The Expanding Cyberspace Threat Environment

Ransomware, identity compromise, exploited vulnerabilities, and critical-infrastructure exposure, updated for the Latin American and Caribbean threat picture.

DOCUMENT ID	PUBLISHED	THREAT LEVEL	CONFIDENCE
SM-2026-TA-102	28 JANUARY 2026	SEVERE	HIGH

FORECAST HORIZON: 12 MONTHS | REGIONS: GLOBAL, WESTERN HEMISPHERE, SOUTH AMERICA, CARIBBEAN, CENTRAL AMERICA
COUNTRIES: UNITED STATES, BRAZIL, MEXICO, COLOMBIA, ARGENTINA, CHILE
UPDATED: 3 SEPTEMBER 2026

DOCUMENT CONTROL

PRODUCT RECORD

FIELD	VALUE
Document ID	SM-2026-TA-102
Product type	Threat assessment - open-source intelligence
Publication date	28 January 2026
Update date	3 September 2026
Threat level / confidence	Severe / High
Forecast horizon	12 months (reviewed at 60-day intervals)
Analytic coverage	Cybersecurity, Critical Infrastructure, Ransomware, Identity Security
Classification / handling	OPEN SOURCE / CLIENT USE. Derived from vendor threat research, public advisories, and incident reporting. Vendor incident counts are reported figures, not audited totals.
Review trigger	A ransomware incident affecting national critical infrastructure in the region, a new mass-exploited edge-device vulnerability, or a material revision to published incident counts.

Government, police, and party statements reproduced here are official claims or allegations and are labelled as such; they are not treated as adjudicated fact.

1. EXECUTIVE SUMMARY

The cyberspace threat environment continues to be dominated by four reinforcing patterns: ransomware and extortion, identity and credential compromise, rapid exploitation of known internet-facing vulnerabilities, and abuse of trusted technology providers to reach downstream victims. None of these requires novel capability. They persist because they are cheap, repeatable, and effective against organisations with incomplete asset inventories and inconsistent multi-factor authentication.

UPDATE, 3 SEPTEMBER 2026: Recorded Future research places Latin America and the Caribbean at the centre of this pattern, reporting 452 ransomware incidents affecting organisations in the region during 2025. Brazil and Mexico absorbed the largest shares, with Argentina, Colombia, and Chile following. The most affected sectors were manufacturing, professional and business services, government and public administration, financial services, and healthcare. Beyond ransomware, the research highlights infostealer malware, hacktivist activity, business email compromise, and state-linked espionage as concurrent pressures on the same defensive base.

The most consequential finding for regional clients is not the incident count but the cause profile. Weak or absent multi-factor authentication, legacy and unsupported systems, limited security staffing, and slow patching of internet-facing infrastructure explain the majority of successful intrusions. These are budget and process problems rather than technology gaps, which means the exposure is addressable but structurally persistent across the forecast horizon.

2. KEY JUDGMENTS

1. Ransomware remains the highest-volume material threat to regional organisations; Recorded Future reported 452 incidents affecting Latin America and the Caribbean in 2025.
2. Brazil and Mexico carry the largest national exposure by incident volume, reflecting economy size, digitalisation, and attack-surface breadth rather than uniquely weak defences.
3. Manufacturing, professional services, government, financial services, and healthcare are the most targeted sectors; each combines operational urgency with legacy dependency, which raises extortion leverage.
4. Identity compromise is the dominant initial access vector. Infostealer-harvested credentials, session-token theft, and MFA gaps convert commodity malware into enterprise intrusion.
5. Legacy and unsupported systems, particularly in government and healthcare, extend recovery times and increase the probability of paying extortion demands.
6. Internet-facing edge devices - VPN appliances, firewalls, routers, and file-transfer systems - remain the most reliably exploited entry point across the region.
7. Hacktivist and politically motivated activity increases around elections and social unrest, adding availability and defacement risk on top of criminal extortion.
8. State-linked espionage against government, energy, and telecommunications targets continues in parallel with criminal activity and frequently uses the same unpatched infrastructure.
9. Business email compromise remains the highest-loss-per-incident financial threat for mid-sized regional firms and is under-reported relative to ransomware.

3. RISK PROFILE

RISK PROFILE (1-5)

Relative severity across the 12-month forecast horizon, updated 3 September 2026 for the Latin America and Caribbean picture.

4. REGIONAL UPDATE: LATIN AMERICA AND THE CARIBBEAN

The September 2026 update incorporates Recorded Future research on the regional threat landscape. Figures below are as reported by the vendor and are used as indicative scale rather than audited totals.

REPORTED 2025 REGIONAL PICTURE

DIMENSION	REPORTED FINDING
Ransomware incidents	452 incidents affecting organisations across Latin America and the Caribbean during 2025.
Most-affected countries	Brazil and Mexico lead by volume, followed by Argentina, Colombia, and Chile.
Most-affected sectors	Manufacturing; professional and business services; government and public administration; financial services; healthcare.
Concurrent threat types	Infostealer malware, hacktivism, business email compromise, and state-linked espionage operating alongside extortion activity.
Principal contributing weaknesses	Weak or missing multi-factor authentication, legacy and unsupported systems, constrained security staffing, and slow patching of internet-facing infrastructure.

RELATIVE NATIONAL EXPOSURE BY REPORTED INCIDENT VOLUME (1-5)

Indexed to reported incident volume; smaller economies may carry higher per-organisation risk than their totals suggest.

5. WHY THE SAME CAUSES RECUR

- Multi-factor authentication is deployed to email but not to VPNs, remote administration, or third-party portals, leaving the highest-value paths single-factor.
- Asset inventories omit edge devices and inherited systems, so patching programmes cannot reach the most exposed infrastructure.
- Legacy hospital, utility, and municipal systems cannot be patched without service interruption, so compensating controls are deferred indefinitely.
- Security staffing is concentrated in a small number of generalists, which limits detection engineering and after-hours response.
- Third-party providers hold privileged access with weaker controls than the organisations they serve.

6. INDICATORS AND WARNINGS

INDICATOR	ANALYTIC SIGNIFICANCE
Ransomware affecting a national utility, port, or health system in the region	Escalates from commercial loss to national-service disruption and government intervention.
Mass exploitation of a new edge-device vulnerability	Historically the fastest path from disclosure to regional intrusion wave.
Sharp increase in infostealer logs referencing corporate domains	Predicts intrusion attempts within weeks and indicates credential hygiene failure.

INDICATOR	ANALYTIC SIGNIFICANCE
Extortion groups publishing regional victim data at higher cadence	Signals successful targeting and rising payment refusal.
Election-linked hacktivist campaigns in Brazil or Colombia	Adds availability risk to public-facing services and payment infrastructure.
Regulatory breach-notification enforcement action	Raises the compliance cost of the same technical exposure.

7. IMPLICATIONS FOR CLIENTS

- Enforce phishing-resistant multi-factor authentication on VPN, remote administration, privileged accounts, and third-party portals before extending it elsewhere.
- Build and maintain an inventory of internet-facing systems, including edge appliances and inherited infrastructure, with an owner for each.
- Prioritise patching against known exploited vulnerability catalogues rather than severity scores alone.
- Segment and monitor legacy systems that cannot be patched; treat compensating controls as a funded programme, not a temporary measure.
- Test recovery, not just backup: measure restore time for the systems that would halt revenue or patient care.
- Require security attestations and incident-notification terms from managed service and software providers with privileged access.

8. INTELLIGENCE GAPS

- Regional incident counts rely on vendor visibility and leak-site observation and understate unreported extortion.
- Payment rates and loss magnitudes in the region are not reliably published.
- Sector attribution varies between vendors, complicating year-over-year comparison.
- The overlap between criminal and state-linked intrusion sets is not fully resolved.
- Small and mid-sized enterprise exposure is systematically under-measured.

9. SOURCES AND METHODOLOGY

This assessment synthesises vendor threat research, public advisories, and incident reporting. The September 2026 update incorporates Recorded Future's reporting on the Latin American and Caribbean threat landscape. Confidence is High for the pattern and Moderate for precise incident counts, which depend on vendor visibility.

- Recorded Future, research on the Latin America and Caribbean threat landscape, 2026.
- Public cybersecurity advisories on known exploited vulnerabilities and edge-device compromise.
- Sentinel Meridian SM-2026-TA-107, Cyber Sleeper Access.

– Sentinel Meridian SM-2026-TA-118, QTFY's IoT Obfuscation Network and Persistent PRC Cyber Access.