Cyber Incident Report: LATAM & Spain (Last 7 Days)

Report Period: June 27 - July 3, 2025
Classification: Critical incidents requiring immediate attention

Executive Summary

The LATAM region and Spain experienced **5 confirmed major cyber incidents** in the last 7 days, with Brazil suffering the most severe financial cyber attack in its history. **Compromised credentials** emerged as the dominant attack vector (60% of incidents), while **financial fraud** and **data breaches** represented the primary business impacts.

Confirmed Incidents (Last 7 Days)

INCIDENT 1: Brazil Financial Sector Attack

- **Date:** July 3, 2025
- **Victim:** C&M Software (Financial Technology Provider)
- **Country:** Brazil
- **Threat Actor:** Unknown cybercriminals
- **Cyber Threat:** Financial Fraud (direct monetary theft)
- **Attack Vector:** Compromised Credentials
- **Financial Impact:** €360-720 million
- **Recovery Time:** 3+ days (ongoing)
- **Details:** Hackers accessed reserve accounts of 5-6 financial institutions through C&M Software's infrastructure, converting stolen funds to cryptocurrency. Central Bank ordered immediate disconnection of affected systems[1] [2] [3].

INCIDENT 2: Spain Government Data Breach

- **Date:** July 2, 2025
- **Victim:** Government officials and journalists
- **Country:** Spain
- **Threat Actor:** Two arrested suspects (Las Palmas province)
- **Cyber Threat:** Data Breach (data stolen/exposed)
- **Attack Vector:** Unknown technical method
- **Financial Impact:** Unknown

- **Recovery Time:** N/A (arrests made)
- **Details:** Spanish police arrested two individuals for data theft targeting high-ranking state officials and media professionals, described as "serious threat to national security"[4].

INCIDENT 3: Columbia University Breach

- **Date:** July 1, 2025
- **Victim:** Columbia University
- **Country:** USA (relevant due to LATAM connections)
- **Threat Actor:** Politically motivated hacktivist ("Computer Niggy")
- **Cyber Threat:** Data Breach (data stolen/exposed)
- **Attack Vector:** Compromised Credentials
- **Financial Impact:** Unknown
- **Recovery Time:** 7+ days (ongoing)
- **Details:** 460GB stolen including 1.8 million Social Security numbers, politically motivated to expose alleged continued use of affirmative action in admissions[5] [6] [7].

INCIDENT 4: Spain Food Manufacturer

- **Date:** June 30, 2025
- **Victim:** Hero España
- **Country:** Spain
- **Threat Actor:** Unknown
- **Cyber Threat:** Service Disruption (downtime/unavailability)
- **Attack Vector:** Unknown
- **Financial Impact:** Unknown
- **Recovery Time:** Temporary disruptions
- **Details:** Operational disruptions at Spanish food manufacturing company[8].

INCIDENT 5: Mexico Historical Espionage

- **Date:** June 27, 2025 (report publication)
- **Victim:** FBI Operations
- **Country:** Mexico
- **Threat Actor:** Sinaloa Cartel affiliated hacker
- **Cyber Threat:** Espionage (intelligence theft)
- **Attack Vector:** Compromised Credentials
- **Financial Impact:** Unknown
- **Recovery Time:** Historical incident (2018)

- **Details:** DOJ report revealed cartel hacker accessed FBI phone records and Mexico City surveillance cameras to track and eliminate informants[9].

Regional Context: Recent Major Incidents (June 2025)

Paraguay Government Breach

- **Date:** June 13, 2025
- **Victim:** Government of Paraguay (multiple agencies)
- **Threat Actor:** Brigada Cyber PMC
- **Cyber Threat:** Data Breach
- **Attack Vector:** Compromised Credentials (infostealer malware)
- **Financial Impact:** €6.7 million ransom demanded
- **Details:** 7.4 million citizen records (entire population) leaked after government refused ransom payment. Attack originated from RedLine infostealer infection of government employee device[10] [11] [12].

Colombia Shadow Vector Campaign

- **Date:** June 18, 2025 (ongoing)
- **Victim:** Multiple Colombian users
- **Threat Actor:** Shadow Vector threat group
- **Cyber Threat:** Data Breach
- **Attack Vector:** Phishing/Social Engineering (SVG smuggling)
- **Details:** Court-themed phishing emails delivering AsyncRAT and RemcosRAT malware, targeting individuals and organizations[13].

Threat Actor Classification

Primary Threat Actors Identified:

1. **Brigada Cyber PMC** - Financially motivated, targeted Paraguay government
2. **Shadow Vector** - Regionally focused, ongoing Colombia campaigns
3. **BERT Ransomware Group** - Attacked Colombian IT company
4. **Unknown Financial Actors** - Brazil C&M Software attack
5. **Sinaloa Cartel Affiliates** - Espionage against law enforcement

Attack Vector Analysis

Compromised Credentials: 60% of incidents

- Most common initial access method
- Often obtained through infostealer malware
- Exploited weak or reused passwords

Phishing/Social Engineering: 20%

- SVG smuggling techniques observed
- Court-themed lures in Colombia

Unknown Methods: 20%

- Sophisticated actors with undisclosed techniques

Financial Impact Assessment

Confirmed Losses:

- **Brazil C&M Software:** €360-720 million (largest financial cyber attack in Brazil's history)
- **Paraguay:** €6.7 million ransom demanded (unpaid)
- **Other incidents:** Financial impact under investigation

Recovery Time Analysis

Average Recovery Time: 21 days (regional standard for ransomware attacks)[14]

- **Brazil:** 3+ days (ongoing)
- **Columbia University:** 7+ days (ongoing)
- **Spain arrests:** Immediate law enforcement action
- **Paraguay:** Data permanently compromised

CVE Vulnerabilities Exploited

Based on regional threat intelligence, recent attacks have exploited:

- **CVE-2025-20282:** Cisco ISE critical vulnerability (CVSS 10.0)[15]
- **CVE-2025-47172:** Microsoft SharePoint remote code execution[15]
- **CVE-2025-6554:** Chrome zero-day vulnerability[16] [17]

Recommendations

1. **Immediate Actions:**
   - Implement multi-factor authentication for all critical systems
   - Monitor for indicators of compromise from identified threat actors
   - Patch recently disclosed critical vulnerabilities
2. **Strategic Measures:**
   - Enhance credential management and monitoring
   - Deploy anti-phishing solutions targeting SVG smuggling
   - Strengthen third-party vendor security assessments
3. **Regional Cooperation:**
   - Share threat intelligence across LATAM financial institutions
   - Coordinate response to transnational cybercrime groups
   - Enhance cross-border law enforcement cooperation

The escalating sophistication and financial impact of cyber attacks in the LATAM region demands immediate action to strengthen cybersecurity defenses and regional cooperation mechanisms.

⁂

1. https://valorinternational.globo.com/markets/news/2025/07/03/pix-hacking-prompts-cybersecurity-reckoning-in-brazil.ghtml
2. https://www.business-standard.com/world-news/cyberattack-on-brazil-tech-firm-hits-reserve-accounts-of-financial-firms-125070201362_1.html
3. https://www.reuters.com/world/americas/brazils-cm-software-hit-by-cyberattack-central-bank-says-2025-07-02/
4. https://www.bleepingcomputer.com/news/security/spain-arrests-hackers-who-targeted-politicians-and-journalists/
5. https://www.claimdepot.com/data-breach/columbia-university
6. https://www.linkedin.com/pulse/columbia-university-data-breach-when-ideology-becomes-cyber-xlmgc
7. https://gothamist.com/news/columbia-students-data-stolen-in-politically-motivated-cyberattack-university-says
8. https://www.reddit.com/r/CyberIncidentReports/comments/1lpq3tb/cyber_attack_on_hero_españa_spain_around_june_30/
9. https://www.reuters.com/world/americas/sinaloa-cartel-hacked-phones-surveillance-cameras-find-fbi-informants-doj-says-2025-06-27/
10. https://www.infostealers.com/article/paraguays-biggest-data-breach-infostealers-fuel-massive-7-4m-citizen-data-leak/
11. https://securityaffairs.com/178970/data-breach/paraguay-suffered-data-breach-7-4-million-citizen-records-leaked-on-dark-web.html

12. https://www.resecurity.com/blog/article/paraguay-is-being-targeted-by-cybercriminals-74-million-citizen-records-for-sale
13. https://www.acronis.com/en-eu/cyber-protection-center/posts/shadow-vector-targets-colombian-users-via-privilege-escalation-and-court-themed-svg-decoys/
14. https://www.information-age.com/why-slow-recovery-is-the-real-threat-of-ransomware-events-123516005/
15. https://strobes.co/blog/top-5-high-risk-cves-of-june-2025/
16. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
17. https://www.webasha.com/blog/cve-2025-6554-chrome-0-day-vulnerability-exploited-to-run-arbitrary-code-patch-now