DARKTRACE

ANNUAL THREAT REPORT 2026:
LATIN AMERICA REGIONAL OUTLOOK

The global cyber threat landscape in 2025 was increasingly defined not by uniform trends, but by regional threat economies shaped by maturity, geopolitics, the speed of digitization, and attacker objectives. This regional breakdown provides a focused analysis of the key threat trends, notable threat actors, and outlook for Latin America.

Latin America is witnessing a rapid shift from traditional ransomware to data-leak extortion and information stealing malware, focusing on credential theft and sensitive data exfiltration by financially motivated threat actors. Regulatory momentum is building as Brazil, Chile, Argentina, Mexico, and others have enacted data protection laws [1, 2] along with continuous narratives to boost investment in cybersecurity solutions, where 2025 market estimates of USD 18-23 billion are projected to reach USD 30-50 billion by 2030 [3, 4].

However, persistent skills shortages, uneven maturity across national cybersecurity strategies, and reliance on Managed Security Service Providers (MSSPs) continue to challenge regional cyber readiness. Further, these challenges are being amplified by geopolitical dynamics, with China's growing digital footprint through telecommunications and infrastructure projects raising concerns over strategic dependency and surveillance.

Meanwhile, the recent US cyber operation against Venezuela underscores how state-level cyber actions could reshape regional threat perceptions and policy priorities.

REGIONAL TRENDS AND STATISTICS

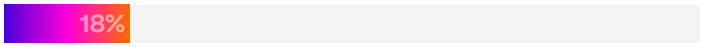
TOP ATTACK VECTORS

Phishing and the use of compromised credentials remain the leading attack vectors. In 44% of cases within the region, malware (excluding ransomware) spread following device compromise through these methods.

While phishing dominates, new ransomware strains surged in the region with attribution to BlackSuit, Sauron, Medusa, and Dire Wolf. These cases also signal a shift from data encryption to data leak extortion.

MOST IMPACTED SECTORS

Education was the most impacted sector, making up 18% of all incidents, followed by Public Administration, and Information and Communication.



The Manufacturing and Wholesale/Retail Trade sectors have experienced an increase in cases from the first half of the year to the second, with an increase in incidents of malware propagation, likely driven by accelerated digitization and greater exposure of sensitive data.

MOST IMPACTED COUNTRY

Colombia was consistently the most impacted country in Latin America, followed by Ecuador, Chile, and Mexico. Threats like malware propagation from eCrime and nation-state aligned cyber espionage groups will likely continue to surge in Colombia due to its large economy, high levels of digitalization, and uneven maturity in cybersecurity skills.

REGIONAL VS. GLOBAL COMPARISON

Due to rapid digitalization mixed with uneven security, underinvestment mixed with lagging legislation, and political/economic instability mixed with limited resources, threat actors very likely view Latin America as a profitable region for financially-motivated crimes like ransomware, data-theft, and nation-state espionage.

CHINA'S INFLUENCE IN LATIN AMERICA

China-nexus activity in Latin America reflects a consistent playbook: rapid exploitation of internet-facing appliances to gain stealthy footholds, followed by long-dwell, tooling-efficient operations. Campaigns leveraging Barracuda ESG (CVE-2023-2868) and Palo Alto PAN-OS (CVE-2024-3400) map to documented People's Republic of China (PRC) tradecraft that prioritizes edge devices for access, collection, and persistence with minimal endpoint noise.

Targeting patterns concentrate on Financial institutions in Panama and Colombia, Brazilian Telecommunications, and Colombian Government entities, aligning with strategic intelligence priorities.

Darktrace observed post-access activity anchored by ShadowPad, with DNS-based command-and-control (C2) tunneling, dynamic-link library (DLL) sideloading (e.g., mscorsvc.dll), and LOLBins (WMI/SVCCTL/PsExec) to blend into enterprise operations.

Operators routinely leverage cloud and ORB infrastructure, including Vultr and Cloudflare ArgoTunnel, and deploy Remote Monitoring and Management (RMM) tools (AnyDesk, RustDesk) for resilient commands and lateral movement. Command-line fetch tools (curl/wget) and occasional FTP exfiltration round out a tradecraft set optimized for portability, speed, and operational security.

Looking across these intrusions, the targeting patterns reinforce a broader strategic arc tied to China's expanding economic and digital footprint in Latin America. The focus on financial development organizations, government ministries, telecommunications, and energy mirrors the sectors most intertwined with Beijing's Belt and Road Initiative (BRI) and its "Digital Silk Road" extensions in the region.

These institutions hold regulatory, transactional, and infrastructure data that can shape investment environments, forecast political shifts, and enable strategic leverage across BRI-participating economies.

As China moves toward its 2030 objectives, securing supply chains, expanding influence over regional infrastructure, and deepening technological dependencies, cyber operations of this nature provide strategic advantage. The tradecraft observed in Latin America suggests a long-term posture: gaining durable access now to environments that will become increasingly consequential as China's economic and geopolitical statecraft integration across the hemisphere accelerates.

NOTABLE THREAT ACTORS

Actor	Motivation & Targets	Key Tactics
BlindEagle (APT-C-36)	**Blind Eagle** characteristically targets government institutions, financial organizations, and critical infrastructure in Latin America with the goal of data exfiltration.	**Initial Access** - T1189 – Drive-by Compromise **Initial Access ICS** - T0865 – Spearphishing Attachment **Initial Access ICS** - T0817 - Drive-by Compromise **Resource Development** - T1588.001 – Malware **Lateral Movement ICS** - T0843 – Program Download **Command and Control** - T1568.002 – Domain Generation Algorithms **Exfiltration - T1041** – Exfiltration Over C2 Channel
Water Saci	**Brazil-focused cybercriminal group** that primarily uses self-propagating malware (named SORVEPOTEL) delivered via WhatsApp to target financial institutions and cryptocurrency exchanges.	**Initial Access** – T1566.003 - Spearphishing via Service **Execution** - T1204.002 – User Execution: Malicious File **Execution** - T1059.005 & T1059.001– Command and Scripting Interpreter: Visual Basic; Command and Scripting Interpreter: PowerShell **Persistence** - T1547.001 – Registry Run Keys / Startup Folder **Credential Access** - T1539 – Steal Web Session Cookie **Command and Control** - T1071.001 – Application Layer Protocol: Web Protocols
SambaSpider	**A Brazil-based cybercrime group that is primarily motivated by financial gain.** Their main target is to steal banking credentials and other sensitive data, predominantly from users and organizations in Latin America. The group is linked to the Mispadu banking trojan.	**Initial Access** - T1566.001 – Phishing: Spearphishing Attachment **Execution** - T1204.002 – User Execution: Malicious File **Execution** - T1059.05 – Command and Scripting Interpreter: VBScript **Execution** - T1027 – Obfuscated Files or Information **Defense Evasion** - T1027 – Obfuscated Files or Information **Defense Evasion** - T1070 – Indicator Removal on Host **Persistence** - T1059 – Command and Scripting Interpreter **Credential Access** - T1555.003 – Credentials from Web Browsers

NOTABLE THREAT ACTORS

CASE STUDY

In July 2025, Darktrace identified activity consistent with likely Dire Wolf ransomware after observing unusual file renaming patterns and the appearance of ransom notes on a customer's network. Initial access was gained through the use of the remote management tool TeamViewer, after which a malicious actor created an RDP tunnel, likely to facilitate lateral movement across the environment.

Evidence of both data encryption and data exfiltration was detected. The incident was contained and thoroughly investigated, with restoration efforts carried out in collaboration with partner organizations. Details of the activity were later shared publicly across multiple open-source intelligence (OSINT) channels.

INSIGHTS & OUTLOOK

Brazil, Mexico, and Colombia have consistently reported the highest number of cases in Latin America across the Darktrace customer base over the past three years. This trend is likely to continue due to the size of their economies and their geopolitical significance.

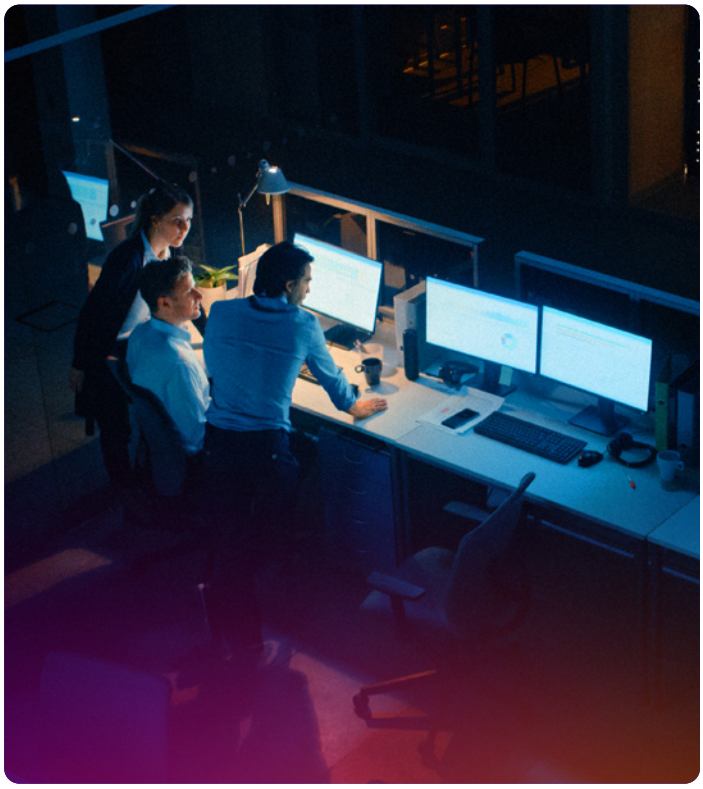
Top reported threats consist of compromised credentials, as seen in numerous software-as-a-service (SaaS) intrusion cases, ransomware data-leak extortion, and malware-related cases with increases in informations stealer activity. These threats may continue to be prevalent in the region as financially-motivated threat groups consistently target Latin America.

The top attack vector for malware delivery observed by Darktrace is email, which will likely continue to be a trend in the region as the economy becomes increasingly highly digitized, paired with human vulnerabilities.

In 2025, the most impacted sectors in Latin America were the Finance and Public Service-related sectors, which recorded the highest number of reported cases across multiple countries. However, Latin America may continue to see an increase in attacks against the Technology and Manufacturing sectors, as these sectors encompass critical infrastructure that nation-state threat actors may seek to target.

REGIONAL ANALYSIS METHODOLOGY:

It is important to note that while the analysis is relevant and broadly representative of wider global trends, it is also influenced by the geographic distribution of Darktrace's customer base. For example, within the Americas (AMS) region, the US represents the largest share of Darktrace customers, meaning insights in this section may be weighted more heavily toward US-based activity.



[1] [Online]. Available: https://www.feedzai.com/blog/latam-financial-regulations/.

[2] [Online]. Available: https://hackenproof.com/blog/for-business/crypto-regulations-latin-america-2025-2026.

[3] [Online]. Available: https://www.mordorintelligence.com/industry-reports/latin-america-cyber-security-market.

[4] [Online]. Available: https://www.grandviewresearch.com/horizon/outlook/cyber-security-market/latin-america .