company's statement downplayed the impact, there were conflicting media reports as to the level of disruption to scheduled loadings at the country's main José oil terminal. Details about the true severity of the attack against the company's digital systems remained unknown at the time of this report.[19]

Extortion, Ransomware

The extortion and ransomware landscape remains a critical threat to both private organizations and government entities across Latin America. Intel 471 observed cyberattacks in the region increased from over 250 in 2024 to over 450 in 2025, while the number of ransomware variants rose from 48 to 79 with the most impactful gangs being the **Qilin**, **The Gentlemen**, **SafePay**, **Akira** and **Inc**. groups. The most targeted sectors in descending order were consumer and industrial products; energy, resources and agriculture; and professional services and consulting, while the most impacted industries were retail, wholesale and distribution; agriculture and food and beverage production; and health care providers and services. Entities based in Brazil accounted for about 30% of victims, followed by Mexico at about 14% and Argentina at about 13%.

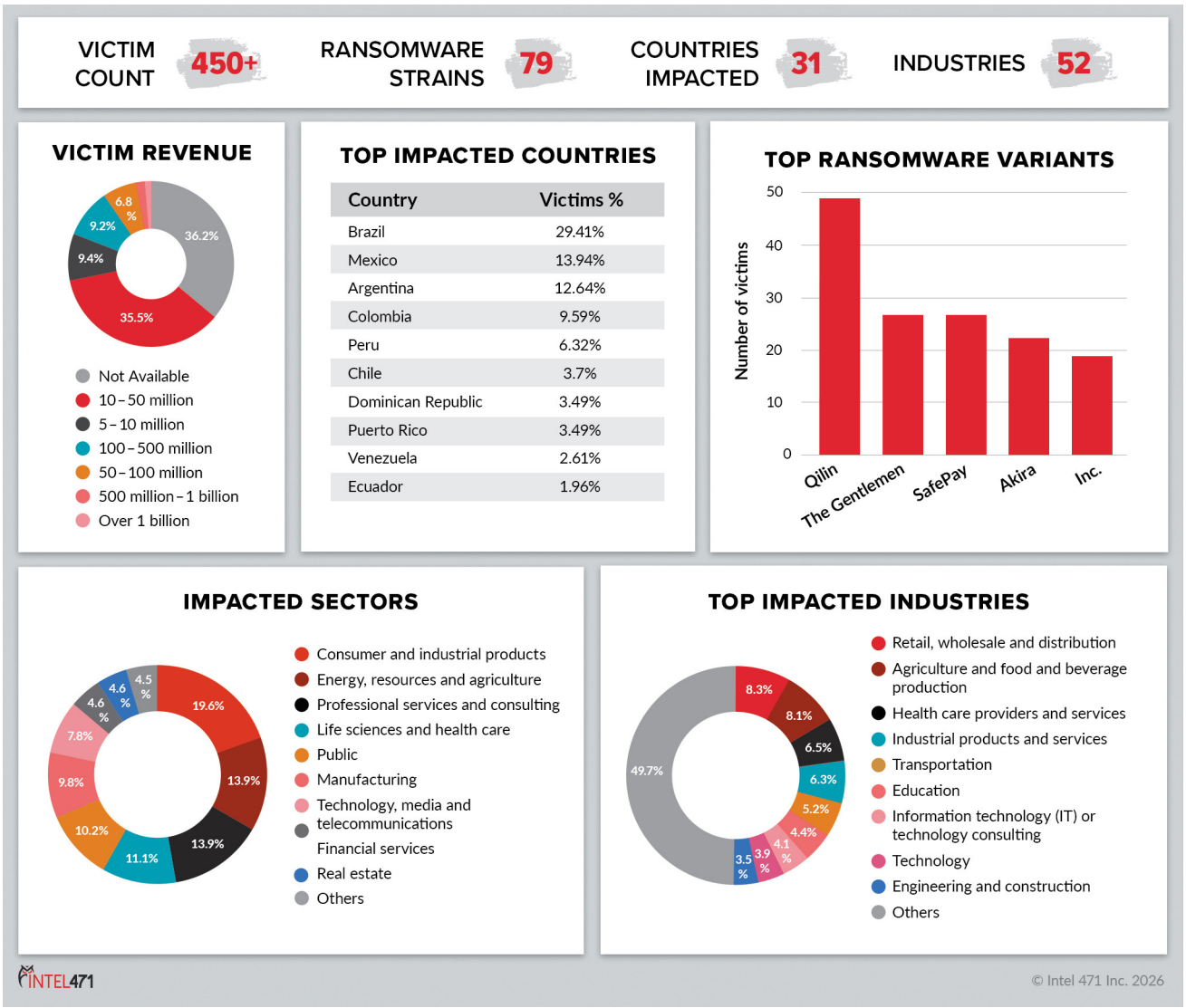

Figure 4: The graphic depicts a breakdown of Latin America-based extortion victims from January 2025 through December 2025.

Initial Access Brokers

Access vendors play a crucial role in today's cybercrime ecosystem, enabling intrusions to a vast spectrum of adversaries through various methods and technologies. We observed over 200 instances of access offers impacting 17 countries in Latin America from January 2025 to December 2025. The most targeted country was Brazil with over 70 victims, followed by Mexico with over 30 and Argentina with over 20. The most impacted sectors in descending order were public; energy, resources and agriculture; and technology, media and telecommunications, while the most impacted industries were national government, agriculture and food and beverage production and education. The top three most impactful IABs during the reporting period were those using the **Pirat-Networks**, ***Red** and ***Blue** handles. The most common method that access brokers leveraged to obtain access to organizations in the region was the abuse of compromised login credentials, while the most targeted technology was corporate remote access portals.

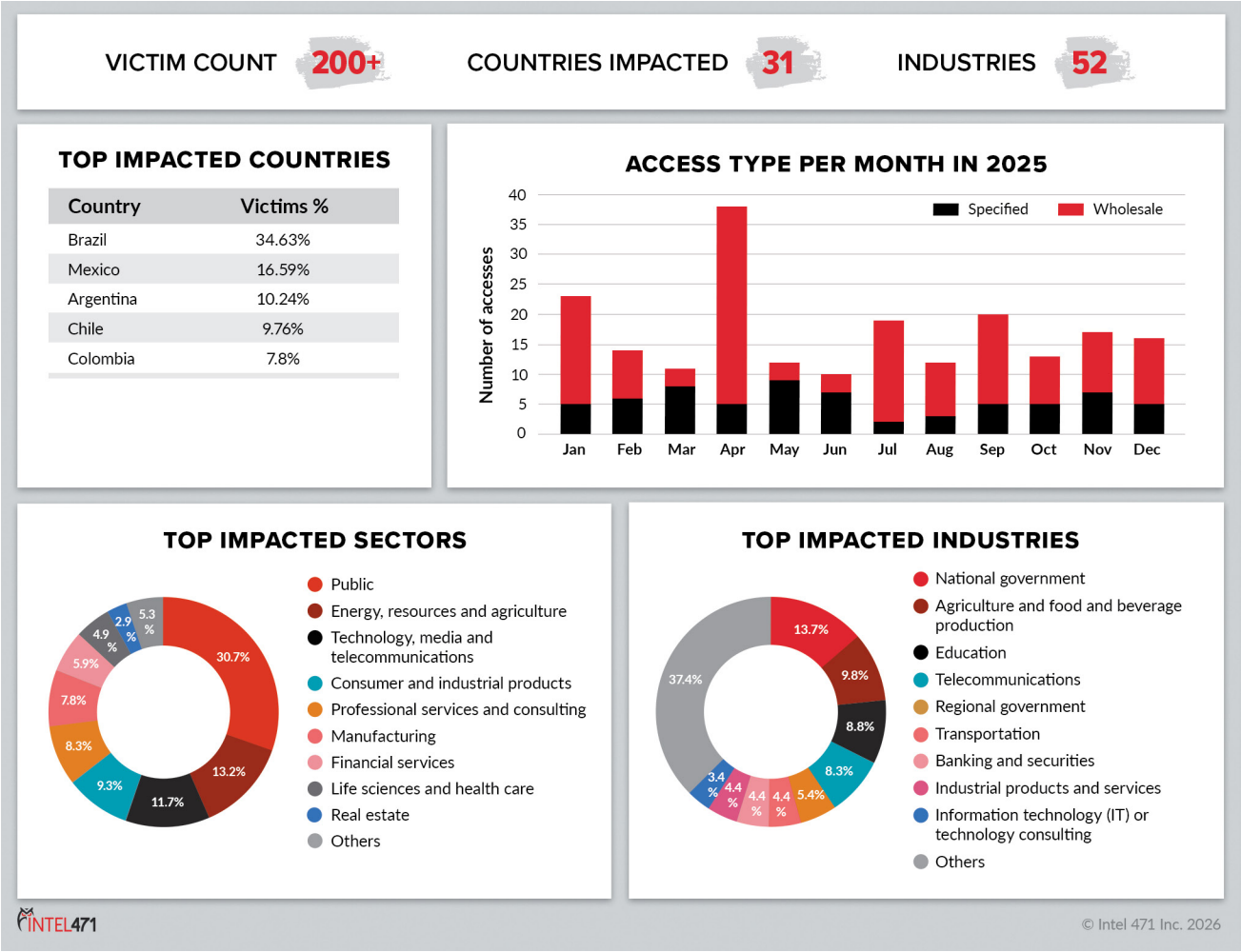

Figure 5: The graphic depicts the number of events and handles monitored and the IABs most actively impacting Latin America from January 2025 through December 2025.

Advanced Persistent Threat Clusters

APT activity reflects highly capable and well-organized adversaries — often aligned with state interests — conducting sustained, targeted cyber operations. These campaigns commonly pursue objectives such as espionage, intellectual property theft or sabotage. In Latin America, APT operations have intensified amid geopolitical tensions, accelerated digital transformation and the region's growing strategic relevance within the China-U.S. rivalry.[20] Cyber operations linked to China, which cybersecurity experts widely view as the leading state actor using these attacks to further economic and diplomatic goals, have significantly increased in frequency and sophistication across Latin America.

China-nexus adversaries such as **Aquatic Panda** aka **Charcoal Typhoon** — associated with the i-Soon private company whose documents were leaked online — reportedly targeted military entities in Peru, undisclosed entities in Brazil and government networks and telecommunications infrastructure in the region. North Korea-nexus adversaries reportedly conducted opportunistic campaigns in the region for financial gain via the IT remote worker scheme.[21,22,23,24]

Beyond foreign state involvement, events disclosed in 2025 revealed evidence of cyber operations originating within Latin America when a cyber espionage revelation triggered a diplomatic incident between Brazil and Paraguay. News media outlets revealed the Agência Brasileira de Inteligência (ABIN) (Eng. Brazilian Intelligence Agency) targeted Paraguayan officials who were engaged in sensitive negotiations over governing financial rules and energy tariffs for the binational Itaipu hydroelectric dam between June 2022 and March 2023. In November 2025, Brazilian Foreign Minister Mauro Vieira provided a confidential report and clarifications to Paraguayan counterpart Rubén Ramírez Lezcano. The incident highlighted deeper issues in Brazil-Paraguay relations and raised concerns about democratic oversight within Brazil's intelligence community.[25]

Additionally, the **Blind Eagle** aka **APT-C-36** sophisticated threat cluster is believed to have operated from Latin America since at least 2018, engaging in both espionage and cybercriminal activity. In 2024 and 2025, the cluster conducted targeted campaigns exploiting the CVE-2024-43451 vulnerability affecting Microsoft Windows to compromise Colombian judicial and government institutions and deploy the Remcos remote access trojan (RAT).[26]

Hacktivism

Hacktivism activity in Latin America is primarily associated with ideologically motivated groups, often focused on causes such as environmental protection or anti-corruption. Hacktivism operations typically target government institutions, security forces and strategic industries.

The notable **Guacamaya** hacktivist group emerged in 2022 and ideologically stands against exploitation of natural resources, corruption, transnational corporations and external intervention in Latin America. The group targeted military and law enforcement entities as

well as companies operating in the mining and oil, gas and consumable fuels industries across Chile, Colombia, El Salvador, Mexico and Peru. The group's operations relied on a hack-and-leak strategy involving unauthorized access, data exfiltration and public disclosure through platforms such as DDoSecrets and Enlace Hacktivista.[27]

The international **SiegedSec** hacktivist group previously targeted government entities in Colombia via the #OpColombia hacktivist campaign and telecommunications companies from Mexico in 2023. The campaigns led to the leak of multiple compromised datasets from public-sector organizations and telecommunications service providers. [28,29,30,31]

Intel 471 observed at least 119 hacktivist attacks across 15 countries of Latin America in 2025, with Brazil being the most targeted country with 34 attacks. Additionally, our monitoring system detected distributed denial-of-service (DDoS) attacks on over 90 entities based in countries of Latin America. Colombia was the most targeted country with over 20 victims, followed by Venezuela and Brazil.

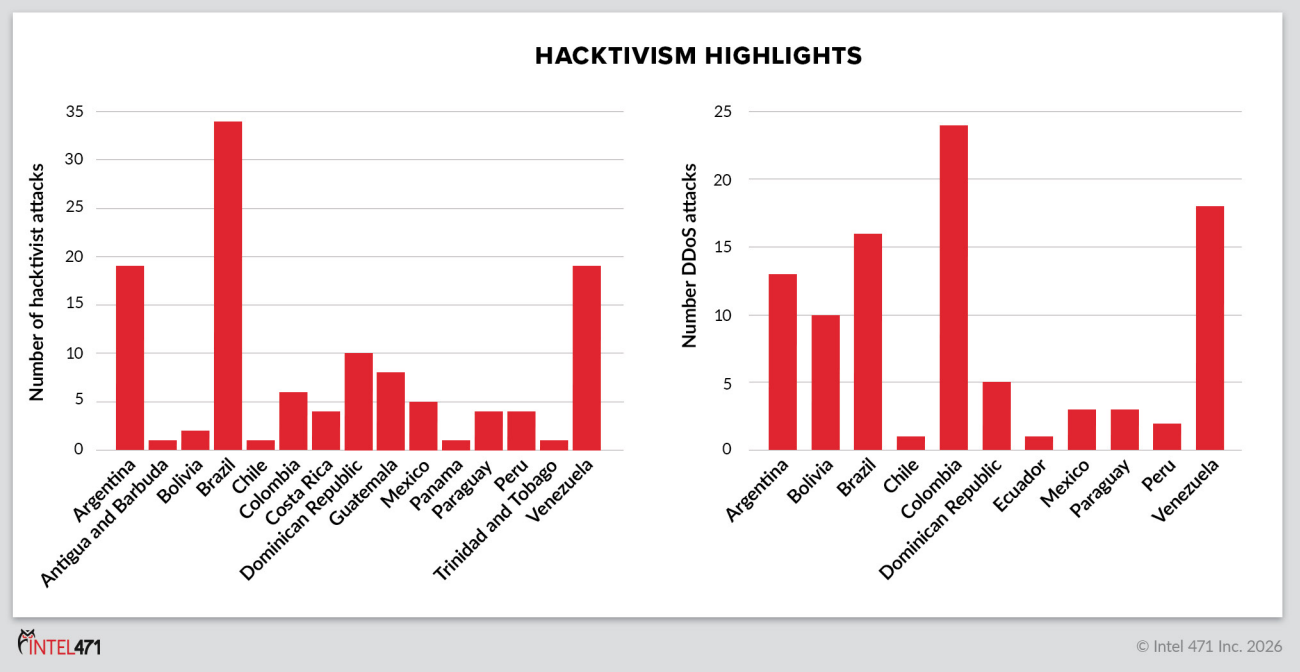

Figure 6: The image depicts hacktivist and DDoS attack statistics impacting countries in Latin America in 2025.

Underground Threats Detected Emanating from Region

Latin America is a major hub for cybercriminal activity, driven by an accelerated digital transformation and widespread adoption of online banking, e-commerce and digital communication across much of the population. This accelerated connectivity has often outpaced the development of mature cybersecurity capabilities, regulatory frameworks and incident response capacity, creating an environment that cybercriminals can readily exploit. Cybercriminals in the region are particularly associated with diverse forms of financial fraud conducted openly through social media platforms, malware operations that leverage Android-based banking trojans, phishing campaigns serving a wide range of objectives and the trafficking of stolen data and credentials.

Financial Fraud

Financial fraud is possibly the most pervasive cybersecurity challenge in South America, driven by a mature and interconnected cybercriminal ecosystem targeting individuals, financial institutions and businesses. Adversaries extensively leverage social media platforms such as Facebook, WhatsApp and Telegram to distribute scams, promote services and operate illicit marketplaces, with a primary focus on compromising credit card data, banking credentials and other monetizable financial assets.

Financial fraud is possibly the most pervasive cybersecurity challenge in South America, driven by a mature and interconnected cybercriminal ecosystem.

Our Intel 471 database contains multiple underground channels where actors actively exchange financial fraud techniques, promote carding practices and recruit collaborators such as money mules. Data panel services play a central role in this ecosystem, providing interfaces to validate stolen credit cards, check available balances or credit limits and trade datasets containing compromised card data, banking credentials, PII and account access.

These operations are largely enabled through social engineering and phishing campaigns and frequently supported by malware — particularly banking trojans tailored to regional financial and retail institutions.

In November 2025, the Brazilian actor ***Green** promoted a web store selling compromised payment cards from multiple financial institutions and offering a data query service since August 2025. The platform also offers recommendations, an exchange option and bank identification number (BIN) reservation capabilities. The store contained more than 80,000 compromised payment cards from multiple financial companies available at the time of this report.[32]

Social Engineering, Phishing

Social engineering serves as the primary enabling tactic for financial fraud across Latin America, with email and short message service (SMS) phishing campaigns the most prevalent delivery mechanisms for malicious lures. The payloads used in these campaigns vary according to adversary objectives and commonly include links or files that prompt victims to install banking trojans on personal or corporate systems, compromise mobile devices or harvest login credentials from varied systems and platforms.

Beyond phishing, fraudulent call centers represent a widespread tactic in the region, redirecting victims to resolve fabricated e-commerce transactions, payment disputes or alleged delivery issues. Social-engineering operations also heavily leverage instant-messaging platforms — particularly WhatsApp, one of the most widely used messenger applications in Latin America — to impersonate financial institutions, logistics providers and trusted contacts, further increasing the effectiveness and reach of these scams.

Social engineering serves as the primary enabling tactic for financial fraud across Latin America, with email and short message service (SMS) phishing campaigns the most prevalent delivery mechanisms for malicious lures.

In May 2025, FortiGuard Labs reported a phishing campaign distributed the Horabot malware, which targeted Windows users in Latin American countries such as Argentina, Chile, Colombia, Guatemala, Mexico and Peru. The campaign lured victims with fake invoices and financial documents to install the banking trojan, steal email credentials and harvest contact lists.[33]

In September 2025, Kaspersky reported the **RevengeHotels** aka **TA558** intrusion cluster launched a campaign that targeted the hospitality industry across Latin America in countries such as Argentina, Brazil, Chile and Mexico. The cluster conducted phishing campaigns that impersonated government agencies or reservation requests to deploy RATs and other malware payloads such as VenomRAT, XWorm and DesckVBRAT to steal credit card data from hotel front desks, enabling fraudulent transactions. The cluster reportedly incorporated artificial intelligence (AI)-generated scripts in loaders and downloaders.[34,35]

In November 2025, Sophos reported a multistage malware campaign that used WhatsApp as distribution vector to deploy the Astaroth aka Guildma banking trojan. The operation targeted WhatsApp Web users in Brazil and delivered compressed (ZIP) attachments containing malicious scripts. When executed, these scripts retrieved second-stage payloads that harvested WhatsApp sessions and installed Astaroth via a Microsoft Software Installer (MSI) package, enabling credential theft and persistence.[36]

Malware Operations

Banking trojans represent a central component of the financial cybercrime ecosystem in Latin America, enabling large-scale credential theft, account takeover and fraudulent transactions against both individual users and enterprises. For over a decade, the regional banking trojan threat landscape has been dominated by well-established and actively maintained malware strains, such as Grandoreiro, Mekotio, Guildma aka Astaroth and Ousaban, many of which originate from or are primarily operated by adversaries within Latin America. These trojans are tailored to local financial institutions, language preferences and user behavior, targeting banking portals, payment platforms and corporate environments.

For over a decade, the regional banking trojan threat landscape has been dominated by well-established and actively maintained malware strains.

The infrastructure of Grandoreiro, one of the most relevant banking trojans in the region, was taken down in a law enforcement operation in January 2024. However, the adversaries responsible for the malware operation rapidly recovered. Grandoreiro also expanded operations to Europe, Africa, South Asia and Oceania, targeting more than 1,500 bank institutions in more than 60 countries.[37,38]

A trend observed in the region is the increase of mobile banking trojans, reflecting the region's heavy reliance on smartphones for banking and digital payments. These trojans primarily target Android-based devices and are distributed through fraudulent application downloads. Once installed, mobile banking trojans may abuse accessibility services and overlay techniques to intercept credentials, capture one-time passwords (OTPs), hijack sessions and facilitate fraudulent transactions. Prominent malware strains that operated in the region include Xenomorph, Andromeda, GoatRAT, BrasDex and Zanubis.

Zanubis is an Android banking trojan that has consistently targeted users in Peru since its emergence in mid-2022. The actors behind the malware targeted Peru-based users by distributing the malicious applications as fake applications for the National Superintendency of Customs and Tax Administration aka SUNAT and were observed impersonating a specific local energy company and a bank in recent campaigns. The malware abuses accessibility services to perform a web-inject attack when one of the targeted applications is opened and is capable of recording the screen of the infected device and logging keystrokes.[39,40]

Another significant malware strain disclosed in 2025 was PhantomCard, an Android-based trojan that targeted banking customers in Brazil and had the capability to relay near-field communication (NFC) payment details to an adversary-controlled device. The ThreatFabric cybersecurity firm reported the actor **Go1ano** offered the trojan via Telegram and identified reliable evidence of a collaboration with Chinese actors from investigated malware samples.[41]

Actors Targeting, Operating from Latin America

Intel 471 investigated multiple actors that targeted or possibly operate from Latin America. Some recent examples include:

- The possible Mexican actor ***Yellow** has been involved in compromising, exfiltrating and monetizing sensitive data. The actor's primary targets included financial, government and telecommunications entities in Mexico, although ***Yellow** also attacked organizations in other countries. The actor's activities on underground forums consistently focused on the distribution and sale of extensive databases, often containing financial, operational and personal data sourced from leaks at Mexican government institutions and enterprises.[42]
- The Argentine actor ***Orange** offered to sell the Prysmax Stealer information-stealer malware, which was designed to extract data from multiple sources such as session data from the Discord and Telegram applications, Minecraft and Valorant accounts, and the MetaMask, Phantom and Trust Wallet cryptocurrency wallets, and allegedly can collect sensitive data such as cookies, credit card data and passwords stored in a web browser.[43]
- From early December 2024 to late May 2025, the Spanish-speaking actor ***Pink** systematically published and sold hacked databases and documents from Latin America-based companies and government entities.[44]
- In early September 2025, the actor ***White** offered to sell unauthorized access to a Mexico-based telecommunications company. The actor allegedly obtained initial access to the network by leveraging an exposed instance of the Zabbix open source software and maintained the access via a reverse shell and secure shell (SSH) remote command line.[45]
- In September 2025, the possible Indonesian actor ***Purple** leaked databases from multiple victims worldwide, including an Argentina-based e-commerce platform. The compromised data allegedly included academic and personal information and customers' addresses, full names and phone numbers.[46]
- In November 2025, the actor ***Silver** advertised a compromised dataset allegedly exfiltrated from the Brazil-based financial institution. The actor, who allegedly was an employee of the impacted entity, originally intended to sell only the compromised dataset but later claimed they also might be able to obtain remote desktop protocol (RDP) access to the bank's payment terminals at a later stage.[47]

Assessment

Latin America's rapid digitalization continues to outpace the adoption of mature security controls, governance frameworks and effective legal mechanisms to deter and prosecute cybercrime. This structural gap was highlighted in the OAS' cybersecurity maturity assessment released in December 2025, which identified uneven progress across policy, technical capacity and institutional coordination in multiple states. As a result, the region has evolved into not only a high-value target, but increasingly also a central hub for cybercriminal activity, with reported incident volumes and attack frequencies exceeding global averages across multiple open source datasets.

The region's role as a cybercrime hub is further reinforced by the exportation of criminal tradecraft initially developed for local contexts to international targets. Financial fraud schemes and banking trojans originally tailored to Latin American financial institutions have demonstrated scalability and adaptability, enabling their reuse against organizations and consumers in North America and Europe. This cross-regional spillover reflects the technical maturity of Latin American cybercriminal ecosystems that lower barriers to expansion beyond the region. Particularly notable is that several banking trojans originating in the region have remained operational for over a decade, with limited disruption efforts targeting their infrastructure and little evidence of sustained prosecution against the individuals responsible.

Looking ahead, we assess that meaningful risk reduction is unlikely in the near term. The development, harmonization and enforcement of national cybersecurity policies and legislation remain slow-moving processes, while cybercriminal innovation continues at a faster pace — especially in the era of AI. Absent significant improvements in regulatory enforcement, public-private cooperation and regional information sharing, Latin America is likely to remain both a primary operating environment and an export hub for financially motivated cybercrime over the coming years.

General Intelligence Requirements (GIRs)

1.1.1 Ransomware malware

1.1.4 Banking trojan malware

1.1.5 Information-stealer malware

1.2.2 Ransomware-as-a-service (RaaS)

1.3.11.5 Remote access tools

2.1.13 Initial access vulnerabilities

3.3 Dedicated criminal infrastructure

4.2 Compromised data or access

4.2.1 Payment card fraud

4.2.2 Compromised credentials

4.2.3 Compromised personally identifiable information (PII)

4.2.4 Compromised intellectual property (IP)

4.2.5 Compromised network or system access

4.7.2 Specified access

5.2.1 Initial access tactic

5.2.6 Credential access tactic

5.2.9 Collection tactic

5.2.11 Exfiltration tactic

5.2.12 Impact tactic

5.5 Information compromise or disclosure tactics

5.5.3 Information or data breach

5.5.4 Blackmail and extortion

5.5.5 Supply chain attack tactic

5.5.6 Hacktivism

6.1 All sectors and industries

6.2.3.2 Costa Rica

6.2.3.3 El Salvador

6.2.3.4 Guatemala

6.2.3.5 Honduras

6.2.3.6 Mexico

6.2.3.7 Nicaragua

6.2.3.8 Panama

6.2.6.1 Bermuda

6.2.8.1 Argentina

6.2.8.2 Bolivia

6.2.8.3 Brazil

6.2.8.4 Chile

6.2.8.5 Colombia

6.2.8.6 Ecuador

6.2.8.8 French Guiana

6.2.8.9 Guyana

6.2.8.10 Paraguay

6.2.8.11 Peru

6.2.8.13 Uruguay

6.2.8.14 Venezuela

6.2.9.8 Cuba

6.2.9.2 Antigua and Barbuda

6.2.9.4 Bahamas

6.2.9.5 Barbados

6.2.9.9 Curacao

6.2.9.11 Dominican Republic

6.2.9.13 Guadeloupe

6.2.9.14 Haiti

6.2.9.16 Martinique

6.2.9.18 Puerto Rico

6.2.9.22 Saint Martin

6.2.9.25 Trinidad and Tobago

7.7.2 Politically motivated cyber activity

Sources

Note: Many of the sources are intelligence reports based within Intel 471's cyber intelligence platform, Verity471, and cannot be made publicly available for operational security reasons. If you're interested in investigating our sources in full, please contact Sales@intel471.com.

1. Inter-American Development Bank (IDB). "2025 Cybersecurity Report: Vulnerability and Maturity Challenges to Bridging the Gaps in Latin America and the Caribbean." Jan.01 2025. https://publications.iadb.org/en/publications/english/viewer/2025-Cybersecurity-Report-Vulnerability-and-Maturity-Challenges-to-Bridging-the-Gaps-in-Latin-America-and-the-Caribbean.pdf
2. GIGA Hamburg (pure.giga-hamburg.de). "Cybersecurity Developments in Latin America: Problems, Models, and Cooperation Channels." Aug.01 2025. https://pure.giga-hamburg.de/ws/files/54047533/DigiTraL-08-Renzullo-Hall.pdf
3. Prosegur. "Cybersecurity in Latin America: a legislative, organizational and technological challenge." Mar 21 2024. https://www.prosegur.com/innovacion/ciber/cybersecurity-latin-america-legislative-challenge
4. Derechos Digitales. "CYBERSECURITY IN LATIN AMERICA: National Strategies in 2024." Dec 01 2024. https://www.derechosdigitales.org/wp-content/uploads/DD_CYRILLA_ENG_2024pdf.pdf
5. Intel 471. "Country Report: Brazil." Aug 14 2024. https://verity.intel471.com/
6. AZ (az.cl). "Chile transforms its digital strategy with Law 21,663 and the 2023–2028 National Cybersecurity Plan." Oct 29 2025. https://www.az.cl/en/chile-transforms-its-digital-strategy-with-law-21663-and-the-2023–2028-national-cybersecurity-plan/
7. Council of Europe (coe.int) – Octopus Programme. "Colombia." Oct 07 2023. https://www.coe.int/fr/web/octopus/country-wiki-ap/-/asset_publisher/CmDb7M4RGb4Z/content/id/64858830
8. Approve-IT. "Peru Publishes National Cybersecurity Strategy 2026-2028." Sept 05 2025. https://approve-it.net/peru-publishes-national-cybersecurity-strategy-2026-2028/
9. World Bank Blogs. "From fiction to reality: How Latin America became the world's most critical cyber battleground." Nov 28 2024. https://blogs.worldbank.org/en/latinamerica/seguridad-cibernetica-en-america-latina-y-el-caribe
10. Phishing for Answers. "Adversaries Targeting LATAM in 2025: Who They Are and How They Operate." https://www.phishingforanswers.com/blog/adversaries-targeting-latam-2025
11. Check Point Research. "Latin America 2025 Mid-Year Cyber Snapshot Reveals 39% Surge in Attacks as AI Threats Escalate Regional Risk." Jul 10 2025. https://blog.checkpoint.com/research/latin-america-2025-mid-year-cyber-snapshot-reveals-39-surge-in-attacks-as-ai-threats-escalate-regional-risk/

12. Center for Cybersecurity Policy and Law. “Bridging the Cybersecurity Gap in LATAM: How ISACs Enhance Regional Cooperation.” Mar 27 2025.
https://www.centerforcybersecuritypolicy.org/insights-and-research/bridging-the-cybersecurity-gap-in-latam-how-isacs-enhance-regional-cooperation

13. The Record. “Hackers reportedly compromise Argentina’s airport security payroll system.” Jan 06 2025.
https://therecord.media/hackers-target-airport-security-payroll

14. Security Affairs. “Paraguay Suffered Data Breach: 7.4 Million Citizen Records Leaked on Dark Web.” June 13 2025.
https://securityaffairs.com/178970/data-breach/paraguay-suffered-data-breach-7-4-million-citizen-records-leaked-on-dark-web.html

15. BankInfo Security. “Ransomware Group Threatens to Dump Paraguayan Citizens’ Data.” June 13 2025.
https://www.bankinfosecurity.com/ransomware-group-threatens-to-dump-paraguayan-citizens-data-a-28686

16. Intel 471, Spot Report. July 04 2025.
https://verity.intel471.com

17. Security Affairs. “INC ransom group claimed the breach of Panama’s Ministry of Economy and Finance.” Sept 15 2025.
https://securityaffairs.com/182203/data-breach/panamas-ministry-of-economy-and-finance-data-breach.html

18. Intel 471, Breach Alert. Sept 10 2025.
https://verity.intel471.com

19. Intel 471, Intelligence Summary. “Geopolitical landscape: Dec. 8, 2025, to Dec. 22, 2025.” Dec 22 2025.
https://verity.intel471.com

20. Americas Quarterly. “Cybersecurity: The Next Frontier of U.S.-China Competition in the Americas.” Jul 25 2023.
https://americasquarterly.org/article/cybersecurity-the-next-frontier-of-u-s-china-competition-in-the-americas/

21. CrowdStrike. “2025 Latin America Threat Landscape Report: A Deep Dive into an Evolving Region.” May 19 2025.
https://www.crowdstrike.com/en-us/blog/2025-latam-threat-landscape-report-deep-dive/

22. Federal Bureau of Investigation (FBI). “AQUATIC PANDA CYBER THREAT ACTORS.” Feb 19 2025.
https://www.fbi.gov/wanted/cyber/aquatic-panda-cyber-threat-actors

23. Intel 471, Information Report. “Actor leaks files with internal documents impacting China-based company.” Mar 13 2025.
https://verity.intel471.com

24. Intel 471, Profile Report. “North Korea information technology workers, online personas, associated entities.” Jul 16 2025.
https://verity.intel471.com

25. Brazil Reports. “Brazil, Paraguay resume Itaipu hydropower talks months after espionage operation fallout.” Nov 18 2025.
https://brazilreports.com/brazil-paraguay-resume-itaipu-hydropower-talks-months-after-espionage-operation-fallout/7205/

26. Check Point Research. “Blind Eagle: …And Justice for All.” Mar 10 2025.
https://research.checkpoint.com/2025/blind-eagle-and-justice-for-all/

27. Journal of Cyber Policy. “Hack-and-leak operations in Latin America: the case of Guacamaya.” Nov 09 2024.
https://www.tandfonline.com/doi/pdf/10.1080/23738871.2024.2419509

28. Jack D. Gordon Institute for Public Policy. “Ransomware Gangs and Hacktivists.” Aug 23 2024.
https://storymaps.arcgis.com/stories/33a809c8484c439b9f942590749a7f5a

29. Intel 471, Breach Alert. Mar 10 2025.
https://verity.intel471.com

30. Intel 471, Breach Alert. Jun 12 2025.
https://verity.intel471.com

31. Intel 471, Breach Alert. June.14 2025.
https://verity.intel471.com

32. Intel 471, Information Report. “Actor promotes underground store selling compromised payment cards.” Nov 27 2025.
https://verity.intel471.com

33. Fortinet. “Horabot Unleashed: A Stealthy Phishing Threat.” May 12 2025.
https://www.fortinet.com/blog/threat-research/horabot-unleashed-a-stealthy-phishing-threat

34. Kaspersky Securelist. “RevengeHotels: a new wave of attacks leveraging LLMs and VenomRAT.” Sept 16 2025.
https://securelist.com/revengehotels-attacks-with-ai-and-venomrat-across-latin-america/117493/

35. The Record. “Hackers steal hotel guests’ payment data in new AI-driven campaign.” Sept 17 2025.
https://therecord.media/hackers-payment-data-guests-steal

36. Sophos. “WhatsApp compromise leads to Astaroth deployment.” Nov 20 2025.
https://www.sophos.com/en-us/blog/whatsapp-compromise-leads-to-astaroth-deployment

37. The Hacker News. “Grandoreiro Banking Trojan Resurfaces, Targeting Over 1,500 Banks Worldwide.” May 19 2024.
https://thehackernews.com/2024/05/grandoreiro-banking-trojan-resurfaces.html

38. Mimecast. “Grandoreiro Infostealer Campaign.” Aug 04 2025.
https://www.mimecast.com/threat-intelligence-hub/grandoreiro-infostealer-campaign/

39. Intel 471, Malware Report. “Zanubis - Banking trojan infects Android users in Peru.” Nov 22 2022.
https://verity.intel471.com

. Crowdfund Insider. “Mobile Malware Posing as Invoice Reportedly Steals Banking Credentials from Unsuspecting Users.” Jun 01 2025. https://www.crowdfundinsider.com/2025/06/240694-mobile-malware-posing-as-invoice-reportedly-steals-banking-credentials-from-unsuspecting-users/

41. ThreatFabric. “PhantomCard: New NFC-driven Android malware emerging in Brazil.” Aug 14 2025. https://www.threatfabric.com/blogs/phantomcard-new-nfc-driven-android-malware-emerging-in-brazil

42. Intel 471, Information Report. “Actor offers to sell dataset, source code.” Oct 06 2025. https://verity.intel471.com

43. Intel 471, Information Report. “Actor promotes Prysmax Stealer information-stealer malware.” Feb 04 2025. https://verity.intel471.com

44. Intel 471, Information Report. “Actor offers to sell database” Dec 11 2024. https://verity.intel471.com

45. Intel 471, Information Report. “Actor offers to sell unauthorized access to undisclosed Mexico-based telecommunication company.” Sept 16 2025. https://verity.intel471.com

46. Intel 471, Information Report. “Actor claims breach of public sector entity.” Sept 04 2025. https://verity.intel471.com

47. Intel 471, Information Report. “Actor offers to sell compromised data, unauthorized access from financial institution.” Nov 17 2025. https://verity.intel471.com/

About Intel 471

Intel 471 equips enterprises and government agencies with intelligence-driven security offerings powered by real-time insights into cyber adversaries, threat patterns, and potential attacks relevant to their operations. By integrating human-sourced intelligence with advanced automation and curation, the company’s platform enhances security measures and enables teams to bolster their security posture by prioritizing controls and detections based on real-time cyber threats. Organizations are empowered to neutralize and mitigate digital risks across dozens of use cases across our solution portfolios: Cyber Threat Exposure, Cyber Threat Intelligence, and Cyber Threat Hunting. Learn more at intel471.com.

Our customers’ eyes and ears outside the wire.