LATAM Financial Sector Threat Landscape 2025

Evaluating Threat Actor Targeting and Defense Strategies for Latin American Financial Sector Institutions

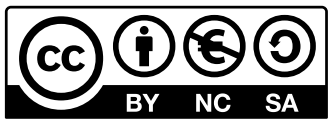
DIGI AMERICAS

Duke | PRATT SCHOOL of ENGINEERING

In collaboration with Recorded Future®

DIGI AMERICAS ALLIANCE MEMBERS

aws, Apple, Batuta, CHECK POINT, CISCO, CLOUDFLARE, CROWDSTRIKE, Google, kriptos, LUMU, mastercard, netskope, paloalto NETWORKS, fluid attacks we hack your software, Resecurity, Schneider Electric, SISAP Sistemas Aplicativos, Telefónica, tenable, Trellix, TREND MICRO



Credits

Duke University

Rupal Kharod
Arturo Ehuan
Justin Hayes
Emmanuel Petrov
Sakthi Vinayak
Shefali Ahuja
Aditya Srikar
Lucy Li
Diego Sanchez

Digi Americas Alliance

Alain Karioty
Alexis Steffaro
Andy Kotz
Belisario Contreras
Brett DeWitt
Carlos Torales
Christian Torres
Cory Bullock
Fernando Quintero
Gene Yoo
Ghassan Dreibi
Hernan Armbruster
Jordana Siegel
Jorge Blanco
José Juan Haro
Mario de la Cruz Sarabia
Mauricio Benavides
Mauricio Nanne
Norberto (Bert) Milan
Patrick Ford
Rafael Alvarez
Ricardo Villadiego
Stephen Fallas

DIGI AMERICAS ALLIANCE MEMBERS

aws Apple Batuta CHECK POINT CISCO CLOUDFLARE CROWDSTRIKE
Google kriptos LUMU netskope paloalto NETWORKS fluid attacks we hack your software
Resecurity Schneider Electric SISAP Sistemas Aplicativos Telefónica tenable Trellix TREND MICRO

Executive Summary

Latin America is among the least prepared regions for cyber attacks, according to the UN Cybersecurity Index.[1] This vulnerability stems from underinvestment in cybersecurity, the scarcity of skilled professionals, and weak regulatory frameworks.[2] While a digital revolution arose in sectors like fintech and e-commerce after the COVID-19 pandemic, these advancements were not matched by adequate security measures. As the founder of the Latin American Cybersecurity Research Network, Louise Marie Hurel, notes, "Latin America's entrepreneurial and innovative spirit does not come with a concern for security".[3]

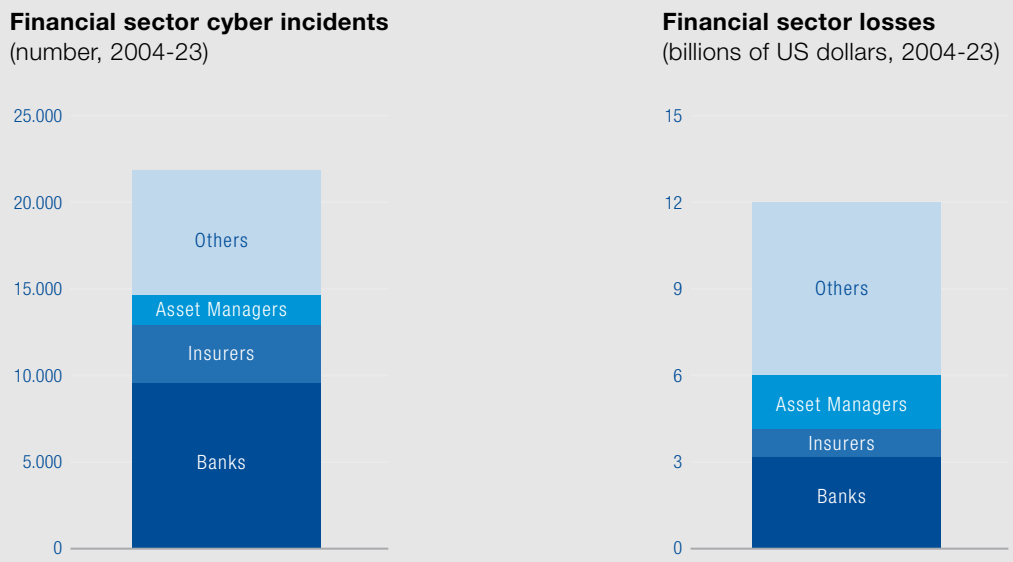
The growing threat is exemplified by high-profile incidents, such as the ransomware attack on Costa Rica's Finance Ministry and Brazil's court system, underscoring the need to address the proliferating threat. Moreover, only 7 of the 32 countries in the region have plans to protect their critical infrastructure, and just 20 have operational Computer Security Incident Response Teams (CSIRTs). As the global cyber-threat landscape matures, with a 34.5% rise in data breaches and an 84% increase in ransomware attacks in 2023, Latin America's cybersecurity challenges are increasingly urgent.[4]

The LATAM Threat Landscape research from Duke University, utilizing data from Recorded Future's Intelligence Graph, discusses the three principal threat-actor groups that are targeting the Latin American financial sector and the suggested controls that can be implemented to avert cyber attacks and mitigate their impact. The extensive data analysis ultimately identified five aggressive threat actors: CL0P, LockBit, Mispadu, Horabot, and Mispadu.

Cyber breaches have become increasingly common in Latin American financial institutions, with distinct cybersecurity challenges. Data from 2023 reveals that Latin American countries experience the highest rate of ransomware attacks on organizations, with 79% of incidents involving ransomware, compared to the global average of 53%.[5] This report explores the approaches and motivations of key threat actors—CL0P, Mispadu, Horabot, Blind Eagle, and LockBit—and the finding that these threat actors utilized similar TTPs.

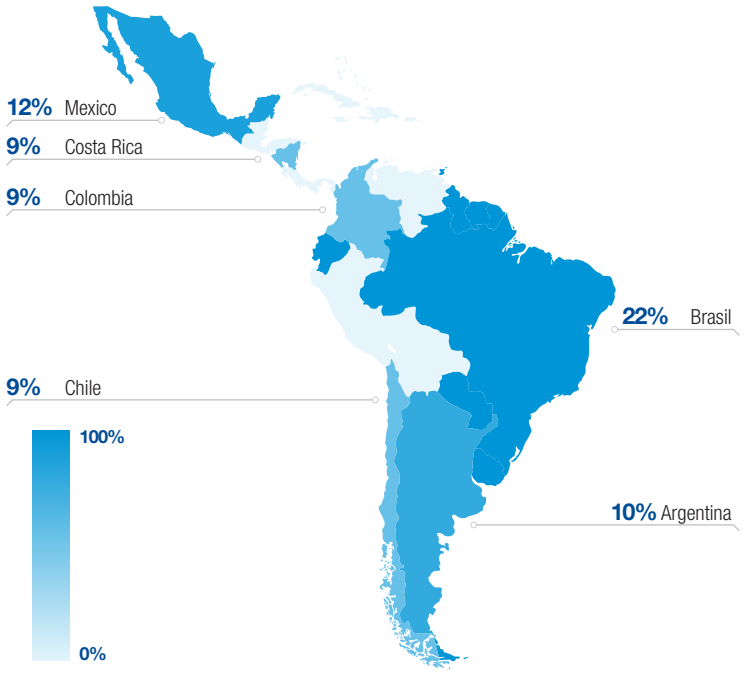
[1] https://www.itu.int/en/ITU-D/Cybersecurity/pages/global-cybersecurity-index.aspx
[2] https://www.itu.int/en/ITU-D/Cybersecurity/pages/global-cybersecurity-index.aspx
[3] https://www.americasquarterly.org/article/new-aq-hackers-paradise-why-latin-america-is-so-vulnerable/#:~:text=%E2%80%9CLatin%20America's%20entrepreneurial%20and%20innovative,cyberbreaches-%20start%20from%20human%20error.
[4] https://go.flashpoint.io/2024-global-threat-intelligence-report-download
[5] https://www.ptsecurity.com/ww-en/analytics/latam-cybersecurity-threatscape-2022-2023- en/

Figure 1: Financial Sector Cyber Incidents and Losses



The Latin America region presents vulnerabilities within financial institutions that are unique within the global landscape and require careful consideration. Primary target countries for threat-actor groups include Brazil, Mexico, Argentina, Colombia, and Peru. These countries accounted for 50% of the victim countries that attackers targeted in 2023, with 12% of the total cyber attacks in the world occurring in Latin America.[6]

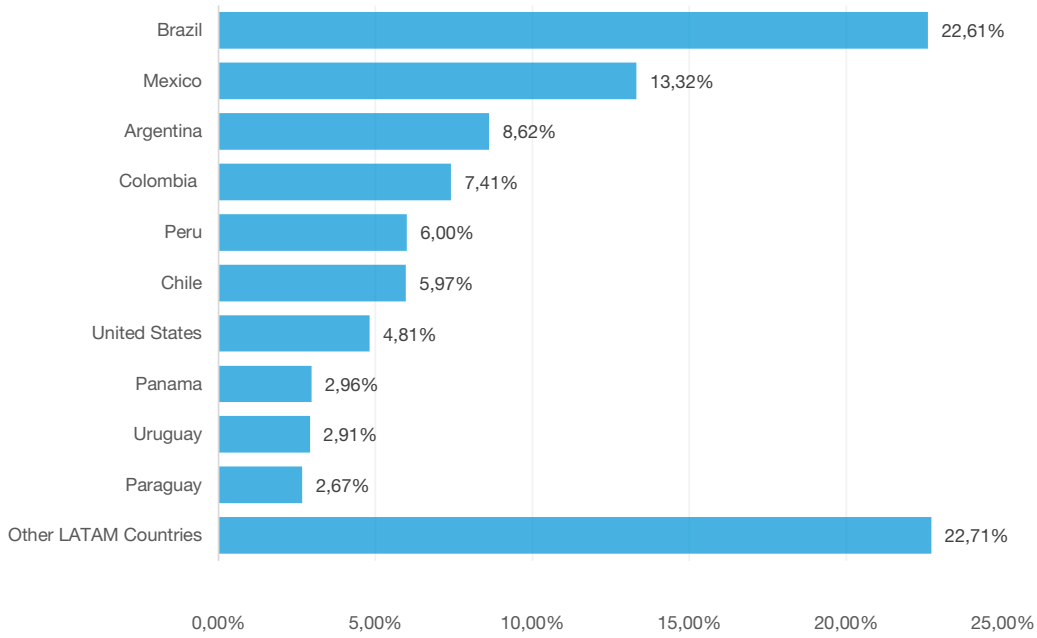
Figure 2: Distribution of Successful Attacks in Latin America



In 2023, LATAM faced 1,498 ransomware attacks and 6,048 phishing attacks by 33 distinct groups (SOCRader, 2024, pp. 4–5).[7] Insufficient investment in cybersecurity, volatile economies, and a highly unregulated environment are believed to have magnified institutional risks.

[6] https://www.ibm.com/reports/threat intelligence
[7] https://doi.org/CyberThreatIntelligenceAnalysis

Figure 3: Distribution of Dark Web Threats by Primary Target Country



The data gathered to create this report offers a broad understanding of the evolving threat landscape while considering the limitations of open-source intelligence, such as labor-intensive processes, limited effectiveness, and the potential to overlook smaller threats when prioritizing higher-profile threat actors.[8] This report provides vital observations to improve recommendations on cybersecurity defenses that can create a more resilient Latin American financial ecosystem.

The LATAM financial services sector should consider the use of a cybersecurity defense strategy that is threat-actor informed to mitigate impacts from cyber attacks. Organizations from the financial services industry that use an informed strategy can prepare themselves for common tactics, techniques, and procedures (TTPs) used by threat actors. By reviewing and incorporating the mapped TTPs that these threat-actor groups use, cyber defenders can more effectively implement cybersecurity controls.

[8] https://www.ptsecurity.com/ww-en/analytics/latam-cybersecurity-threatscape-2022-2023-en/

Table of Contents

1 Introduction

In recent years, the financial sector in Latin America has undergone a rapid digital transformation, fueled by the expansion of fintech services, increased internet penetration, and a growing demand for digital banking. However, this technological progress has outpaced the development of robust cybersecurity practices, leaving financial institutions increasingly vulnerable to sophisticated cyber threats. As cybercrime becomes more organized and opportunistic, the financial sector, which is already a high-value target, faces heightened risks that threaten economic stability, consumer trust, and national security.

This paper investigates the cybersecurity landscape of the Latin American financial market, with a particular focus on the actors, methods, and systemic vulnerabilities that define the region's current risk posture. Drawing on threat intelligence data, regional case studies, and insights from security researchers, this study seeks to analyze the motivations and tactics of prominent threat actors targeting Latin American financial systems. It also explores the structural challenges such as regulatory gaps, talent shortages, and underinvestment that hinder effective cybersecurity defense.

The objective of this research is twofold: first, to provide a comprehensive overview of the evolving threat environment facing financial institutions in Latin America, and second, to recommend practical, threat-informed strategies for improving cyber resilience in the region. Particular emphasis is placed on the activities of five major threat actor groups—CL0P, LockBit, Mispadu, Blind Eagle, and Horabot—whose operations exemplify broader trends in cybercrime targeting the financial sector.

The following sections of this paper are organized as follows: Section 2 outlines the threat landscape and introduces the key cybercriminal groups active in the region, as well. Section 3 evaluates the region's cybersecurity readiness, institutional vulnerabilities, and national response strategies. Section 4 highlights the regulatory gaps that currently exist in Latin America. Section 5 dives into 5 different APTs, their activity in the region, their TTPs, and recommendations to organizations on how to deal with these threats. Finally, Section 6 provides a series of strategic recommendations for cybersecurity in Latin America's financial sector.

1.1 Objectives

The research team evaluated open-source data from the Recorded Future platform to form an assessment of how different threat-actor groups might use similar TTPs when attacking financial services firms in LATAM. This report offers analysis with four primary objectives:

(1) Identifying major threat-actor groups targeting Latin American financial institutions and their operational bases.

(2) Analyzing the TTPs employed by these threat actors.

(3) Assessing the impact of their targeting strategies on financial institutions in the region.

(4) Formulating actionable recommendations for mitigating the identified TTPs, leveraging the MITRE ATT&CK framework and insights for cybersecurity professionals.

2 Background

Cyber attacks on financial institutions in Latin America have significantly increased over the past five years, reflecting the global trend of rising cyber threats, which have grown at an annual rate of 25% over the past decade, as of 2024.[9] According to the 2024 Global Financial Stability Report,[10] the risk of extreme cyber-related losses has more than quadrupled since 2017, reaching $2.5 billion. Furthermore, the 2024 LATAM CISO Report highlights that countries such as Costa Rica, Mexico, Brazil, and Argentina attribute the frequency and success of these attacks to gaps in response preparedness. These gaps ranged from deficiencies in technical capabilities to communication breakdowns between public- and private-sector entities between 2020 and 2025. Only about half of the countries surveyed had a national cybersecurity strategy specifically focused on the financial sector or had implemented dedicated cybersecurity regulations.

Consequently, Latin America alone accounted for 12% of the total cyber attacks worldwide in 2022, surpassing the Middle East and Africa, which comprised 7%, despite being comparably under-resourced.[11] Attackers primarily targeted organizations and individuals in Brazil, Mexico, and Argentina, which together accounted for 44% of all attacks. These countries have the largest economies and financial institutions in Latin America, making them attractive targets for cybercriminals.[12] As cyber incidents continue to rise, the region's financial stability is increasingly at risk given that financial institutions are among the key targets for cyber-threat actors and constitute a significant portion of the target sectors. The financial and insurance sector alone accounts for 39.47% of disclosed cyber incidents in Latin America.[13] If left unaddressed, these threats could lead to severe economic repercussions, highlighting the need for robust cybersecurity measures.

2.1 Miseducation Regarding Threats

Latin American financial institutions face heightened susceptibility to cyber attacks due to a combination of factors, which include the following.

1. A lack of cybersecurity awareness and training within financial institutions: The primary challenge is not only a general lack of cybersecurity awareness but a training and learning gap within financial institutions. Employees need comprehensive cybersecurity training, while consumers require awareness campaigns against potential cyber threats.

2. The absence of cybersecurity standards and regulations, which leaves many financial institutions vulnerable to cyber threats: Organizations choose not to implement the Cybersecurity Framework (NIST CSF) or ISO 27001 frameworks voluntarily, leaving themselves exposed to cyber attacks from threat-actor groups that must find only one vulnerability to compromise a victim company.

3. Insufficient investment in technology at hardware and software levels: The use of outdated software creates security gaps in critical infrastructure and weakens the region's defenses against cyber attacks. The technological disparity between Latin American countries and their more developed counterparts in North America and Europe exacerbates these vulnerabilities, making it more difficult for the region to effectively counter sophisticated cyber threats.[14]

The financial impact of cybersecurity breaches has been staggering worldwide. According to IBM Security, “the average data breach cost in 2020 was estimated at $3.86 million" including the cost of legal fees, compliance fines, reputational damage, and loss of customer trust.[15] In May 2021, the Colonial Pipeline ransomware attack crippled fuel distribution across the United States, disrupting critical infrastructure and causing widespread shortages. The attack, attributed to the DarkSide ransomware group, forced the company to halt operations, leading to panic-buying and fuel-price surges. In response, Colonial Pipeline paid a $4.4 million ransom to regain access to its systems, but the economic repercussions persisted long after, such as supply-chain disruptions and heightened regulatory scrutiny.[16] This incident exposed critical cybersecurity vulnerabilities in industrial control systems, highlighting the urgent need for stronger cybersecurity frameworks and proactive risk-mitigation strategies to prevent similar large-scale attacks.

[9] https://blogs.worldbank.org/en/latinamerica/seguridad-cibernetica-en-america-latina-y-el-caribe
[10] https://www.ptsecurity.com/ww-en/analytics/latam-cybersecurity-threatscape-2022-2023-en/
[11] https://www.ibm.com/reports/threat-intelligence
[12] https://www.statista.com/statistics/802640/gross-domestic-product-gdp-latin-america-caribbean-country/
[13] https://blogs.worldbank.org/en/latinamerica/seguridad-cibernetica-en-america-latina-y-el-caribe
[14] 10.3390/informatics10030071 10.47460/athenea.v3i9.43
[15] https://www.ibm.com/reports/threat intelligence
[16] https://www.cnn.com/business/live-news/us-cyberattacks-cybersecurity-06-08-21/index.html

The vulnerabilities exploited in the Colonial Pipeline attack, and the resulting harm, highlight Latin America's susceptibility to cyber threats due to insufficient regulatory frameworks, weaker cybersecurity infrastructure, and lower business and consumer awareness, which cybercriminals manipulate for financial gain. Latin America has the highest percentage of ransomware attacks at 79% compared to the global average of 53%, with 94% of attacks attributed to system intrusion, social engineering, and basic web-application attacks.[17] The average cost of a data breach has risen to USD 4.45,[18] and to the highest since 2020 at USD 2.46M in Latin America.[19] Latin America has the lowest levels of cybersecurity preparedness, making it the most susceptible to attacks according to the 2020 Global Cybersecurity Index.[20] This will continue to impact the region's economy.

2.2 Historical Ransomware Vulnerabilities

2.2.1 Introduction

The Latin American financial sector experienced a significant surge in sophisticated cyber attacks between 2018 and 2024, highlighting critical vulnerabilities in the region's digital infrastructure. This analysis examines 12 major incidents that targeted banks, financial institutions, and government systems across Chile, Brazil, Mexico, Argentina, and other Latin American countries. The attacks, ranging from the $10 million Banco de Chile heist in 2018 [21] [22] to the 2024 Bankingly data leak affecting 135,000 clients,[23] demonstrate an evolving threat landscape dominated by ransomware and advanced persistent threat (APT) groups.

The investigation reveals a concerning pattern: attackers increasingly target third-party service providers and financial-technology platforms to breach multiple institutions simultaneously. Organizations increasingly rely on various third-party providers, exposing them to distinct cyber risks. Software and SaaS (Software as a Service) providers face vulnerabilities and supply-chain attacks, where flaws in widely used applications, such as Progress Software's Managed File Transfer solution, can lead to mass data exfiltration.[24] Likewise, Infrastructure as a Service environments can present risks due to misconfigurations, access-control weaknesses, and service outages, potentially disrupting business operations. The Bankingly breach, involving a SaaS-based digital fintech platform, compromised seven Latin American banks due to misconfigured storage buckets lacking proper authentication, exposing sensitive customer data.[25] These incidents highlight the need for stronger third-party risk management, continuous monitoring, and zero-trust security models to mitigate cascading threats.

Most attacks followed a similar pattern: initial compromise through phishing or vulnerable systems, lateral movement through networks, data exfiltration, and often deployment of ransomware. The financial impact of these incidents is substantial, with losses exceeding 1% of some countries' GDP and potentially rising to 6% if critical infrastructures are targeted.[26] A 1% GDP loss from cybercrime equates to USD 25 billion for Brazil, USD 15 billion for Mexico, and USD 6.1 billion for Argentina, while a 6% loss could reach USD 150 billion, USD 90 billion, and USD 36.6 billion, respectively. Smaller economies such as Chile ($3.9B–$23.5B) and Colombia ($3.2B–$19.3B) also face major risks.[27] With Brazil, Mexico, and Argentina among the hardest hit, cyber attacks threaten business continuity, investor confidence, and long-term economic stability across the region. The scale of potential economic damage underscores the urgent need for strengthened cybersecurity measures, particularly in third-party risk management and critical-infrastructure protection within Latin America's financial sector.

[17] https://latinlawyer.com/guide/the-guide-corporate-compliance/fifth-edition/article/mitigating risk-data-breaches-and-cyber-incidents-surge-in-latin america#:~:text=Globally%2C%20the%20average%20cost%20of,regions%20included%20in%2 0the%20report.
[18] https://latinlawyer.com/guide/the-guide-corporate-compliance/fifth-edition/article/mitigating risk-data-breaches-and-cyber-incidents-surge-in-latin america#:~:text=Globally%2C%20the%20average%20cost%20of,regions%20included%20in%2 0the%20report
[19] https://www.americaeconomia.com/en/business-industries/cybersecurity-new-center-concern latin-american-companies
[20] https://www.cisa.gov/news events/cybersecurity-advisories/aa23-158a
[21] https://www.trendmicro.com/en_us/research/18/f/new-killdisk-variant-hits-latin-american-financial-organizations-again.html
[22] https://www.zdnet.com/article/north-korea-s-apt38-hacking-group-behind-bank-heists-of-over-100-million/
[23] https://cybernews.com/security/bankingly-dataleak/#:~:text=On%20May%2024th%2C%20the,anyone%20online.&text=identified%20seven%20Azure%20 Blob,anyone%20online.&text=authentication.%20The%20misconfiguration%20exposed,anyone%20online.&text=of%20ne arly%20135%2C000%20 clients,anyone%20online
[24] https://unit42.paloaltonetworks.com/threat-brief-moveit-cve-2023-34362/
[25] https://cybernews.com/security/bankingly-dataleak/#:~:text=On%20May%2024th%2C%20the,anyone%20online.&text=identified%20seven%20Azure%20 Blob,a nyone%20online.&text=authentication.%20The%20misconfiguration%20exposed,anyone%20online.&text=of%20nearly%20135%2C000%20 clients,anyone%20online
[26] https://latam.cs4ca.com/wp-content/uploads/2024-Annual-Report-The-State-of-OT-Cyber-Security-in-LATAM.pdf
[27] https://www.statista.com/statistics/802640/gross-domestic-product-gdp-latin-america-caribbeancountry/#:~:text=In%202024%2C%20Brazil%20 and,and%20the&text=were%20expected%20to%20be,and%20the&text=countries%20with%20the%20largest,and% 20the&text=domestic%20product%20 %28GDP%29%20in,and%20the

2.2.2 Vulnerability Pattern Analysis

This section analyzes prevalent technical vulnerabilities, industry-specific weaknesses in the financial sector, and regional security challenges, providing organizations with insights into common risk patterns. By understanding these vulnerabilities, businesses can identify gaps in their security posture and implement proactive defenses. The findings in this section aim to help organizations recognize recurring vulnerability patterns, understand their potential business impact, and take preemptive actions to mitigate risks before they escalate into security incidents. Section 6: Strategic Recommendations, at the end of this paper, provides actionable remediations to address these vulnerabilities effectively.

Commonly Observed Technical Vulnerabilities:

- Weak network segmentation
- Insufficient internal-access controls
- Inadequate incident-response protocols
- Employee susceptibility to social engineering
- Over-reliance on legacy systems
- Weak third-party security
- Limited monitoring of internal transactions

Industry-Specific Patterns and Vulnerabilities (Finance):

- Inadequate network segmentation between critical systems
- Weak access controls on internal networks
- Insufficient authentication on the systems of third-party service providers
- Vulnerable public-facing infrastructure
- Sophisticated banking trojans using legitimate authorities to deceive users

Region-Specific Patterns and Vulnerabilities:

- Heavy reliance on social engineering targeting regional trust in financial authorities
- Sophisticated phishing campaigns exploiting tax-related concerns
- Cross-border nature of banking operations creating security inconsistencies
- Widespread adoption of digital banking in rural areas through potentially vulnerable channels
- Centralized payment-processing systems (like Brazil's SPEI) becoming high-value targets[28]

2.2.3 Gap Analysis and Future Impact

This section examines key cybersecurity gaps in Latin America, focusing on their root causes, recent improvements, and anticipated future risks. The analysis highlights systemic issues, such as underinvestment, outdated infrastructure, and insufficient collaboration, all of which contribute to persistent security challenges. By reviewing past incidents and their impact on financial institutions, organizations can better understand evolving threats. Additionally, this section explores emerging risks from AI-driven cyberattacks, supply-chain vulnerabilities, and geopolitical risks. Section 6: Strategic Recommendations, at the end of this paper provides concrete solutions to address these vulnerabilities and strengthen regional cybersecurity resilience.

Root-Cause Analysis:

1. Chronic underinvestment in cybersecurity: Latin America faces significant cybersecurity vulnerabilities due to underinvestment.[29] According to the Organization of American States (OAS), Latin American countries allocate <1% of GDP to cybersecurity infrastructure,[30] leaving financial systems vulnerable to advanced attacks. The region has the lowest average cybersecurity score globally, at 10.2 out of 20.[31]

2. Insufficient cross-border collaboration: There is a lack of harmonization between national laws, creating challenges for multinational companies.[32] However, recent efforts, such as the EU-LAC Digital Alliance, aim to strengthen bi-regional partnerships.[33]

3. Outdated infrastructure and software: Many companies still operate with outdated systems or use pirated software, leaving gaps that attackers can easily exploit.[34]

4. Cybersecurity skills gap: There is an urgent need for upskilling current teams and fostering the next generation of cybersecurity professionals.[35]

5. Inadequate legislation and enforcement: Cybersecurity laws in some countries are either outdated or poorly enforced. Only three out of 21 countries in Latin America have a defined national digital-security strategy.[36]

6. Lack of public awareness: Many Latin American countries have not yet widely publicized the dangers of the internet. There is a lack of preventative programs despite some countries adopting national cyber strategies.[37]

[28] https://www.wired.com/story/mexico-bank-hack/
[29] https://www.centerforcybersecuritypolicy.org/insights-and-research/insights-from-the-annual-latam-ciso-summit-costa-rica
[30] https://grcoutlook.com/cybersecurity-risks-latin-america-versus-asia-a-rising-concern/
[31] https://blogs.worldbank.org/en/latinamerica/seguridad-cibernetica-en-america-latina-y-el-caribe
[32] https://www.wired.com/story/mexico-bank-hack/
[33] https://www.eeas.europa.eu/eeas/europe-and-latin-america-caribbean-step-cooperation-cybersecurity_en
[34] https://www.datto.com/blog/ransomware-and-cybersecurity-in-latin-america/
[35] https://www.centerforcybersecuritypolicy.org/insights-and-research/insights-from-the-annual-latam-ciso-summit-costa-rica
[36] https://www.wired.com/story/mexico-bank-hack/
[37] https://latam.cs4ca.com/wp-content/uploads/2024-Annual-Report-The-State-of-OT-Cyber-Security-in-LATAM.pdf

2.2.4 Security-Posture Improvements from 2018 to Present

The security posture of Latin American financial institutions has significantly transformed between 2018 and 2024. In 2018, as evidenced by the Banco de Chile attack, financial institutions primarily relied on reactive security measures, such as system disconnection, forensic investigation after the breach, and restoration from backups. The bank was unaware of the malware in its systems until it was faced with the KillMBR alert, which caused a widespread system shutdown. Compared to best practices, such as proactive threat detection, network segmentation, and real-time monitoring, the bank's incident response lacked early threat identification, precise containment, and security controls to prevent financial loss.[38]

The case of Mexico's SPEI system in 2018 further highlighted the prevalent weak network segmentation and limited monitoring capabilities of the era.[39] The heist exposed severe vulnerabilities in the Sistema de Pagos Electrónicos Interbancarios (SPEI) system, with hackers identified as part of the APT38 group, a financially motivated threat-actor group believed to be backed by North Korea.[40] APT38 infiltrated the banking networks, compromised endpoints handling SPEI transactions, and injected fraudulent payment requests. Exploiting weak network security, including poor network segmentation and access controls, they were able to alter transfer instructions without triggering immediate alarms, ultimately stealing USD 15–20 million and moving the funds to mule accounts before laundering them internationally.[41]

As of 2024, the security landscape of Latin American financial institutions has advanced significantly, with organizations adopting more structured incident-response protocols and improving coordination through national CERT teams. A notable example is the Chilean Customs' swift containment of the Black Basta ransomware attack, demonstrating enhanced response capabilities and collaboration.[42] However, despite these advancements, financial institutions continue to grapple with an evolving threat landscape driven by rapid digitalization, increased interconnectivity, and emerging vulnerabilities in third-party SaaS and software integrations.

A prime example is the 2024 Bankingly breach, which affected 135,000 clients across multiple LATAM countries, exposing critical data due to misconfigurations in Azure Blob Storage.[43] The breach was traced back to misconfigured Azure Blob Storage buckets used by Bankingly to store customer data. These misconfigurations left the data exposed to unauthorized access, highlighting significant vulnerabilities in third-party integrations and cloud-service configurations.[44]

Similarly, the Banco Português de Gestão data leak, caused by a misconfiguration in Nearsoft's systems, exposed highly sensitive client financial data due to missing authentication controls. Alarmingly, Nearsoft failed to comply with critical security standards like ISO 27001 and PCI DSS, leaving data unencrypted and vulnerable to unauthorized access.[45] These incidents highlight persistent security gaps stemming from poor risk management, cloud misconfigurations, and inadequate vendor oversight. As such, they underscore the risks associated with modern digital infrastructure. While financial institutions have strengthened defenses, such incidents reveal that security misconfigurations and insufficient oversight remain key weaknesses. Addressing these gaps will be essential to mitigating future risks and maintaining a strong security posture in an increasingly digital financial ecosystem.

2.2.5 Future Impact Analysis

1. AI-driven Cyber Attacks: Threat actors are increasingly leveraging AI to create destructive malware, sophisticated phishing campaigns, convincing deep fakes, and advanced cyberespionage operations that exploit infrastructure vulnerabilities.[46] The primary challenge when tackling these sophisticated attacks is the critical shortage of professionals with specialized expertise to understand and design appropriate risk-management frameworks. Success depends on building technical competency to effectively assess and mitigate these sophisticated, emerging threats through proper governance and controls.

[38] https://www.infosecurity-magazine.com/news/bank-of-chile-suffers-10m-loss/
[39] https://latam.cs4ca.com/wp-content/uploads/2024-Annual-Report-The-State-of-OT-Cyber-Security-in-LATAM.pdf
[40] https://attack.mitre.org/groups/G0082/
[41] https://latam.cs4ca.com/wp-content/uploads/2024-Annual-Report-The-State-of-OT-Cyber-Security-in-LATAM.pdf
[42] https://therecord.media/chile-black-basta-ransomware-attack-customs-department
[43] https://cybernews.com/security/bankingly-dataleak/#:~:text=On%20May%2024th%2C%20the,anyone%20online.&text=identified%20seven%20Azure%20Blob,anyone%20online.&text=authentication.%20The%20misconfiguration%20exposed,anyone%20online.&text=of%20ne arly%20135%2C000%20clients,anyone%20online
[44] https://cybernews.com/security/bankingly-dataleak/#:~:text=On%20May%2024th%2C%20the,anyone%20online.&text=identified%20seven%20Azure%20Blob,anyone%20online.&text=authentication.%20The%20misconfiguration%20exposed,anyone%20online.&text=of%20ne arly%20135%2C000%20clients,anyone%20online
[45] https://cybernews.com/security/banco-portugues-de-gestao-data-leak/
[46] https://insightcrime.org/news/four-ways-ai-is-shaping-organized-crime-in-latin-america/

2. Exploitation of Digital-Transformation Vulnerabilities: As Latin American countries promote further digitization to foster socioeconomic growth, they become more vulnerable to cyber criminals. The increased use of technology also escalates the potential for attacks.[47]

3. Supply-Chain Vulnerabilities: Notably, 54% of large organizations identified supply-chain challenges as the biggest barrier to achieving cyber resilience. The increasing complexity of supply chains, coupled with a lack of visibility into the security levels of suppliers, has emerged as a leading cybersecurity risk.[48]

4. Geopolitical Influences: Geopolitical tensions are contributing to a more uncertain cybersecurity environment. For example, 97% of organizations saw an increase in cyber threats since the start of the Russia–Ukraine war in 2022, demonstrating the profound effect of geopolitical tensions on cybersecurity.[49]

5. Regional Disparities: Latin America is projected to experience a greater increase in cyberattacks than other regions. In Q2 2024, cyber attacks increased by 53% year-over-year in Latin America, and this trend is likely to continue.[50]

2.3 Ransomware Losses for the Financial Services Industry

As of 2024, the financial services industry in LATAM has become a primary target for ransomware attacks, reflecting a broader trend of escalating cyber threats in the region. Brazil, Mexico, and Chile have been the hardest-hit countries, with ransomware groups such as LockBit 3.0, Akira, and Play being identified as the actors behind the attacks. These groups leverage sophisticated methods, including exploiting vulnerabilities in software and deploying ransomware-as-a-service (RaaS) models. The financial losses attributed to ransomware incidents in the LATAM financial sector are estimated to exceed hundreds of millions of dollars in 2024 as organizations face costs related to ransom payments, data recovery, operational downtime, and reputational damage. This surge in attacks underscores the critical need for robust cybersecurity measures within the region's financial institutions.

2.3.1 Case Study 1 - LockBit 3.0's Targeted Attack on a Brazilian Bank

In July 2024, the LockBit 3.0 ransomware group conducted a highly targeted attack against a major Brazilian financial institution. The attackers exploited a vulnerability in the bank's virtual-desktop infrastructure to gain unauthorized access and encrypt critical operational files. To further pressure the victim, LockBit 3.0 threatened to publish sensitive stolen data on dark-web forums unless the institution complied with their ransom demand of $2.5 million in Bitcoin.

The attack resulted in significant operational and financial damage. The bank experienced a prolonged downtime of online banking services, disrupting customer transactions and access to accounts. This not only eroded customer trust but also subjected the institution to regulatory scrutiny. Additionally, the financial costs extended beyond the ransom demand to include expenses for system recovery, forensic investigations, and public-relations efforts to restore its reputation.

2.3.2 Case Study 2 - Play Ransomware's Attack on a Chilean Financial Firm

Also in July 2024, the Play ransomware group targeted a Chilean financial firm by deploying a Linux variant specifically engineered to exploit VMware ESXi environments. The attackers infiltrated the firm's virtualized infrastructure, encrypted critical server data, and left a ransom note demanding $1.8 million in cryptocurrency.

The attack caused extensive financial and operational repercussions for the firm. In addition to the ransom demand, the organization incurred costs related to restoring its IT systems and

reinforcing its cybersecurity defenses. The incident also resulted in reputational harm, as clients and partners expressed concerns over the firm's ability to protect sensitive data. These cumulative losses further underscored the growing threat of ransomware to the LATAM financial services sector.

In conclusion, ransomware remains a pressing and escalating threat to the financial services industry in LATAM, with countries such as Brazil, Chile, and Mexico emerging as primary targets in 2024. Ransomware groups such as LockBit 3.0 and Play have demonstrated increasing sophistication by exploiting vulnerabilities in virtualized infrastructures and leveraging RaaS models to scale their operations. The financial losses incurred far surpass ransom payments, encompassing system restoration, downtime, and reputational damage,

[47] https://grcoutlook.com/cybersecurity-risks-latin-america-versus-asia-a-rising-concern/
[48] https://www.weforum.org/publications/global-cybersecurity-outlook-2025/digest/
[49] https://www.accenture.com/content/dam/accenture/final/accenture-com/document/Accenture-State-Cybersecurity.pdf
[50] https://blog.checkpoint.com/research/check-point-research-reports-highest-increase-of-global-cyber-attacks-seen-in-last-two-years-a-30-increase-in-q2-2024-global-cyber-attacks/

collectively amounting to hundreds of millions of dollars across the region. As the financial sector in LATAM continues to digitalize, organizations must prioritize comprehensive cybersecurity strategies, including vulnerability management, employee training, and advanced threat-detection systems, to mitigate the impact of these pervasive attacks. The resilience of the financial services sector hinges on proactive measures to counteract the evolving tactics of ransomware operators.

2.4 Ransomware Response Capabilities

The growing trend of ransomware attacks across LATAM has exposed critical gaps in regional response capabilities that create immediate vulnerabilities for the financial services sector. This section examines how institutional frameworks, technical capabilities, and coordination mechanisms in LATAM contribute to elevated ransomware risk exposure for financial institutions.

2.4.1 Regional Response Infrastructure Assessment

Recent comparative data, including Fortinet's Global Ransomware Report, reveals important nuances in LATAM's response capabilities relative to other regions.[51] [52] [53] While Latin American organizations demonstrate stronger capabilities in rapid attack detection and social-engineering resistance[54], this relative strength in detection capabilities should be contextualized within the broader regional infrastructure limitations. Namely, the data suggests that while individual enterprise capabilities may be developing, systemic response infrastructure gaps persist. The uneven disclosure landscape and limited number of LATAM countries with established plans for critical-infrastructure protection (let alone in the financial services sector) is evidence of this gap.

One 2022 study introduces a comprehensive cybersecurity disclosure index examining practices across major LATAM markets between 2016 and 2020 on a 0–1 scale. The research developed a 27-element framework across four dimensions: governance (5 elements), strategy (6 elements), risk management (13 elements), and financial implications (3 elements). These dimensions were based on international standards, including ISO 27000; SEC guidelines; GDPR; and frameworks from OECD, IDB, OAS, and GRI.[55]

The research reveals a complex landscape of cybersecurity disclosure in LATAM's financial sector, with financial institutions maintaining the highest disclosure levels across sectors, increasing from 0.28 in 2016 to 0.52 in 2020.[56] This leadership position is particularly evident in Argentina, where financial institutions comprise 57% of sampled companies, with 86% filing SEC Form 20-F reports.[57] However, despite this relative maturity, significant governance disclosure gaps persist. While board involvement in cybersecurity supervision improved from 0.18 in 2016 to 0.53 in 2020, specialized committee disclosure remained weak at 0.24 in 2020, and the oversight disclosure of audit committees scored only 0.20.[58]

The governance gap is particularly concerning given the evolution of financial malware exploiting regional and institutional contexts, such as specific banking implementations. By conducting a longitudinal study of Brazilian financial malware between 2012 and 2020, researchers revealed how malicious tactics rapidly evolve based on new attack opportunities. For example, threat actors are curating social engineering and malware scripts to local banking contexts that diverge from global or historical trends (e.g., malware targeting PIN-based credit cards, Brazilian Portuguese VBE code).[59] Ransomware is no exception to these evolving tactics. Therefore, setting risk tolerance at the highest level through board-level cybersecurity governance is necessary to ensure local countermeasures are context-aware (i.e., attentive to geographic and enterprise characteristics).

Other concerns include findings regarding risk-management disclosure (0.40 in 2020); alignment with international security standards (0.39 in 2020); and ongoing cybersecurity-investment disclosure, improving only from 0.02 in 2016 to 0.21 in 2020.[60] These scores suggest that, while financial institutions may have security frameworks in place, they struggle to effectively communicate their security investments and alignment with international standards. The research identifies clear correlations between regulatory frameworks and disclosure quality, with early adopters of data-protection laws and national cybersecurity strategies, such as Argentina (2016) and Brazil (2018), showing stronger financial sector disclosures than countries like Peru, where lower disclosure scores (0.25 in 2020) correlate with the absence of a national strategy.[61]

[51] https://www.fortinet.com
[52] https://doi.org/10.1145/3429741
[53] https://doi.org/10.3390/su14031390
[54] https://www.fortinet.com
[55] https://doi.org/10.3390/su14031390
[56] https://doi.org/10.3390/su14031390
[57] https://doi.org/10.3390/su14031390
[58] https://doi.org/10.3390/su14031390
[59] https://doi.org/10.1145/3429741
[60] https://doi.org/10.3390/su14031390
[61] https://doi.org/10.3390/su14031390

The trends suggest a broader pattern: while LATAM financial institutions lead in cybersecurity disclosure compared to other sectors, their performance varies significantly based on regulatory maturity and national cybersecurity frameworks. The sector's critical role in national infrastructure and international financial networks makes these gaps particularly concerning, suggesting a need for more standardized disclosure practices and improved alignment with international standards across the region.

The comprehensive nature of the research findings indicates significant implications for ransomware incident-response capabilities across LATAM financial institutions. The disparity between strategic disclosure scores (0.53) and operational risk-management scores (0.40) suggests potential vulnerabilities in actual incident-response execution.[62] Of particular concern are the low scores for the disclosure of incident-response procedures (0.36) and monitoring effectiveness (0.47). These scores indicate potential gaps in operational response capabilities that could directly impact an institution's ability to detect, contain, and recover from ransomware attacks.[63] When combined with the previously discussed findings about disclosure practices and regulatory frameworks, these gaps suggest that, while LATAM financial institutions may have basic ransomware response plans in place, their actual operational readiness for complex attacks may be insufficient.

This supposition is well-founded. The Inter-American Development Bank reports that only seven of the 32 Latin American countries have established plans for critical-infrastructure protection, while just 20 have operational CSIRTs.[64] This fragmented response landscape has created specific challenges for financial institutions operating across borders. For example, this rift was particularly acute during Colombia's September 2023 ransomware incident, where the blast radius spread to financial entities in Argentina, Panama, and Chile due to limited coordination mechanisms.[65]

2.4.2 Technical Response Capabilities and Resource Constraints

While LATAM organizations demonstrate stronger initial detection capabilities, there are significant regional variations in technical readiness that create vulnerabilities. For instance, the Costa Rica 2022 ransomware emergency reveals how relative detection advantages can be undermined by subsequent response limitations. Even after detection, the Costa Rican government spent approximately $24 million on response operations, with the rehabilitation phase alone costing the Social Security Fund over $18 million.[66] This scale of impact suggests that the full response cycle faces significant constraints. One of these constraints includes cross-sector disparities in technical readiness.

Based on empirical data for 2020, LATAM financial institutions' cybersecurity disclosure patterns indicate that investments are heavily weighted toward strategic initiatives like security-management systems (scoring 0.68) and awareness programs (scoring 0.72). Critical operational elements like incident-response procedures scored only 0.36, and testing/monitoring activities reached just 0.47.[67]. A best-practice model would demonstrate balanced investment and maturity across both strategic and operational domains. For example, rather than only reporting the broad adoption of security-management systems, institutions should demonstrate concerted investments in incident detection and response capabilities, regular penetration testing and vulnerability assessments, and quantifiable metrics for security-program effectiveness. Disclosure should show security investments being distributed across critical operational areas, including toward detection and response infrastructure, continuous testing and monitoring, and threat intelligence and proactive defense capabilities. This would reflect a security program focused on tangible risk reduction rather than only policy compliance, with clear metrics demonstrating the operational impact of security investments.

This disparity between strategy and implementation is also evident in resource-allocation patterns beyond the private sector. Compared to LATAM financial services providers, the public sector shows a notably lower implementation of general security best practices than private-sector institutions.[68] This can create potential vulnerabilities in the broader financial ecosystem, where public and private systems are interconnected.[69] Additionally, documented resource-allocation challenges could impact future ransomware response capabilities. While organizations in North America and Europe, the Middle East, and Africa are planning more substantial

[62] https://doi.org/10.3390/su14031390
[63] https://doi.org/10.3390/su14031390
[64] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
[65] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
[66] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
[67] https://doi.org/10.3390/su14031390
[68] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
[69] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf

investments in zero trust network access (ZTNA) tools, LATAM organizations report more constrained security investment plans.[70] As both a proactive and reactive incident-response measure, ZTNA tools can micro-segment enterprise networks to contain ransomware, preventing lateral movement, data exfiltration, and unauthorized access to critical services through fine-grained default deny-access controls. Therefore, this investment gap could exacerbate existing limitations in response infrastructure, especially for financial institutions operating across regions that must maintain parity with global security standards while interfacing with both public- and private-sector systems.

As a multinational bank, Santander provides a prime example of this complexity. Santander's operations across LATAM, EU, and US markets illustrate the complex interplay between voluntary and mandatory cybersecurity disclosures. In Brazil, where the Global Cybersecurity Index shows the highest regional development score (97.68) and strongest legal measures (20.0), Santander must navigate both stringent local regulations and mandatory SEC Form 20-F reporting requirements.[71] This contrasts with their operations in Argentina, where the cybersecurity-maturity score is significantly lower (50.12), yet the bank still maintains SEC reporting obligations alongside less developed local disclosure frameworks.[72]

This disparity affects threat mitigation and incident response, particularly threat-intelligence and response coordination with public entities or critical service operators. In Brazil, Santander's disclosures reflect the country's robust bilateral and multilateral cooperation agreements (scoring 19.41 in cooperative measures), enabling more effective threat-intelligence sharing and incident coordination.[73] However, in Argentina, while SEC Form 20-F requirements ensure baseline cyber-risk reporting, the lower national cybersecurity-maturity score suggests potential gaps in local threat response coordination.

The bank's European operations face additional complexity through GDPR compliance requirements, which have influenced LATAM disclosure practices through what the researchers identify as the "adaptation of the European model of regulations related to data privacy".[74]This creates an interesting dynamic where Santander's LATAM operations often benefit from more stringent EU standards, particularly in countries like Brazil that have modeled their data- protection laws on European frameworks. The research shows this regulatory influence has generated increased standards and the dissemination of cybersecurity information across the region, though implementation varies significantly by country.[75]

This multi-jurisdictional reality requires Santander to maintain the highest common denominator in security practices while adapting disclosure approaches to meet varying regional requirements, from SEC Form 20-F compliance to EU GDPR standards to local regulatory frameworks. While institutions' overall security posture might theoretically benefit from meeting the highest common denominator of security requirements across all jurisdictions, practical implementation at the local level presents considerable challenges.

The varying institutional environments across LATAM nations create operational gaps in security implementation. For example, while Santander's Brazilian operations benefit from robust national frameworks and mature security infrastructure, their branches in neighboring countries may struggle to maintain equivalent capabilities due to resource constraints and less developed local security ecosystems. These disparities manifest in several critical areas: human-capital availability for security operations, advanced detection and logging capabilities, and incident-response coordination.

When organizations default to meeting minimum standards in regions with less mature frameworks, they risk creating security vulnerabilities that could impact their broader operational network. These disparities become particularly problematic in supply-chain security, where country-specific branches operating at different security maturity levels may create vulnerable entry points into the broader institutional network. Furthermore, when institutions must upgrade local operations to meet higher security standards—whether driven by SEC Form 20-F requirements or European GDPR compliance—they may find local resources insufficient to support the transition. This resource constraint becomes particularly acute in markets where both human capital and technical infrastructure for cybersecurity lag behind international standards.

[70] https://www.fortinet.com
[71] https://doi.org/10.3390/su14031390
[72] https://doi.org/10.3390/su14031390
[73] https://doi.org/10.3390/su14031390
[74] https://doi.org/10.3390/su14031390
[75] https://doi.org/10.3390/su14031390

2.4.3 Cross-Border Response Coordination

The interconnected nature of LATAM financial systems creates amplified risk from coordination deficiencies in cross-border response. While some bilateral agreements exist, such as between Costa Rica and Panama, comprehensive regional response frameworks remain limited.[76] Furthermore, LATAM's relative early-detection advantage may not translate into effective cross-border incident management.[77] The September 2023 attack on Colombia's internet service provider, IFX Networks, demonstrates this vulnerability, where despite patient-zero detection, the attack still spread to 78 additional public entities and 762 private companies across multiple countries.[78] While this blast radius can be attributed to many factors, including detection and remediation capabilities, it primarily demonstrates a widespread lack of third-party compromise procedures. Exacerbated by the government's inability to determine and disclose the extent of the affected entities, organizations were unable to sever or isolate compromised connections as part of their supply chains.[79]

2.4.4 Information-Sharing Mechanisms and Their Impact on Financial Sector Vulnerability

Significant limitations in regional information-sharing mechanisms can hamper financial institutions' ransomware response efforts. During Colombia's 2023 ransomware attack, the presidential advisor for digital transformation issued nine information bulletins before the event concluded. However, the lack of standardized cross-sector sharing protocols resulted in the uneven distribution of critical threat intelligence.[80] This gap in coordinated information sharing led to extended vulnerability windows where interconnected financial systems remained exposed.[81]

2.4.5 Variation in Public–Private Coordination Frameworks

There are substantial gaps in public–private coordination across most LATAM countries that directly impact financial sector resilience.[82]. For instance, while Ecuador has 14 CSIRTs dedicated to offering incident-response services to companies, there is no financial CSIRT.[83] Additionally, while these response teams span critical infrastructure and commercial domains such as the telecommunications and energy sectors, which could address some overlapping interests of the financial sector, they have no formal mechanism for communicating with each other.[84] As a regional financial hub, Panama also faces public–private coordination challenges with securing critical services. Despite launching the National Digital Agenda, the country is struggling to strengthen "sectoral interoperability platforms" and spur private investment in the digital ecosystem.[85]

However, there are also examples of successful cross-sector coordination. In Chile, the Cybersecurity Framework Law was passed in 2023 to upscale security-control accountability and incident-response capabilities for critical service providers. The law created sector specific CSIRTs and the National Cybersecurity Agency (ANCI), which defines standards for essential services providers (e.g., financial services) and issues fines for non-compliance with national cybersecurity regulations.[86]

Private organizations have also taken an increasingly central role in developing and implementing cybersecurity measures, with specialized bodies emerging to address sector-specific challenges. A notable example is the Alianza Chilena de Ciberseguridad (Chilean Cybersecurity Alliance), formed through the collaboration of nine major institutions spanning critical sectors, including financial sector partners.[87] This alliance exemplifies how multi-stakeholder partnerships between private industry, government agencies, and academic institutions can create robust cross-sector informational exchange during cybersecurity incidents. The development of dedicated institutes such as the Instituto Nacional de Ciberseguridad de Chile (Chilean National Institute of Cybersecurity) further strengthens this ecosystem by focusing on security awareness and trust-building across both individual and corporate stakeholders.[88] The rise of technology-focused trade associations, such as Chiletec, with its membership of over 100 Chilean technology companies, provides additional infrastructure for coordinating cybersecurity efforts.[89]

[76] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
[77] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
[78] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
[79] https://elpais.com/america-colombia/2023- 09-14/el-gobierno-aun-no-sabe-cuantas-entidades-estan-afectadas-por-el-hackeo-a-ifx networks.html
[80] https://therecord.media/colombia government-ministries-cyberattack
[81] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
[82] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
[83] https://doi.org/10.1007/978-3-030-60467-7_24
[84] https://doi.org/10.1007/978-3-030-60467-7_24
[85] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
[86] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
[87] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
[88] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
[89] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf

The integration of public–private cybersecurity coordination in Colombia demonstrates a sophisticated approach to financial sector resilience, particularly through collaboration between government entities (ColCERT, CCOC, MINTIC) and private-sector initiatives like Asobancaria's CSIRT.[90] This partnership exemplifies how regulatory frameworks can effectively merge with industry-led operational capabilities to create robust defense mechanisms.

The operational impact of this coordination is particularly noteworthy in the financial sector. According to recent data, Colombia's financial system has demonstrated remarkable resilience: out of nearly 20 billion cyber attacks in the past year, only two achieved successful penetration.[91] This success rate can be attributed to Asobancaria's CSIRT deployment of 17 cybersecurity experts who have processed over 300 security events and managed more than 450 early alerts in early 2024 alone.[92]

The scale of this collaboration is evident in how Asobancaria's CSIRT functions as both a national and international focal point for crisis management and incident response within the financial sector. Their Operations Center and Information Exchange Program has established itself as one of Latin America's most advanced cybersecurity-operations centers, serving as a model for how public–private partnerships can enhance sector-wide cyber resilience. This is particularly significant given Colombia's position as the second most targeted country for cyber attacks in Latin America. The success of this approach provides valuable insights for other LATAM nations seeking to develop similar public–private cybersecurity frameworks, particularly in protecting critical financial infrastructure.

[90] https://doi.org/10.25062/9789585216549
[91] https://www.mintic.gov.co/portal/inicio/
[92] https://www.mintic.gov.co/portal/inicio/

3 Industry Trends

3.1 Major Cyber-Threat Actors Targeting the Financial Industry in Latin America

The development of organizational cybersecurity programs in Latin America is mirrored by the expansion of ransomware as a significant cyber threat. The National Cybersecurity Index (NCSI) highlighted the void in robust cybersecurity policies and regulations across the LATAM region and, more so, revealed the risks and consequences of ransomware attacks for financial institutions.[93] According to the LATAM CISO 2024 report, in April 2022, Costa Rica's Ministry of Finance faced a $10M ransomware attack from Russia-based threat actor Conti, which shut down tax-filing systems and caused economic turmoil and mandates for more skilled workers in cybersecurity.[94]

As increasing cyber risks are explored within the financial sector, the Latin American industry trends of skilled workers, capital, investments, and user preferences are vital to this ecosystem. Ultimately, they provide quantifiable insights into what voids and best practices cybersecurity professionals must prioritize to address their cyber-hygiene needs.

3.1.1 More Cybersecurity Professionals Needed

According to Vergara Cobos in the "2024 Latin America and Caribbean" report, from 2023 to 2024, the global cybersecurity industry grew by 14%, and the global workforce gap grew to 4M, which is twice the growth rate of the IT sector and four times that of the worldwide economy. This presents significant potential for job creation via investments in cyber training and awareness.[95] The LATAM cybersecurity industry is predicted to grow by 8% in 2025, with growth in a skilled workforce at 15%.[96]

Although industry growth and workforce development are on par globally, Latin America's regional cyber readiness suggests low confidence in its nations' ability to resolve cyber attacks with its current critical infrastructure. North America and Europe show the highest confidence levels at 15%. Meanwhile, Africa and Latin America have the lowest confidence levels at 36%, and 42% of security professionals in these regions doubt their country's ability to resolve cyber attacks.[97] Latin American countries have been desperately seeking professionals who can protect their digital assets.[98] As cyber hygiene and issues around threat-awareness training make containment efforts challenging, updating national strategies and developing incident protocols have increased in priority for Latin American security professionals.[99] A skilled workforce is not traditionally considered part of physical critical infrastructure. However, it is essential for the security of the infrastructure and is a crucial void in LATAM that CISOs must prioritize. The human factor remains one of the most vulnerable points within an organization.[100]

Training and global partnerships in academia can be an investment in a skilled cybersecurity workforce. A shortage of cybersecurity professionals renders financial institutions vulnerable to the advanced attacks experienced by many within the region, as indicated in a report by the International Telecommunication Union (ITU). Critical infrastructure plans for cyber attacks are only established in seven of 32 LATAM countries, and 20 of 32 have CSIRTs. The Inter-American Bank assessment also notes that LATAM requires significant capacity improvements in skilled professionals.[101] This highlights an urgency for regional improvement in cyber readiness.[102]

Highlight: Critical enhancement in trained IT professionals, incident-response plans, and cybersecurity policies are priorities in improving LATAM's cyber posture. Planning, playbooks, and assessment exercises with third-party organizations are essential. Due to the lack of trained staffing and tools to communicate challenges across sectors in response, preparedness is consistently revealed as one of the most pressing challenges Training and education initiatives can help address the region's shortage of skilled cybersecurity professionals.

3.1.2 Greater Cybersecurity Budget to Address Increased Cyber Threats

In Latin America, banks are the most attacked organizations, with health and educational institutions trailing shortly behind. When considering specific countries, Brazil has the most cyber attacks, with Mexico and Colombia following. However, the frequency and severity of cyber attacks in other Latin American countries are not reduced.[103]

---

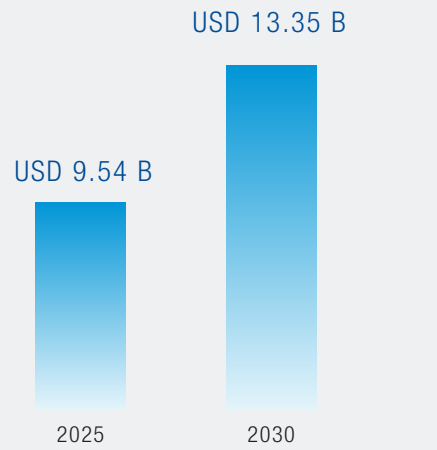
93 https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
94 https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
95 https://blogs.worldbank.org/en/latinamerica/seguridad-cibernetica-en-america-latina-y-el-caribe
96 https://www.nucamp.co/blog/coding-bootcamp-mexico-mex-mexico-cybersecurity-job-market-trends-and-growth-areas-for-2025
97 https://www.nucamp.co/blog/coding-bootcamp-mexico-mex-mexico-cybersecurity-job-market-trends-and-growth-areas-for-2025
98 https://www.nucamp.co/blog/coding-bootcamp-mexico-mex-mexico-cybersecurity-job-market-trends-and-growth-areas-for-2025
99 https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
100 https://mexicobusiness.news/cybersecurity/news/beyond-spending-strategic-investment-cybersecurity-2025
101 https://www.mordorintelligence.com/industry-reports/latin-america-cyber-security-market
102 https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
103 https://www.americaeconomia.com/en/business-industries/cybersecurity-new-center-concern-latin-american-companies

Due to emerging technology such as AI and cyber attacks worsening in 2024, Latin America has increased its investments in overcoming cybercrime.[104] The cost of cyber attacks in 2023 was USD 6T globally and USD 2.4M in Latin America. The growth in 2025 is expected to increase by 60% globally and 76% in Latin America, which is an all-time high for the region since 2020.[105] Notably, while 77% of Latin American organizations plan to increase cybersecurity budgets, only 25% of organizations in LATAM have adopted comprehensive cybersecurity plans.[106] Global spending on cybersecurity will exceed USD 1T in 2025, which creates opportunities to address Latin America's confidence in cybersecurity readiness.[107] Budgeting for cybersecurity often reflects the economic conditions of an area, which is becoming a spending priority as an organization understands the need for data assurance and trust in their brand.[108]

Highlight: The United States has committed to providing advanced hardware, specialized training, and logistic support, offering USD 25M by 2026 to help Costa Rica enhance its cybersecurity capabilities. In June 2022, USD 24M was allocated by the Costa Rican government for incident response and security operations. The severity of the LATAM threat landscape is not attributed to the increasing funds sowed into their commitment to cyber defense. More so, it is based on the nation becoming the first globally to declare a state of emergency due to a cyber attack.[109]

As highlighted in Figure 4, the Latin American cybersecurity market is estimated to be USD 9.54B in 2025. It is expected to reach USD 13.35B by 2030, at a CAGR of 6.95% from 2025 to 2030, which is driven by the rapid digitalization of financial services and banking infrastructure.[110] Budgets reflect the current, more established plans for cyber readiness and response to cyber attacks, whereas investments attest to awareness and proactive preparation to create a more effective regional cyber posture. Increased investments in cyber-readiness solutions and services suggest an impact on the growing recognition of cybersecurity's importance in Latin America.[111]

Figure 4: Latin American Cybersecurity Market



[104] https://www.americaeconomia.com/en/business-industries/cybersecurity-new-center-concern-latin-american-companies
[105] https://www.americaeconomia.com/en/business-industries/cybersecurity-new-center-concern-latin-american-companies
[106] https://mexicobusiness.news/cybersecurity/news/beyond-spending-strategic-investment-cybersecurity-2025
[107] https://mexicobusiness.news/cybersecurity/news/beyond-spending-strategic-investment-cybersecurity-2025
[108] https://www.pwc.com/gx/en/services/forensics/gecs/2024-global-economic-crime-survey.pdf
[109] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
[110] https://www.mordorintelligence.com/industry-reports/latin-america-cyber-security-market
[111] https://www.mordorintelligence.com/industry-reports/latin-america-cyber-security-market

3.1.3 Reasons for Investments

The digitization of the financial industry in LATAM requires more investments in cybersecurity, which includes machine learning and AI for improved threat detection and response capabilities. If not, many regional fintech startups will become highly attractive targets for cybercriminals. Overall, this suggests a need for more cybersecurity investments in Latin America.

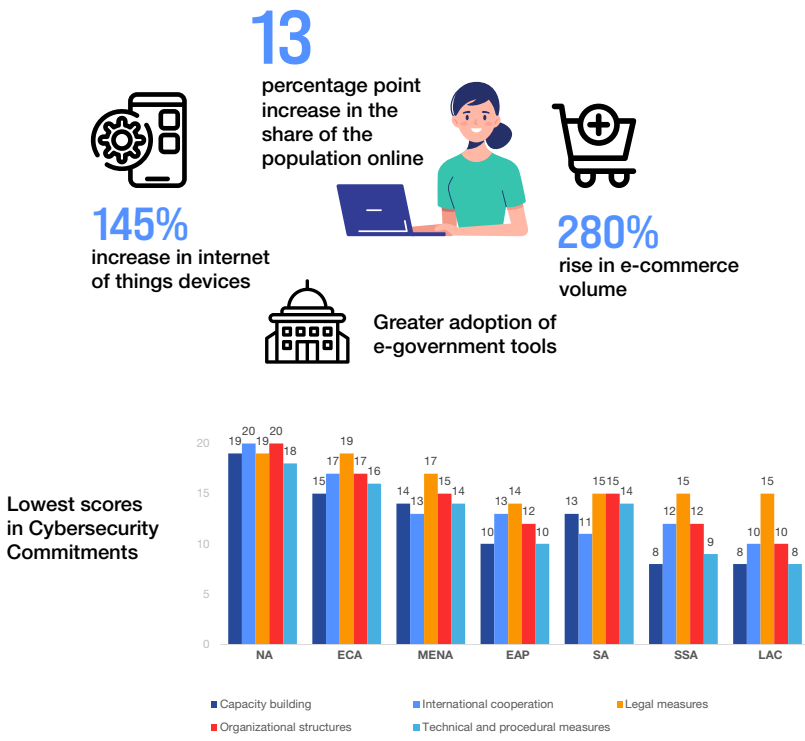
Unfortunately, the increase in digitalization is not scaling with the risk associated with the government sector, and it is imperative that ransomware threats be addressed due to the lack of maturity in organizational cybersecurity programs and policies for critical infrastructure in LATAM.[112]

Highlight: It is imperative to address cyber risks regarding data protection and national security. Due to significant ransomware attacks, 200 executive-level security professionals in the public and private sectors agree on prioritizing cybersecurity.[113]

Investing in cybersecurity can create positive economic effects, with an expected increase of 1.5% GDP per capita if cyber protections are enhanced and cyber incidents are reduced from 50 to seven major incidents. The "Cybersecurity Economics for Emerging Markets" reports how digitalization has outpaced the region's cybersecurity capacity. As of 2024, Latin America and the Caribbean are the least protected regions, with an average cyber score of 10.2 out of 20, and the world's fastest-growing regions for disclosed cyber incidents at a 25% annual growth rate over the last 10 years.[114] Rapid digitalization in Latin America has increased cyber threats, specifically in the financial sector.

Internet usage corresponds to the share of the population using the internet. Figure 5 highlights that LATAM went from 68% to 81% between 2019 and 2023, according to ITU.

Figure 5: Effect of LAC's Digitalization



Source: Cybersecurity Economics for Emerging Markets (2024).[115]

[112] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
[113] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
[114] https://blogs.worldbank.org/en/latinamerica/seguridad-cibernetica-en-america-latina-y-el-caribe
[115] https://blogs.worldbank.org/en/latinamerica/seguridad-cibernetica-en-america-latina-y-el-caribe

3.1.4 Shift from Brick & Mortar to Online and App-Based Banking

Financial institutions both in Latin America and globally focus on enhancing front-end user experience through easy-to-use apps and web-based features. However, this shift has created new vulnerabilities in sophisticated social engineering and phishing methods, primarily in online-banking markets.[116] Convenience drives digital and mobile banking solutions favored by Latin American consumers, and users too often accept new technology or solutions based on ease of use versus security requirements, which increases the risk of social engineering attacks like phishing.[117]

Highlight: Colombia is focused on improving incident tracing; Costa Rica has prioritized international partnerships for response capabilities, such as digital forensics and skilled-workforce training; and Chile established cyber standards in its Digital Agenda 2035 initiative to address digitization and cybersecurity.[118] To ensure that cybersecurity measures do not negatively impact the user experience, financial institutions and banks must be aware of user preferences for digital services.

Investments in cybersecurity for the financial industry in Latin America are rising. Nonetheless, the industry must improve the culture of cyber awareness and adopt innovative solutions to address ongoing threats to protect assets and customers. An enhanced security posture will help confront the complex cyber-threat landscape of organized cybercriminals, state-sponsored actors, and insider threats.

3.2 Contextual Socio-Economic Factors Impacting Risk Exposure

3.2.1 Rapid Fintech Growth

Latin America's fintech sector has grown considerably over the past six years, driven by socio-economic factors such as increasing mobile-phone adoption and large underbanked populations. This growth is characterized by a 340% increase in the number of financial technology companies, which rose from 703 across 18 countries in 2017 to 3,069 across 26 countries by 2023.[119]. Notably, this expansion surpasses the growth observed in more established markets like the United States, where fintech innovation has been significant but limited to its more mature market. However, this rapid development has exposed new vulnerabilities as many emerging fintech companies in Latin America often lack the robust cybersecurity measures common in more established markets. A study by the IMF highlights that these cybersecurity challenges stem from factors such as low awareness, outdated software, insufficient standards, critical-infrastructure gaps, and limited professional training.[120]

3.2.2 Reliance on Outdated Systems

Due to developing infrastructure and lackluster technological and data systems, many economic enterprises in Latin America often rely on outdated systems. An analysis published in MDPI's Informatics journal identifies the use of outdated software as a critical vulnerability in Latin American countries.[121] This dependency on obsolete technology leaves these systems vulnerable to newer threats as they often lack essential security updates and patches. Even when updates are available, the underlying architecture of these outdated systems may remain susceptible due to hardware limitations. Consequently, financial institutions with such poor systems can be easily targeted by cybercriminals. Addressing this issue requires substantial investment in modernizing IT infrastructure and the implementation of maintenance protocols. Encouraging financial institutions to move to the cloud would provide modern, more secure systems and automated updates. According to the World Economic Forum's report on Latin America's cybersecurity challenges, adopting risk-management frameworks (RMFs) and using public cloud technologies to improve cyber resilience and protect vital infrastructure could combat ransomware attacks.[122] To fully realize the security infrastructure gains of the cloud, financial institutions would need to hire or rely on third parties to ensure security controls are in place and consistent.

[116] https://www.mordorintelligence.com/industry-reports/latin-america-cyber-security-market
[117] https://www.statista.com/statistics/1481783/online-bankingpenetration-latin-america-forecast/:~:text=Online%20banking%20penetration%20in%20Latin%20America%20increased%20gradually%20between%202019,to%2033%20percent%20in%202023
[118] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
[119] https://www.iadb.org/en/news/study-fintech-ecosystem-latin-america-and-caribbean-exceeds-3000-startups
[120] https://www.imf.org/en/Publications/fintech-notes/Issues/2023/03/28/The-Rise-and-Impact-of-Fintech-in-Latin-America-531055
[121] https://www.mdpi.com/2227-9709/10/3/71
[122] https://www.weforum.org/stories/2024/05/latin-america-cybersecurity-report-ransomware attacks/

3.2.3 Economic & Digital Disparities

Latin America exhibits significant economic and digital disparities across its territory, leading to a pronounced digital divide. As of 2022, 67.3% of households in the region had internet access, compared to 91.1% in OECD countries.[123] This disparity poses challenges for small and medium-sized enterprises (SMEs), which are vital to the region's economy.[124] Many of these enterprises operate on limited budgets, restricting their ability to invest in robust cybersecurity measures. This financial constraint makes them attractive targets for cybercriminals as SMEs often lack the advanced defenses found in larger corporations. Investing in digital infrastructure to reduce the digital divide among individuals and SMEs can improve cybersecurity and mitigate prominent risks.

[123] https://www.undp.org/latin-america/blog/missed-connections-incomplete-digital-revolution-latin-america-and-caribbean-0
[124] https://www.iadb.org/en/news/ninety-six-percent-banks-latin-america-and-caribbean-view-small-and-medium-enterprises#:~:text=Ninety%2Dsix%20percent%20of%20the,policy%20for%20SMEs%20in%20place.

4 Regulatory Gaps

4.1 Ransomware Breach Reporting Requirements and Lack of Standards

Cybersecurity reporting requirements across LATAM are inconsistent, leading to vulnerabilities in the region's ability to combat cyber threats effectively.

For instance, consider the following:

1. Brazil's General Data Protection Law (LGPD) mandates organizations to report breaches to the National Data Protection Authority (ANPD) within two business days and notify affected individuals.[125]

2. Colombia requires organizations to report security-code violations to the Delegatura para la Protección de Datos Personales (Office for the Protection of Personal Data) and affected data subjects.[126]

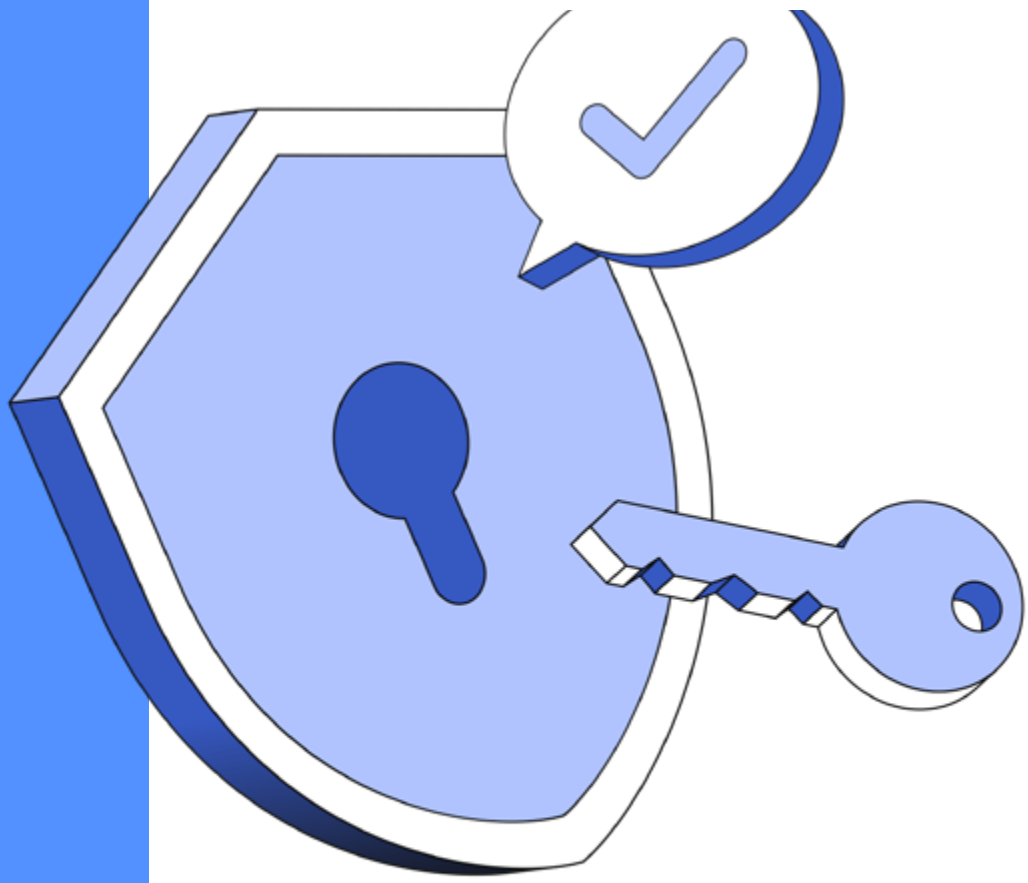
3. Mexico enforces reporting of "data vulnerabilities" impacting individuals' rights but does not specify a timeline.

4. Argentina merely recommends voluntary reporting as a best practice.[127]

5. Many countries, such as Peru, Ecuador, and Costa Rica, lack comprehensive reporting frameworks altogether.[128]

This fragmented regulatory landscape creates significant gaps, making LATAM increasingly susceptible to ransomware attacks. Countries with limited or no mandatory reporting, such as Central American nations, face challenges in tracking and responding to threats due to insufficient data sharing and threat-intelligence coordination.[129] The lack of harmonized security standards results in inconsistent practices across the region, leaving weak points for cybercriminals to exploit.[130] Furthermore, inadequate cybersecurity infrastructure, insufficient education, and limited resources exacerbate these vulnerabilities, especially in sectors such as manufacturing and finance, which have faced over 100 ransomware incidents since 2023.[131] [132] The absence of stringent reporting frameworks also delays breach response times, allowing ransomware operators to further exploit compromised systems.[133] Rapid digital transformation in LATAM, especially within financial services, has outpaced regulatory developments, creating additional attack surfaces.[134] [135] Without robust incident-reporting requirements and coordinated defense strategies, many LATAM nations are struggling to combat increasingly sophisticated ransomware threats targeting government and financial institutions.[136] [137]

[125] https://iapp.org/news/a/reporting-cyber-incident-requirements-in-some-latin-american-jurisdictions
[126] https://iapp.org/news/a/reporting-cyber-incident-requirements-in-some-latin-american-jurisdictions
[127] https://iapp.org/news/a/reporting-cyber-incident-requirements-in-some-latin-american-jurisdictions
[128] https://www.dacbeachcroft.com/en/What-we-think/Stepping-up-in-Latin-America-Chile-enacts-a-new-Cybersecurity-Law
[129] https://www.moodys.com/web/en/us/insights/credit-risk.html
[130] https://www.moodys.com/web/en/us/insights/credit-risk.html
[131] https://www.cloudsek.com/whitepapers-reports/latin-america-latam-cyber-threat-landscape-2023-24
[132] https://www.recordedfuture.com/research/latin-american-governments-targeted-by-ransomware
[133] https://www.datto.com/blog/ransomware-and-cybersecurity-in-latin-america/
[134] https://www.datto.com/blog/ransomware-and-cybersecurity-in-latin-america/
[135] https://www.trustwave.com/en-us/resources/blogs/trustwave-blog/trustwave-spiderlabs-reveals-the-ransomware-threats-targeting-latin-american-financial-and-government-sectors/
[136] https://www.trustwave.com/en-us/resources/blogs/trustwave-blog/trustwave-spiderlabs-reveals-the-ransomware-threats-targeting-latin-american-financial-and-government-sectors/
[137] https://industrialcyber.co/analysis/recorded-future-detects-escalation-of-ransomware-attacks-across-latam-government-entities/



5 Threat-Actor Profiles

5.1 CL0P

CL0P emerged in early 2019 as a derivative of the Cryptomix ransomware family.[138] The ransomware group quickly evolved from utilizing traditional ransomware-deployment methods into a sophisticated cyber-threat group targeting global enterprises.[139] The group's ransomware is characterized by its unique ".clop" file extension and the distinctive "Don't Worry CL0P" string in its ransom notes.[140] The group's initial operations relied primarily on traditional ransomware deployment through phishing campaigns. However, their methodology underwent a significant transformation as they adopted a RaaS model. This transition proved crucial, allowing them to leverage relationships with sophisticated threat actors, including TA505, FIN11, and UNC 2546, for deployment operations.

5.1.1 Victim Profile and Impact Analysis

Analyzing CL0P's victim list suggests that the ransomware group primarily targets large enterprises with revenues exceeding USD 5M.[141] The main target entities of CL0P are from the following sectors: banking and finance, healthcare, manufacturing, education, and energy.[142] CL0P's activities have been prevalent in the United States, United Kingdom, Germany, Canada, Brazil, and Mexico, which account for 77.3% of their attacks.[143]

The impact of CL0P's operations in Latin American countries has been substantial, particularly in Brazil and Mexico.[144] In LATAM, where cybersecurity frameworks are nascent, organizations face amplified vulnerabilities due to interconnected systems and limited incident-response capabilities. Moreover, financial institutions in Latin America face a dual threat: direct attacks on banking systems and supply-chain compromises, such as the MOVEit zero-day exploit, which affected hundreds of organizations.

Impact and Scale of CL0P's Operations:

- CL0P's activities saw a 340% increase in victims compared to the previous quarter, potentially due to the MOVEit zero-day vulnerability exploitation.[145]
- The group is expected to earn $75–100 million from extorting victims in their massive MOVEit data-theft campaign.[146]

5.1.2 Malware Capabilities and Functionality

CL0P's technical sophistication is evident in their carefully structured attack chains. Their initial access vectors have evolved from simple phishing campaigns to sophisticated zero-day exploitation techniques.[147]. The group maintains a diverse toolkit, including specialized malware, such as SDBot for lateral movement, Cobalt Strike for post-exploitation activities, and custom tools like FlawedAmmyy/FlawedGrace for command-and-control operations.[148]

CL0P's use of TrueBot, an advanced malware component associated with the Silence Group, demonstrates their connections to sophisticated financial threat actors. TrueBot's capability to deploy additional payloads while maintaining stealth through self-deletion mechanisms showcases their focus on operational security.[149] Furthermore, the malware's association with TA505 and its use of an exclusive backdoor named FlawedGrace, indicates CL0P's position within a sophisticated cyber-threat ecosystem.[150] The group's initial network penetration typically follows an orchestrated multi-stage approach:

1. The exploitation of public-facing web applications using the LEMURLOOT web shell, written in C# coding language and disguised as an ASP.NET file.
2. Credential-harvesting operations enabling lateral movement and access to sensitive data. 3. Data-theft operations showing careful attention to operational security, focusing on exfiltration rather than encryption.[151]

[138] https://www.sangfor.com/blog/cybersecurity/Cl0p ransomware-gang-what-you-need-to-know
[139] https://unit42.paloaltonetworks.com/cl0p-group-distributes-ransomware-data-with-torrents/
[140] https://www.sangfor.com/blog/cybersecurity/Cl0p ransomware-gang-what-you-need-to-know
[141] https://www.sangfor.com/blog/cybersecurity/Cl0p ransomware-gang-what-you-need-to-know
[142] https://www.securin.io/blog/all-about-clop-ransomware/
[143] https://socradar.io/dark-web-threat-profile-clop-ransomware/
[144] https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware spotlight-clop
[145] https://www.dragos.com/blog/dragos-industrial-ransomware-analysis-q3- 2023/
[146] https://www.dragos.com/blog/dragos-industrial-ransomware-analysis-q3- 2023/
[147] https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware spotlight-clop
[148] https://blog.talosintelligence.com/breaking-the-silence-recent-truebot-activity/
[149] https://em360tech.com/tech-article/what-is-cl0p-ransomware
[150] https://em360tech.com/tech-article/what-is-cl0p-ransomware
[151] https://em360tech.com/tech-article/what-is-cl0p-ransomware

5.1.3 Evolution of CL0P's Operations

1. Shift in attack vector: Initially, CL0P relied primarily on phishing campaigns with macro-enabled documents to deliver the Get2 malware dropper.[152] In recent campaigns, they have pivoted to exploiting zero-day vulnerabilities in widely used file-transfer applications.[153] [154]

2. Focus on data exfiltration: While their initial attacks involved both file encryption and data theft, recent campaigns have concentrated more on data exfiltration without necessarily encrypting files.[155] [156]

3. Scale of attacks: Recent campaigns have targeted significantly more victims simultaneously through supply-chain attacks. For example, the MOVEit exploit in 2023 impacted up to 400 organizations.[157]

4. Sophistication of techniques: CL0P has evolved to use more advanced evasion techniques, including digital signatures to bypass endpoint detection.[158]

5. Expansion to new platforms: Initially targeting only Windows systems, CL0P developed a Linux variant in late 2022, broadening their potential victim base.[159]

6. Ransom approach: Recent campaigns have seen CL0P directly contacting upper level executives with ransom demands, rather than leaving traditional ransom notes on infected systems.[160]

7. Exploitation timeline: CL0P has shown increased patience and strategic planning, with evidence suggesting they may have been preparing the MOVEit exploit since 2021.[161]

CL0P's shift from encrypting devices to focusing solely on data exfiltration makes their attacks potentially stealthier and more difficult to detect. This change in modus operandi could allow CL0P to operate undetected for longer periods as there are no immediate signs of compromise, such as encrypted files or ransom notes.

The move towards only data exfiltration is a logical evolution of CL0P's tactics for several reasons:

1. Reduced detection risk: Without file encryption, there are fewer obvious indicators of compromise (IOCs), making it difficult for organizations to quickly identify an ongoing attack.

2. Extended access: By not alerting victims through encryption, CL0P can potentially maintain access to systems for longer periods, allowing for more comprehensive data theft.

3. Simplified operations: Focusing solely on data exfiltration streamlines the attack process, potentially allowing CL0P to target more victims simultaneously.

4. Increased pressure: The threat of leaking sensitive data can be just as effective as file encryption in forcing victims to pay, without the added complexity of providing decryption tools.

The success of this approach is evident in CL0P's recent campaigns, such as the 2023 MOVEit attack, where they claimed to have breached hundreds of companies by exploiting a zero-day vulnerability (CVE-2023-34362) to mass download organizations' data without encrypting files.[162] By adopting this stealthier approach, CL0P can potentially increase the success rate of their attacks and the likelihood of ransom payments as organizations may feel more pressure to prevent the leak of sensitive data.

Although there is less concrete evidence for CL0P's shift explicitly to stealth, cybersecurity experts acknowledge that groups are adopting only data extortion to circumvent traditional defenses. Data exfiltration provides ransomware groups with a greater advantage over their victims in several ways:

1. Prolonged extortion potential: Once data is stolen, cybercriminals can continue exploiting it for additional extortion long after the initial incident, even if the original ransom is paid.[163]

2. Tailored demands: Exfiltrated data allows attackers to customize their extortion demands based on the sensitivity and value of the stolen information.[164] [165]

---

[152] https://www.nuspire.com/blog/a-deep-dive-into-cl0p-ransomware/
[153] https://em360tech.com/tech-article/what-is-cl0p-ransomware
[154] https://www.criticalstart.com/threat-research-cl0p-ransomware-increases-activity
[155] https://em360tech.com/tech-article/what-is-cl0p-ransomware
[156] https://www.criticalstart.com/threat-research-cl0p-ransomware-increases-activity
[157] https://www.criticalstart.com/threat-research-cl0p-ransomware-increases-activity
[158] https://em360tech.com/tech-article/what-is-cl0p-ransomware
[159] https://www.criticalstart.com/threat-research-cl0p-ransomware-increases-activity
[160] https://em360tech.com/tech-article/what-is-cl0p-ransomware
[161] https://em360tech.com/tech-article/what-is-cl0p-ransomware
[162] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware double-extortion-and-beyond-revil-clop-and-conti
[163] https://www.grcilaw.com/blog/top-3-reasons ransomware-groups-are-focusing-more-on-data-exfiltration-than-encryption
[164] https://www.grcilaw.com/blog/top-3-reasons ransomware-groups-are-focusing-more-on-data-exfiltration-than-encryption
[165] https://www.vadesecure.com/en/blog/data-exfiltration-why ransomware-is-about-more-than-the-ransom

3. Increased pressure: The threat of leaking sensitive data can be more effective than file encryption in forcing victims to pay as it exploits fears of regulatory fines, reputational damage, and competitive disadvantage.[166] [167]

4. Bypassing backups: While organizations can restore encrypted files from backups, they cannot retrieve data that has already been stolen, which makes traditional backup solutions ineffective against modern ransomware attacks.[168]

5. Secondary-attack potential: Compromised data can fuel future breaches through tactics such as credential stuffing, social engineering, and password-reuse attacks.[169]

6. Higher profitability: Stolen data can be more valuable than ransom payments as it can be sold on the dark web or used for ongoing blackmail.[170]

This shift towards data exfiltration demonstrates the evolving tactics of ransomware groups as they adapt to improved organizational defenses and seek more effective ways to pressure victims into paying ransoms.[171] [172]

The ransomware group has significantly evolved its operational methodology since its emergence in 2019, becoming one of the most feared ransomware groups by 2023. The group's focus on zero-day vulnerabilities in file transfer applications (FTAs) is driven by several factors:

1. Widespread use: FTAs are commonly used in corporate environments, providing attackers with numerous potential entry points.[173]

2. Supply-chain attack potential: Exploiting FTA vulnerabilities allows CL0P to potentially compromise multiple organizations simultaneously.[174] [175]

3. Efficient data exfiltration: FTAs are designed for efficient data transfer, facilitating the theft of large amounts of data.

4. Compliance requirements: Many FTAs, like MOVEit, are approved for use in regulated industries, meaning they often contain highly sensitive data.[176]

5. High-value targets: Organizations using FTAs often include large enterprises and government agencies, which are lucrative targets for ransomware attacks.[177] [178]

6. Stealth: Accessing systems through legitimate file-transfer tools can make malicious activities appear normal, helping attackers evade detection.

This approach has proven highly effective for CL0P, as evidenced by their successful attacks on the Accellion FTA, GoAnywhere MFT, and MOVEit Transfer, each affecting hundreds of organizations and potentially exposing millions of individuals' data.[179] [180]

5.1.4 Impact on Financial Infrastructure

The systematic nature of CL0P's operations against financial institutions has revealed fundamental vulnerabilities in sector-wide security architectures. The group's successful exploitation of managed file-transfer systems has exposed critical weaknesses in the financial sector's approach to secure data transfer and the integration of third-party software.[181] The MOVEit campaign serves as a particularly instructive example, where a single vulnerability in a widely used platform led to compromises across multiple financial institutions.[182]

Additionally, the impact extends beyond immediate operational disruption. Financial institutions affected by CL0P operations have faced complex challenges in maintaining regulatory compliance and developing updated policies while managing ongoing compromise scenarios. In Peru alone, 47% of CISOs list complying with geographically fragmented and overly prescriptive regulations as their most stressful responsibility. Of all industries, the financial services industry is most concerned about fragmented regulations, with 67% of global CISOs in the sector anticipating that international regulations will become more complex and difficult to manage in the next year. Accordingly, CL0P's understanding of financial sector regulatory frameworks has allowed them to structure their extortion demands in

[166] https://www.grcilaw.com/blog/top-3-reasons ransomware-groups-are-focusing-more-on-data-exfiltration-than-encryption
[167] https://www.infosecurity-magazine.com/news/ransomware defense-evasion-data/
[168] https://www.grcilaw.com/blog/top-3-reasons ransomware-groups-are-focusing-more-on-data-exfiltration-than-encryption
[169] https://www.grcilaw.com/blog/top-3-reasons ransomware-groups-are-focusing-more-on-data-exfiltration-than-encryption
[170] https://www.infosecurity-magazine.com/news/ransomware defense-evasion-data/
[171] https://www.vadesecure.com/en/blog/data-exfiltration-why ransomware-is-about-more-than-the-ransom
[172] https://www.infosecurity-magazine.com/news/ransomware defense-evasion-data/
[173] https://cyberint.com/blog/dark-web/cl0p-ransomware/
[174] https://cyberint.com/blog/dark-web/cl0p-ransomware/
[175] https://www.cisa.gov/sites/default/files/2023- 06/aa23-158a-stopransomware-cl0p-ransomware-gang-exploits-moveit-vulnerability_5.pdf
[176] https://cyberint.com/blog/dark-web/cl0p-ransomware/
[177] https://cyberint.com/blog/dark-web/cl0p-ransomware/
[178] https://www.cisa.gov/sites/default/files/2023- 06/aa23-158a-stopransomware-cl0p-ransomware-gang-exploits-moveit-vulnerability_5.pdf
[179] https://cyberint.com/blog/dark-web/cl0p-ransomware/
[180] https://www.cisa.gov/sites/default/files/2023- 06/aa23-158a-stopransomware-cl0p-ransomware-gang-exploits-moveit-vulnerability_5.pdf
[181] https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware spotlight-clop
[182] https://securityandtechnology.org/blog/2023-rtf-global-ransomware-incident-map

ways that create maximum pressure within a patchwork of emerging regulatory obligations [26]. Based on their MOVEit campaign, CL0P has demonstrated the advanced timing of releases and extortion demands as it batch-releases victim data to maximize pressure.[183]

With over 1,600 cyber-attack attempts per second on Latin American companies, LATAM financial institutions have faced specific challenges due to the interconnected nature of regional financial networks.[184] The exploitation of shared infrastructure and common software platforms has created cascading effects across multiple institutions.[185] This regional impact is exemplified by the aftermath of the GoAnywhere MFT campaign, where multiple regional institutions discovered compromises through shared infrastructure dependencies.[186]

5.1.5 Regulatory and Policy Gaps

1. Limited Frameworks for Critical-Infrastructure Protection

One fundamental vulnerability stems from Latin America's nascent frameworks for critical-infrastructure protection. According to the Inter-American Development Bank, only seven of 32 Latin American countries have established plans to protect critical infrastructure from cyber attacks, with only 20 attesting to any CSIRTs.[187] This regulatory immaturity particularly affects financial institutions, which lack federal sector-specific security protocols and incident-reporting requirements standardized across LATAM jurisdictions.[188]

2. Fragmented Incident-Response Coordination

The absence of centralized cybersecurity governance creates significant coordination challenges during cybersecurity incidents. This gap was evident in both Costa Rica's 2022 ransomware crisis and Colombia's September 2023 IFX Networks attack, which initially affected 20 public entities and indirectly impacted another 78 public entities and 762 private companies—including financial institutions across multiple LATAM nations.[189] The lack of standardized incident-response protocols across the region creates opportunities for threat actors like CL0P to exploit gaps in cross-border coordination. CL0P has demonstrated a sophisticated understanding of these gaps, as demonstrated by their systematic targeting of widely used enterprise software platforms that can affect multiple institutions simultaneously.

3. Insufficient Mandatory Reporting Requirements

Many Latin American countries lack comprehensive mandatory breach reporting requirements, particularly for financial institutions. This regulatory gap aligns with CL0P's documented tactics of exploiting information asymmetries and delayed incident detection.[190] The absence of stringent reporting requirements can extend the window of opportunity for sophisticated gangs like CL0P to maintain persistence and expand their access within compromised networks.

4. Data-Protection Implementation Challenges

While countries such as Brazil, Argentina, Mexico, Panama, and Colombia have enacted data-protection laws, implementation and enforcement remain inconsistent. This creates vulnerabilities for financial institutions handling sensitive customer data, aligning with CL0P's demonstrated focus on data theft and multi-stage extortion operations targeting financial services providers. Their use of FlawedAmmyy/FlawedGrace for command-and-control operations demonstrates specific adaptation to regional financial sector security controls, allowing them to maintain persistent access.

5.1.6 Market Structure and Digital-Transformation Context

The Latin American banking market remains the fastest-growing globally, with revenue before cost of risk growing at a compound annual rate of 12% since 2012, reaching $418 billion in 2017.[191] Since 2020, the LATAM retail-banking sector has nearly doubled its compound annual-revenue growth rate (measured in trillions USD) from 2013 to 2019.[192] Furthermore, LATAM has experienced significant growth in online-payments revenues and is projected to outpace all other regions until 2027.[193]. This rapid historical growth, combined with relatively low banking penetration rates of 30–50% compared to 90%+ in developed markets, creates pressure for rapid digital transformation that often outpaces security implementation.[194]With the number of LATAM consumers who prefer mobile and card payments doubling since 2021, LATAM banks are shifting to a mobile-first delivery strategy while prioritizing IT investments to improve user experiences.[195]

---

[183] https://www.cisa.gov/sites/default/files/2023- 06/aa23-158a-stopransomware-cl0p-ransomware-gang-exploits-moveit-vulnerability_5.pdf
[184] https://www.cisa.gov/sites/default/files/2023- 06/aa23-158a-stopransomware-cl0p-ransomware-gang-exploits-moveit-vulnerability_5.pdf
[185] https://www.cisa.gov/sites/default/files/2023- 06/aa23-158a-stopransomware-cl0p-ransomware-gang-exploits-moveit-vulnerability_5.pdf
[186] https://www.cisa.gov/sites/default/files/2023- 06/aa23-158a-stopransomware-cl0p-ransomware-gang-exploits-moveit-vulnerability_5.pdf
[187] https://publications.iadb.org/publications/english/document/2020-Cybersecurity-Report-Risks-Progress-and-the-Way-Forward-in-Latin-America-and-the-Caribbean.pdf
[188] https://iapp.org/news/a/reporting-cyber-incident-requirements-in-some-latin-american-jurisdictions
[189] https://www.metabaseq.com/e-book/cyber-readiness-in-latin-american-public-sectors/
[190] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
[191] https://www.mckinsey.com/industries/financial-services/our-insights/lessons-from-leaders-in-latin-americas-retail-banking-market
[192] https://www.mckinsey.com/industries/financial-services/our-insights/global-banking-annual-review
[193] https://www.mckinsey.com/industries/financial-services/our-insights/global-banking-annual-review
[194] https://www.mckinsey.com/industries/financial-services/our-insights/lessons-from-leaders-in-latin-americas-retail-banking-market
[195] https://www.mckinsey.com/industries/financial-services/our-insights/global-banking-annual-review

5.1.7 Profitability Pressures Creating Security Tradeoffs

While Latin American banks were once the most profitable globally, with an ROE of 14% in 2017, they continue to face significant cost-efficiency challenges. Operating expenses average 3.9% of assets, which is 1.5% higher than the next closest region.[196] This cost pressure creates vulnerabilities as institutions balance digital-transformation investments with security spending. Furthermore, consumer finance and mortgage services (which account for more than one-third of after-risk revenues) are especially attractive for threat actors due to their high concentration of sensitive customer data.[197]

5.1.8 Sector-Specific Vulnerabilities

1. Digital-Transformation Pressures

The Latin American financial services sector is undergoing rapid digital transformation, particularly accelerated by the bankarization (the level of access to and the degree of use of financial and banking services) after the COVID-19 pandemic. This creates an expanded attack surface that CL0P has demonstrated proficiency in exploiting. The adoption of managed file transfer (MFT) solutions often outpaces security implementations, as evidenced by the widespread impact of CL0P's MOVEit campaign across the region's financial institutions.[198] Financial institutions should ensure they have adequate security and operational resilience “know-how” before onboarding technology to assure the safety and soundness of the institution.

2. Operational Vulnerability Drivers

The banking sector's vulnerabilities can be traced to three distinct market archetypes identified in the region[199]:

- Efficiency-Driven Markets: These markets, such as Chile, operate with lean cost structures but may underinvest in security infrastructure. Their operational expense ratio below 3.4% of assets often necessitates reduced security spending.
- Balanced Markets: Markets like Brazil combine moderate revenue generation (4.5–7% of assets) with mid-range operational costs, creating potential security gaps when balancing competing investment priorities.
- Revenue-Driven Markets: Markets like Argentina generate high revenues but operate with operational expenses above 5.5% of assets, potentially lacking efficiency in security operations despite higher spending.

3. Workforce-Development Challenges

A critical industry vulnerability stems from the severe shortage of cybersecurity professionals across Latin America. For example, Chile alone faces an annual deficit of approximately 6,000 IT professionals.[200] This human-capital gap particularly affects financial institutions' ability to do the following:

- Implement sophisticated security controls
- Maintain effective security operations
- Respond rapidly to emerging threats
- Adapt to evolving attack methodologies

The workforce shortage aligns with CL0P's documented tactics of exploiting gaps in security monitoring and incident-response capabilities.

4. Infrastructure Dependencies

Latin American financial institutions frequently rely on shared infrastructure and common technology platforms, creating systemic vulnerabilities that CL0P has proven adept at exploiting. The September 2023 IFX Networks attack demonstrated how the compromise of a single service provider could impact multiple financial institutions across several countries.[201] Such interdependence is exacerbated by the gap in the region’s infrastructure-protection frameworks.

5.1.9 Public-Sector Gaps Creating Downstream Risk

1. Resource-Allocation Disparities

Public-sector cybersecurity budgets in Latin America consistently lag behind private-sector investments. This creates particular challenges for financial institutions that must interface with government systems, especially in areas such as the following:

- Tax collection and reporting
- Regulatory-compliance systems
- National payment infrastructures
- Identity-verification services

196 https://www.mckinsey.com/industries/financial-services/our-insights/lessons-from-leaders-in-latin-americas-retail-banking-market
197 https://www.mckinsey.com/industries/financial-services/our-insights/lessons-from-leaders-in-latin-americas-retail-banking-market
198 https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
199 https://www.mckinsey.com/industries/financial-services/our-insights/lessons-from-leaders-in-latin-americas-retail-banking-market
200 https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
201 https://www.metabaseq.com/e-book/cyber-readiness-in-latin-american-public-sectors/

CL0P's targeting methodology often exploits these public–private interconnections, as demonstrated in both the Costa Rica and Colombia incidents.[202]

5.1.10 Convergence of Vulnerabilities Creating Strategic Opportunity for CL0P

The combination of regulatory gaps and industry trends creates multiple vectors that align with CL0P's sophisticated targeting methodology and operational patterns:

1. Multi-Stage Exploitation Opportunities

CL0P's documented preference for multi-stage extortion operations has proven effective in Latin America due to the convergence of several factors:

- Delayed detection capabilities due to workforce shortages
- Complex cross-border coordination requirements
- Inconsistent incident-reporting frameworks
- Regional interconnectivity of financial systems

This environment enables CL0P to maximize both initial access and lateral movement opportunities.[203]

2. Financial Sector Attack Surface

The financial services industry's digital-transformation initiatives, combined with regulatory-compliance requirements, create an expanded attack surface that CL0P has demonstrated expertise in exploiting. The group's sophisticated understanding of financial sector operational patterns is evidenced in their targeting of the following:

- Managed file-transfer systems essential for regulatory reporting
- Weak authentication and access-control protocols
- Shared service providers serving multiple institutions
- Cross-border payment and settlement systems
- Core banking platforms with regional deployments

This targeting aligns with the documented capabilities of their advanced malware toolkit, which includes TrueBot and FlawedGrace, which are specifically adapted to financial sector security controls.[204]

3. Regional Amplification Effects

The interconnected nature of Latin American financial markets creates opportunities for threat actors to amplify the impact of single compromises. This multiplicative effect makes the region particularly attractive for sophisticated ransomware operations seeking maximum leverage for extortion demands.

5.1.11 Forward-Looking Implications

Evolving Threat Landscape

The combination of regulatory gaps and industry pressures suggests the continued targeting of Latin American financial institutions by sophisticated threat actors. CL0P's demonstrated ability to adapt their tactics to regional vulnerabilities indicates the following:

- Attack sophistication will likely increase
- Cross-border incidents will become more common
- Supply-chain compromises will continue to be leveraged
- Multi-stage extortion operations will expand

[202] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
[203] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
[204] https://blog.talosintelligence.com/breaking-the-silence-recent-truebot-activity/

5.1.12 CL0P Tactics, Techniques, & Procedures

Tactics	Techniques	Procedures
Reconnaissance (TA0043)	T1592: Gathering Host Information	Uses phishing and social engineering tactics to collect information about their targets
	T1589.002: Email Addresses	Gains access to target's credentials through phishing, social engineering, and IABs
	T1589.001: Credentials	To be determined
	T1590: Gather Victim Network Information	Gains access to target's network information through phishing, social engineering, and IABs
	T1589: Gather Victim Identity Information	Gains access to target's network information through phishing, social engineering
Resource Development (TA0042)	T1586: Compromise Accounts	Compromises existing accounts with techniques such as phishing, social engineering and, IABs.
Initial Access (TA0001)	T1133: External Remote-Services Compromise	Access to enterprise network through compromised user accounts
	T1190: Exploit Public-Facing Applications	Scans for public-facing application to identify and exploit zero-day vulnerabilities
	T1566: Phishing	Sends phishing emails to targets to gain access to their systems and exfiltrate data and credentials
	T1091: Replication Through Removable Media	Checks for available system drives (often done to infect USB drives)
	T1078.003: Local Accounts	To be determined
Execution (TA0002)	T1059.001: PowerShell	To be determined
	T1059.003: Windows Command Shell	To be determined
	T1047: Windows Management Instrumentation	Queries BIOS Information (via WMI, Win32_Bios)
	T1106: Native API	To be determined
	T1053.003: Cron	To be determined
	T1053.005: Scheduled Task	To be determined
	T204.002: Malicious File	To be determined
Persistence (TA0003)	T1098: Account Manipulation	Uses compromised accounts to escalate administrator privileges or create new accounts with admin privilege
	T1574.001: Registry Run/ Startup Folder	Stores files to the Windows startup directory
	T1037.004: RC Scripts	To be determined

Tactics	Techniques	Procedures
	T1136: Create Account	Uses compromised accounts to escalate to administrator privileges or create new accounts with admin privilege
	T1543.002: Systemd Service	To be determined
	T1133: External Remote Services	To be determined
	T1574.002: DLL Side-Loading	Attempts to load missing DLLs
	T1053.003: Cron	To be determined
	T1053.005: Scheduled Task	To be determined
	T1505: Server Software Component	To be determined
	T1505.001: SQL Stored Procedure	To be determined
	T1505.003: Web Shell	To be determined
	T1078: Valid Accounts	Uses compromised accounts to escalate to administrator privileges or create new accounts with admin privilege
	T1078.003: Local Accounts	Uses compromised accounts to escalate to administrator privileges or create new accounts with admin privilege
Privilege Escalation (TA00 04)	T1548.002: Bypass User Account Control	Runs malicious code with administrator privileges
	T1098: Account Manipulation	Uses compromised accounts to escalate administrator privileges or create new accounts with admin privilege
	T1574.001: Registry Run/ Startup Folder	Stores files to the Windows startup directory
	T1037.004: RC Scripts	To be determined
	T1543.002: Systemd Service	To be determined
	T1068: Exploitation For Privilege Escalation	Exploits known vulnerabilities in software or applications to escalate privileges
	T1574.002: DLL Side-Loading	Attempts to load missing DLLs
	T1053.003: Cron	To be determined
	T1053.005: Scheduled Task	Deletes volume shadow copies to prevent system recovery
	T1078.003: Local Accounts	Uses compromised accounts to escalate to administrator privileges or create new accounts with admin privilege
Defense Evasion (TA0005)	T1222.002: Linux and Mac file and Directory Permissions Modification	To be determined
	T1497.001: System Checks	References anti-VM strings targeting Xen
	T1078: Valid Accounts	Uses compromised accounts to escalate to administrator privileges or create new accounts with admin privilege

Tactics	Techniques	Procedures
	T1078.003: Local Accounts	Uses compromised accounts to escalate to administrator privileges or create new accounts with admin privilege
	T1218.007: Msiexec	To be determined
	T1218.010: Regsvr32	To be determined
	T1218.011: Rundll32	To be determined
	T1553.002: Code Signing	To be determined
	T1112: Modify Registry	Uses registry keys to establish persistence and disable security systems on infected systems
	T1070.002: Clear Linux or Mac System Logs	To be determined
	T1574.002: DLL Side-Loading	Attempts to load missing DLLs
	T1140: Deobfuscate/Decode Files or Information	To be determined
	T1622: Debugger Evasion	Sample may be VM or debugger-aware; queries disk information (often used to detect virtual machines)
	T1548.002: Bypass User Account Control	Runs malicious code with administrator privileges
Credential Access (TA0006)	T1003.001: LSASS Memory	To be determined
	T1552.007: Container API	To be determined
Discovery (TA0007)	T1622: Debugger Evasion	Sample may be VM or debugger-aware; queries disk information (often used to detect virtual machines)
	T1083: File and Directory Discovery	Enumerates the file system, reads INI files, enumerates files on Windows, enumerates files recursively, and acquires file size
	T1135: Network Share Discovery	Enumerates network shares
	T1057: Process Discovery	Queries a list of all running processes and enumerates processes
	T1012: Query Registry	Queries or enumerates registry value and queries or enumerates registry key
	T1082: System Information Discovery	Queries BIOS information (via WMI, Win32 Bios), queries the volume information (name, serial number, etc.) of a device, reads software policies, and acquires disk information
	T1497.001: System Checks	To be determined
Lateral Movement (TA0008)	T1021.002 SMB/Windows Admin Shares	To be determined
	T1021.002 SSH	To be determined
	T1021.006 Windows Remote Management	To be determined

Tactics	Techniques	Procedures
	T1091: Replication Through Removable Media	Checks for available system drives (often done to infect USB drives)
	T1021.001: Remote Desktop Protocol	To be determined
Collection (TA0009)	T1005: Data from Local System	Collects disk information
Command and Control (C2) (TA0011)	T1071.001: Web Protocols	Uses application layer protocol to download malware and encryption keys
	T1573.001: Symmetric Cryptography	
	T1105: Ingress Tool Transfer	To be determined
	T1104: Multi-Stage channels	To be determined
	T1571: Non-Standard Port	To be determined
Exfiltration (TA0010)	T1041: Exfiltration Over C2 Channel	Establishes connection with C2 server over HTTPS to download malware and encryption keys
	T1052.001: Exfiltration Over USB	Checks for available system drives (often done to infect USB drives)
	T1567.002: Exfiltration to Cloud Storage	To be determined
Impact (TA00 40)	T1485: Data Destruction	To be determined
	T1486: Data Encrypted for Impact	To be determined
	T1565: Data Manipulation	To be determined
	T1496: Resource Hijacking	To be determined
	T1489: Service Stop	To be determined

Indicators of Compromise (IoCs):

Hashes:

- 004ba25f40b641a3a276b84ebdc44971
- 00773e87ad74417abaf825839c4dd014
- 00a276d2a09a49b684237013d26a91dc
- 00a60855a14e458896d70c052e22e11c
- 00e815ade8f3ad89a7726da8edd168df13f96ccb6c3daaf995aa9428bfb9ecf
- 010428443d5547a58995767d14d1c785
- 013f0f61bf96431e8a10e3cb982f4af5
- 01a0e1d97f97455a8da6012977169b40
- 01dc7dc6ad774b39a36d13d55d273a52

Internet Domain Name:

- 4ad.onion
- abcwdl.co.uk
- aclara.com
- adaresec.com
- aha.org
- ajoomal.com
- alektum.com
- alogent.com
- amerisave.com
- amf.se
- androidauthority.com
- antiy.cn
- arrow.com
- awaze.com
- axisbank.com

Malware Signature:

- BlackByte Ransomware
- IceFire Ransomware
- Conti Ransomware
- Akira Ransomware
- AtomSilo Ransomware
- Money Message Ransomware
- Karma Ransomware
- Snatch
- AvosLocker Ransomware
- Black Kingdom Ransomware
- Monti Ransomware
- Rorschach

IP Address:

- 103.151.172.28
- 109.172.45.28
- 109.172.45.77
- 141.98.82.201
- 143.244.188.172
- 146.70.116.20
- 147.78.47.219
- 147.78.47.231
- 147.78.47.235
- 147.78.47.241
- 157.230.143.100
- 158.255.2.244
- 158.255.2.245
- 158.255.225.25

Mentioning the CVEs, etc.:

- CVE-2021-30116
- CVE-2023-27532
- CVE-2023-40044
- CVE-2023-36884
- CVE-2018-4878
- CVE-2017-0144
- CVE-2017-11882
- CVE-2022-41040
- CVE-2019-11043
- CVE-2023-20269
- CVE-2021-26084
- CVE-2021-34527
- CVE-2023-3519
- CVE-2019-19781
- CVE-2023-28252
- CVE-2019-15846
- CVE-2021-45105
- CVE-2019-7192

5.1.13 CL0P Technical/Tactical Recommendations

The following tactical recommendations are designed to provide technical mitigations to CL0P's MITRE ATT&CK techniques. The techniques are categorized based on criticality level, as determined by their potential impact and risk to business continuity, data security, and operational resilience.

Grounded in MITRE's D3FEND mitigation knowledge graph, these recommendations outline prescriptive instructions, desired outcomes, and key considerations for implementation and resource allocation. These recommendations are not meant to be exhaustive but rather are most suited for mitigating the respective ATT&CK technique.

Recommendations for High-Criticality Attack Techniques:

T1190 (Exploit Public-Facing Applications)

1. Deploy and configure web application firewalls (WAFs) to filter malicious traffic: Implement WAFs to inspect and block exploit attempts targeting web applications, including SQL injection, cross-site scripting (XSS), and remote code execution (RCE). Configure rule sets to detect known attack patterns and anomalous request behaviors. Regularly update WAF policies to address emerging threats and reduce false positives. WAFs provide an essential layer of protection by filtering exploit traffic before it reaches the application.

2. Segment externally facing services from internal systems: Use a demilitarized zone (DMZ) or isolated hosting infrastructure to separate public-facing applications from internal networks. Implement strict firewall rules to control traffic flow between these segments and limit the exposure of sensitive resources. Enforce access controls to prevent lateral movement from compromised services. Network segmentation reduces the attack surface and mitigates the impact of a successful breach.

3. Regularly scan and patch externally facing applications: Conduct frequent vulnerability scans on public-facing systems to identify weaknesses before attackers exploit them. Establish a structured patch-management process to apply security updates promptly, prioritizing critical vulnerabilities. Use automated tools to track software versions and enforce update policies. Proactive scanning and patching help minimize the risk of exploitation through known vulnerabilities.

T1566 (Phishing)

1. Deploy advanced email-filtering solutions to detect and block phishing attempts: Implement secure email gateways (SEGs) with AI-driven filtering capabilities to analyze email headers, body content, and attachments for phishing indicators. Configure rules to block or flag emails containing suspicious links, unexpected attachments, or impersonation attempts. Use threat-intelligence feeds to update filtering mechanisms against evolving phishing tactics. Advanced filtering reduces the likelihood of phishing emails reaching end users.

2. Combine homoglyph detection with user training to prevent domain-impersonation attacks: Deploy tools that detect domain similarity to identify lookalike domains used in phishing campaigns. Implement continuous monitoring for newly registered domains that mimic internal or trusted domains. Conduct regular employee training sessions to enhance awareness of social-engineering tactics, domain-manipulation techniques, and suspicious email indicators. Provide hands-on exercises, phishing simulations, and real-world examples to reinforce recognition skills. A combined approach of automated detection and educated users significantly reduces the risk of falling victim to domain spoofing and spear-phishing attacks.

3. Implement anti-spoofing and email-authentication mechanisms to verify sender legitimacy: Implement a sender policy framework (SPF) to verify authorized email senders; DomainKeys Identified Mail (DKIM) to ensure message integrity; and Domain-Based Message Authentication, Reporting, and Conformance (DMARC) to define policies for handling unauthorized emails. Enforce these authentication mechanisms within the organization and encourage external partners to adopt them. Configure email-security policies to reject or quarantine messages that fail authentication checks. These measures reduce the risk of email spoofing and phishing-based impersonation attacks.

T1078 (Valid Accounts – Domain Accounts)

1. Continuously monitor domain accounts for unauthorized access: Deploy user behavior analytics (UBA) and anomaly-detection tools to identify deviations in login patterns, such as unusual locations, excessive failed attempts, or logins outside business hours. Configure automated alerts for suspicious activity and integrate with a security information and event management (SIEM) platform for investigation. Proactive monitoring helps detect compromised accounts before they can be exploited.

2. Enforce strong authentication and least-privilege access: Require multi-factor authentication (MFA) for all privileged accounts and enforce role-based access controls (RBAC) to limit account permissions. Implement just-in-time (JIT) access controls for high-privilege accounts to minimize persistent access risks. Regularly review and disable inactive accounts to reduce potential attack surfaces. These measures limit adversaries' ability to exploit valid credentials for lateral movement.

3. Regularly review and manage domain accounts: Conduct periodic audits of domain accounts to ensure only active and necessary accounts exist. Implement automated lifecycle management for account creation, modification, and deactivation based on user roles and employment status. Enforce strict offboarding procedures to immediately disable accounts when employees leave the organization. Reducing unnecessary accounts helps prevent adversaries from leveraging dormant credentials.

T1041 (Exfiltration Over C2 Channel)

1. Deploy both inbound and outbound traffic filtering at network boundaries, enforcing strict egress controls to known-good destinations and protocols: Implement application-layer filtering to allow only authorized data-transfer protocols and block commonly abused services. Configure filtering rules to segment different business units, especially those handling sensitive financial data, while maintaining logs of all blocked connection attempts. Consider performance impact on legitimate business traffic and allocate sufficient resources for real-time filtering without introducing latency.

2. Establish baseline profiles of normal client–server communication patterns specific to financial services applications and data flows: Deploy monitoring solutions that can analyze payload characteristics (e.g., size, frequency, and entropy) across all client–server communications. Configure automated alerts for any statistical deviations that could indicate data-exfiltration attempts while maintaining historical profiles for trend analysis. Consider the computational resources required for real-time profiling and the potential impact on system performance.

3. Implement comprehensive protocol metadata collection and analysis focusing on session characteristics, timing patterns, and protocol-specific attributes: Deploy real-time analysis capabilities that can identify statistical outliers in protocol usage, particularly protocols that could be used for data exfiltration. Set up adaptive thresholding based on historical protocol usage patterns while maintaining detailed logs for forensic analysis. Consider storage requirements for metadata collection and processing overhead for real-time analysis.

T1003.001 (LSASS Memory Dumping – Credential Theft)

1. Deploy process-monitoring tools that specifically track spawn attempts targeting local security authority subsystem service (LSASS) memory space and related system processes: Configure the detailed logging of process attributes (e.g., user context, image path, and security content) for all process-creation events. Implement automated alerts for any unauthorized process-spawn attempts targeting LSASS while maintaining whitelists for legitimate security tools. Consider the processing overhead of continuous process monitoring and storage requirements for process-creation logs.

2. Implement hardware-based isolation mechanisms using technologies such as IOMMU to prevent unauthorized memory access between processes: Configure strict memory-access controls that prevent direct memory access to LSASS process space from unauthorized sources. Deploy monitoring solutions to track any attempted violation of process isolation boundaries while maintaining business continuity for legitimate authentication processes. Consider the hardware requirements and potential performance impact on system resources.

3. Configure automated process-termination responses for any unauthorized processes attempting to access LSASS memory space: Implement proper access controls and permissions for process-termination capabilities while ensuring legitimate security tools remain functional. Set up logging and alerting for all process-termination events with detailed context about the terminated process and reason for termination. Consider the potential impact of false positives and establish clear escalation procedures for security teams.

Recommendations for Moderate- to High-Risk Attack Techniques:

T1059.001 (PowerShell Execution)

1. Set PowerShell execution policy to only allow signed scripts: Configure PowerShell to allow only signed scripts to run, preventing the execution of untrusted or malicious scripts. Restrict PowerShell usage to administrators to limit the attack surface. Doing so reduces the likelihood of malicious PowerShell-based attacks.

2. Disable/restrict the Windows Remote Management (WinRM) Service to prevent remote execution: Disable or limit access to the WinRM service to prevent attackers from executing PowerShell remotely. Use firewall rules to restrict WinRM access to trusted hosts only. Doing so prevents unauthorized use of PowerShell for remote command execution.

3. Use PowerShell Constrained Language Mode and application control: Enable PowerShell Constrained Language Mode to restrict access to sensitive functionality, such as executing arbitrary Windows APIs. Utilize application whitelisting tools to control which applications and scripts can run, reducing the potential for abuse. Doing so mitigates the risk of PowerShell being leveraged for malicious activities.

T1068 (Exploitation for Privilege Escalation)

1. Regularly assess and remediate system vulnerabilities: Perform routine vulnerability scans and manual security assessments to identify and mitigate system weaknesses. Implement a structured patch-management process to address critical security flaws before exploitation. Use configuration-management tools to enforce security baselines and harden guidelines. Regular assessments help reduce the attack surface and ensure compliance with security policies.

2. Restrict unnecessary services and enforce least privilege: Disable non-essential system services and restrict administrative-tool usage to minimize potential attack vectors. Implement RBAC and privilege management solutions to enforce the least-privilege principle. Regularly review user permissions and remove excessive access rights to reduce lateral movement opportunities. These measures significantly lower the risk of privilege escalation.

3. Deploy exploit detection and mitigation controls: Enable security mechanisms such as kernel-integrity verification, exploit-protection frameworks, and memory-based attack prevention. Utilize endpoint detection and response (EDR) solutions to monitor for behavioral indicators of privilege-escalation attempts. Configure logging and alerting to detect and respond to suspicious process injections or unauthorized modifications. These techniques enhance system resilience against exploitation attempts.

T1021.001 (Remote Desktop Protocol)

1. Restrict and monitor remote desktop protocol (RDP) access: Limit RDP access by enforcing network segmentation and firewall rules that block unnecessary external connections. Require VPN or zero-trust network access for remote desktop usage and enforce MFA for all RDP sessions. Implement strict access controls using allowlists for authorized IP addresses. These restrictions reduce exposure to brute-force attacks and unauthorized access attempts.

2. Detecting and analyzing abnormal RDP activity: Deploy network monitoring tools to analyze RDP session patterns, geolocation inconsistencies, and excessive failed login attempts. Use host and network-based anomaly detection to identify suspicious behavior, such as unexpected administrative logins or persistent connections. Implement alerting mechanisms for unusual RDP activity to enable rapid investigation and response. Monitoring reduces dwell time and helps identify potential intrusions.

3. Audit and control remote-access tools: Maintain a strict inventory of approved remote-access applications and prohibit the use of unauthorized tools through application whitelisting. Regularly audit endpoint and network logs for indicators of unauthorized remote-access attempts. Enforce execution-control policies to prevent unapproved portable remote-access software from running. Doing so ensures only sanctioned remote management tools are used, reducing the risk of compromise.

T1021.002 (SMB/Windows Admin Shares)

1. Filter and monitor SMB network traffic to detect unauthorized access: Apply network segmentation and firewall rules to restrict SMB traffic to only authorized systems. Monitor SMB authentication logs and detect anomalous access patterns, such as unexpected connections or excessive failed login attempts. Analyzing traffic helps prevent unauthorized access and data exfiltration over SMB.

2. Deny remote use of local admin credentials to log into systems: Restrict the use of local administrator accounts for remote logins by enforcing Group Policy settings and implementing the Local Administrator Password Solution (LAPS). Ensure that unique and complex passwords are used for each system's local administrator account. Preventing credential reuse reduces the risk of lateral movement if an account is compromised.

3. Monitor for remote execution attempts using WMI and SMB shares: Deploy endpoint monitoring to detect the use of WMI's Win32_Process class and the creation of remote processes through SMB. Correlate activity with known attack techniques to identify potential lateral movement or remote code-execution attempts. Early detection of abnormal behavior helps prevent unauthorized system compromise.

T1574.002 (DLL Side-Loading)

1. Enforce strict application controls to prevent unauthorized dynamic link library (DLL) execution: Use application whitelisting to allow only trusted applications and libraries to execute. Implement code-signing verification to prevent the execution of unsigned or tampered DLLs. Restricting DLL execution ensures adversaries cannot exploit weak application controls for persistence.

2. Regularly update software to patch DLL side-loading vulnerabilities: Maintain an effective patch-management process to address known DLL side-loading risks. Review application dependencies and remove or replace vulnerable libraries with secure versions. Keeping software updated reduces the risk of adversaries exploiting outdated DLL loading mechanisms.

3. Enable behavioral-based detections to identify DLL side-loading techniques: Use EDR capabilities to detect anomalies such as a process-loading DLL from non-standard directories, unexpected DLL injection into high-privilege applications, or abnormal memory-access patterns. Implement heuristic and machine-learning-based detections to flag deviations from normal DLL loading behavior.

T1548.002 (Bypass User Account Control)

1. Harden User Account Control (UAC) settings and monitor for bypass attempts: Enable UAC in "Always Notify" mode to require explicit approval for administrative actions. Conduct regular assessments to identify systems with weak UAC configurations and enforce security best practices. Disabling auto-elevation prevents attackers from leveraging system utilities to bypass UAC controls. Strengthening UAC configurations reduces the attack surface and minimizes unauthorized privilege-escalation attempts.

2. Monitor process execution for suspicious UAC bypass attempts: Track the execution of known UAC bypass tools and processes, such as eventvwr.exe and sdclt.exe, that can elevate privileges without user consent. Implement endpoint-detection rules to correlate process execution with privilege-escalation events and flag anomalous behavior. Organizations should use behavioral analytics to identify patterns indicative of UAC bypass techniques. Early detection of unauthorized privilege-elevation attempts allows for timely response and mitigation.

3. Implement executable denylisting to prevent unauthorized privilege escalation: Use application-control policies to block the execution of untrusted administrative utilities commonly abused for UAC bypass. Maintain an up-to-date denylist of known bypass techniques to proactively mitigate threats. Enforce strict execution policies using operating-system security controls to block non-administrative users from executing high-risk binaries. Preventing the execution of malicious or unapproved applications reduces the attack surface and strengthens endpoint security.

T1133 (External Remote Services)

1. Implement automated session-termination controls for all external remote services including VPN and remote management tools with strict timeout parameters: Configure forced session disconnection after a period of inactivity while maintaining detailed logs of all termination events for audit purposes. Ensure that session-termination policies account for legitimate business needs while preventing unauthorized persistence through abandoned sessions. Consider the impact on user productivity and establish clear communication channels for users who require extended sessions.

2. Implement network segmentation using proxies, gateways, and firewalls to control and monitor all remote-access paths into the network: Deploy a defense-in-depth approach that forces all remote connections through designated security checkpoints while maintaining detailed access logs. Configure strict boundary controls that prevent direct remote access to internal systems while ensuring business continuity through properly secured access channels. Consider the complexity of implementing segmentation and the potential impact on network performance and legitimate remote-access needs.

3. Deploy MFA for all external remote service accounts including VPN and remote management tools: Implement a robust MFA solution that combines multiple authentication factors while being aware of potential MFA interception techniques. Configure the detailed logging of all authentication attempts while maintaining proper procedures for handling legitimate MFA issues or lockouts. Consider the user-experience impact, support-resource requirements, and the need for backup authentication methods for critical access scenarios.

Stealth and Persistence Risk (Evasion & Long-Term Compromise):

T1140: (Deobfuscate/Decode Files or Information)

1. Monitor and log process execution to detect file extraction or decryption attempts: Implement process monitoring to detect the execution of file-extraction utilities and scripts attempting to decrypt or manipulate files. Correlate activity with unauthorized file modifications or unexpected system behavior to identify potential malicious activity while reducing false positives.

2. Restrict and validate script execution to prevent unauthorized decoding attempts: Configure logging to capture script executions, especially those occurring outside of standard administrative tasks. Restrict unauthorized script execution and analyze captured scripts for potential malicious intent. Monitoring script activity helps identify adversary attempts to automate obfuscation or payload decoding.

3. Detect and block misuse of built-in utilities commonly used for deobfuscation: Monitor the usage of built-in system utilities that can be leveraged for decoding, extracting, or modifying files. Set up alerts for unauthorized or unexpected executions and correlate them with system activity. Detecting the misuse of such utilities early can prevent unauthorized data access and the execution of malicious code.

T1070.002: (Clear Linux or Mac System Logs)

1. Encrypt and centralize log storage: Use strong encryption protocols to protect system logs at rest and in transit, preventing unauthorized modifications. Implement centralized logging solutions that forward logs to secure remote storage with integrity-verification mechanisms, such as cryptographic hashing. Encrypted and centralized logs ensure forensic integrity and prevent attackers from tampering with evidence.

2. Enforce strict log access controls: Apply granular file permissions to restrict log modification and deletion rights to authorized system processes and administrators. Implement mandatory access control (MAC) frameworks to enforce security policies at the operating-system level. Regularly audit log access permissions to identify and mitigate potential privilege abuse. These controls help prevent attackers from erasing forensic evidence.

3. Monitor and alert on log-tampering attempts: Configure security monitoring tools to track log-file modifications, deletions, and unexpected clearing activities. Implement real-time alerting mechanisms to notify security teams when unauthorized log tampering is detected. Correlate log events across multiple sources to identify patterns of malicious activity. Continuous monitoring helps detect and mitigate threats before they escalate.

T1574.00: (Registry Run/Startup Folder)

1. Deploy file integrity monitoring focused on Windows Registry run keys and startup folder location with real-time/near real-time alerting for modifications: Implement baseline comparisons that track any changes to autostart locations while maintaining detailed audit logs of all modifications. Configure whitelisting for known good startup entries while ensuring proper change-management procedures for legitimate modifications. Consider the performance impact on continuous monitoring and storage requirements for audit logs.

2. Implement strict application-allowlisting controls that prevent unauthorized executables from being added to startup locations or run keys: Configure policies that only permit trusted/signed applications to continue through startup procedures while maintaining a comprehensive inventory of approved applications. Set up automated alerts

for any attempted violations of allowlisting policies while ensuring business continuity for legitimate software updates. Consider the administrative overhead of maintaining allowlists and the impact on software deployment processes.

3. Deploy continuous monitoring of system-initialization configurations related to the registry and startup folder: Implement analysis capabilities that can detect anomalous changes to startup configurations while maintaining baselines of legitimate startup entries. Configure automated responses to unauthorized configuration changes.

T1078.003: (Local Accounts – Persistence)

1. Monitor local-account creation, modification, and usage patterns across all systems: Deploying real-time alerting for suspicious local-account activities can help detect potential malicious activity associated with off-hours usage, unauthorized privilege escalation, or unusual access patterns. Configure detailed logging of all local account operations while maintaining baselines of normal account behavior. Consider the storage requirements for account activity logs and processing overhead for real-time analysis.

2. Deploy automated account locking triggered by suspicious activities or policy violations on local accounts: Implement progressive lockout policies that increase lockout duration with repeated violations while maintaining proper procedures for legitimate account unlocking. Configure notifications for security teams when accounts are locked due to suspicious activity while ensuring business continuity through proper backup access procedures for critical services. While lockout mechanisms may evict threat actors, consider the impact on legitimate users and help-desk resource protocols for secure account unlocking requests.

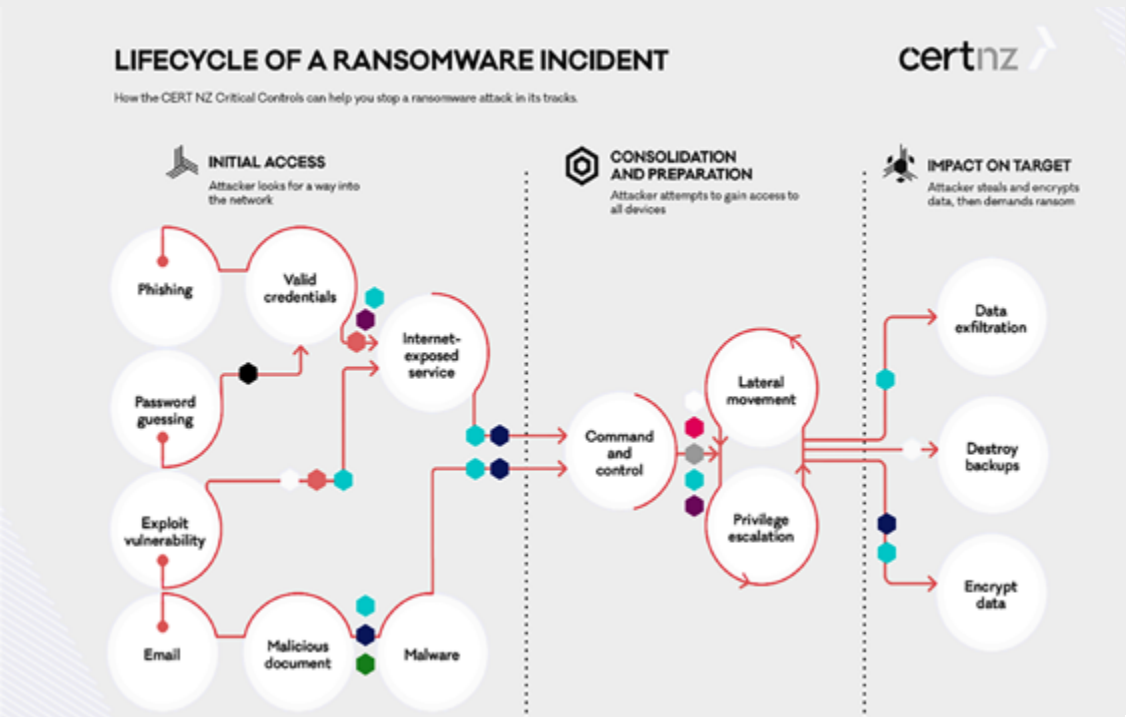
3. Implement strict permission controls and access restrictions for all local accounts based on the principle of least privilege (PoLP): Configure regular permission reviews and automated detection of unauthorized privilege changes while maintaining detailed documentation of approved access levels. Establish alerts for any attempts to modify account permissions while ensuring proper change-management procedures for legitimate permission updates. Consider the administrative overhead of managing granular permissions and the impact on operational efficiency.

5.2 LockBit

5.2.1 Relevant Threat-Actor Activity

LockBit is a highly active ransomware group primarily targeting medium-to-large-sized businesses, including Royal Mail, Ion Group, and TSMC.[205] The group gains initial access to target networks through purchased access, unpatched vulnerabilities, insider access, and zero-day exploits. LockBit is designed to operate in the United States, Canada, Europe, Asia, and Latin America. In late February of 2024, LockBit underwent a significant takedown in which over 200 cryptocurrency accounts were frozen, sanctions were enforced, and 34 servers and 14,000 accounts were shut down.[206] Since then, this takedown has significantly disrupted LockBit's activities. However, despite substantial law enforcement, LockBit remains the most prominent ransomware organization.[207]

Figure 6: Lifecycle of a Ransomware Incident



Source: CISA[208]

[205] https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware spotlight-lockbit
[206] https://globalinitiative.net/analysis/the-lockbit-takedown law-enforcement-trolls-ransomware-gang/
[207] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a
[208] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a

LockBit operates as a RaaS model, recruiting affiliates to execute ransomware attacks using LockBit tools and infrastructure. This results in significant variation in TTPs across different attacks.[209] A standard method used by LockBit affiliates involves exploiting unpatched vulnerabilities or using compromised credentials to gain initial access to a target network. Once inside, they often deploy tools like Mimikatz to extract credentials and escalate privileges, allowing lateral movement across the network. Data can be reached and compromised through these methods, allowing for data exfiltration or encryption.

The impact of LockBit has been profound, particularly in Latin America financial institutions, leading to significant disruptions and financial losses. It was reported that RaaS groups, including LockBit, have exerted continuous pressure on the region's economic- and government-services sectors.[210] Since April 2022, countries such as Costa Rica, Peru, Mexico, Ecuador, Brazil, and Argentina have faced ransomware attacks, likely involving Russian-speaking threat actors, including LockBit.[211]

5.2.2 Background

Lockbit was first observed in September 2019 and has evolved through multiple versions, with the current version, LockBit 3.0, discovered in June 2022. LockBit maintained the top position throughout 2022, accounting for over a third of victim organizations in the first three quarters.[212] Lockbit maintains a strong presence in Latin America. In October 2022, ransomware occurred in a bank in Brazil using the LockBit malware. The attackers requested 50 bitcoins—the equivalent of 1 million USD—and caused data leakage and temporary disruptions in client services.

In addition to this incident, LockBit's victims span various sectors. Among the most significant is the private sector, where LockBit has targeted industries ranging from finance to manufacturing.[213] The group has also impacted other critical-infrastructure sectors, such as energy, healthcare, and transportation.[214] Furthermore, governmental entities have been affected, leading to national crises, as seen in the case of Costa Rica.[215] These industries are particularly appealing to LockBit due to their high importance, data sensitivity, and potential to create national crises. Their substantial financial resources also make them lucrative targets, increasing the likelihood of ransom payments.

5.2.3 Correlation

LockBit attacks often use a double-extortion strategy to pressure victims into paying, first to recover access to their encrypted files and second to stop their stolen data from being publicly released. This double-extortion technique, in particular, allows LockBit to not only profit from the data ransom but also recover data from the user's end and potentially even utilize additional data leakage if the victim does not comply.

LockBit and CL0P operate as RaaS, using affiliates or initial access brokers (IABs) to deploy the initial malware or secure access to a target organization's systems. Like LockBit, CL0P has gained notoriety for its large-scale attacks, such as exploiting zero-day vulnerabilities in widely used software such as MOVEit. Moreover, both groups use techniques like DLL side-loading and advanced persistence mechanisms to maintain control of compromised systems.

5.2.4 LockBit Techniques, Tactics, & Procedures

LockBit employs sophisticated TTPs to compromise and control victim networks. For privilege escalation, LockBit uses methods such as bypassing User Account Control (UAC) via the ucmDccwCOM Method from UACMe, exploiting boot or login autostart execution and modifying domain policies through Group Policy to allow its control over systems.

Additionally, it employs token impersonation to replicate and assume the privileges of other processes, causing deeper network infiltration. LockBit also exploits zero-day and n-day vulnerabilities to gain unauthorized access and execute remote code, with notable cases including the exploitation of the Fortra GoAnywhere MFT Vulnerability (CVE-2023-0669) and the Apache Log4j2 Vulnerability.

LockBit utilizes tools such as Splashtop for remote access and Cobalt Strike for navigating networks in lateral movement. By targeting SMB shares and utilizing Admin Shares or Domain Group Policy, LockBit affiliates achieve seamless movement across compromised environments.

[209] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a
[210] https://doi.org/102279083/1729705714101/module_128102279083_Global-Header
[211] https://www.recordedfuture.com/research/latin-american-governments targeted-by-ransomware
[212] https://global.ptsecurity.com/analytics/latam-cybersecurity-threatscape-2022-2023
[213] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a
https://www.logpoint.com/wp-content/uploads/2023/07/etp-lockbit.pdf
[214] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a
[215] https://www.recordedfuture.com/research/latin-american-governments targeted-by-ransomware

For command and control, the ransomware group relies on various protocols and software, including FileZilla for file transfers, ThunderShell for HTTP-based remote access, and Ligolo for creating secure SOCKS5 tunnels. Tools such as Plink automate SSH activities, while commonly used in remote-access software like AnyDesk and TeamViewer, further facilitate LockBit's ability to maintain access to infected systems. The following table, representing LockBit's tactics, techniques, and procedures, showcase LockBit's flexible operation and persistence, posing a severe threat to cybersecurity across various sectors, particularly in LATAM.[216]

Tactics	Techniques	Procedures
Execution (TA0002)	T1059.003: Windows Command Shell	Abuses Windows command prompt to access almost any part of the system
	T1072: Software Development Tools	Leverages system services to execute or launch malicious code as a persistence mechanism
	T1569.002: System Services	Uses PsExec to execute commands or payloads
Persistence (TA0003)	T1547: Boot or Logon Autostart Execution	Enables automatic logon for persistence
	T1078: Valid Accounts	Uses compromised user accounts to maintain persistence on the target network
Initial Access (TA0001)	T1189: Drive-By Compromise	LockBit affiliates gain access through a user visiting a compromised website
	T1190: Exploit Public-Facing Application	Exploits vulnerabilities (e.g., Log4Shell) in internet-facing systems
	T1133: External Remote Services	Exploits RDP to gain access to victims' networks
	T1566: Phishing	Uses phishing and spear-phishing to gain network access
Privilege Escalation (TA0004)	T1548: Abuse Elevation Control Mechanism	Uses User Account Control (UAC) bypass techniques (e.g., ucmDccwCOM method)
	T1547: Boot or Logon Autostart Execution	Enable automatic logon for privilege escalation
	T1484.001: Domain Policy Modification: Group Policy Modification	Modifies Group Policy for lateral movement.
	T1078: Valid Accounts	Uses compromised user accounts to escalate privileges
Defense Evasion (TA0005)	T1480.001: Execution Guardrails: Environmental Keying	Decrypts or continues execution only if certain environmental factors are present
	T1562.001: Impair Defenses: Disable or Modify Tools	Disables EDR tools (e.g., using Backstab, Process Hacker, etc.)
	T1070.001: Indicator Removal: Clear Windows Event Logs	Clears Windows Event Log files to avoid detection
	T1070.004: Indicator Removal: File Deletion	LockBit 3.0 deletes itself from the disk after execution

[216] https://www.logpoint.com/wp-content/uploads/2023/07/etp-lockbit.pdf

Tactics	Techniques	Procedures
	T1027: Obfuscated Files or Information	Encrypts or obfuscates host and bot information during communication with C2 servers
	T1027.002: Obfuscated Files or Information: Software Packing	Uses software packing or virtual machine protection to conceal code
Credential Access (TA0006)	T1110: Brute Force	Uses brute force VPN or RDP credentials for initial access
	T1555.003: Credentials from Password Stores: Credentials from Web Browsers	Recovers stored credentials from Firefox using PasswordFox
	T1003: OS Credential Dumping	Uses tools like ExtPassword or LostMyPassword to recover system credentials
	T1003.001: OS Credential Dumping: LSASS Memory	Uses Microsoft Sysinternals ProDump or Mimikatz to dump credentials from LSASS
Discovery (TA0007)	T1046: Network Service Discovery	Uses SoftPerfect Network Scanner, Advanced IP Scanner, or Advanced Port Scanner to scan victim networks
	T1082: System Information Discovery	Enumerates system information, including hostname, configuration, and domain information
	T1614.001: System Location Discovery: System Language Discovery	LockBit 3.0 avoids infecting systems with specific language settings based on an exclusion list
Lateral Movement (TA0008)	T1021.001: Remote Services: Remote Desktop Protocol.	Uses Splashtop or similar remote desktop software to facilitate lateral movement
	T1021.002: Remote Services: Server Message Block (SMB)/Admin Windows Shares	Uses Cobalt Strike to target SMB shares for lateral movement
Collection (TA0009)	T1560.001: Archive Collected Data: Archive via Utility	Uses 7-zip to compress or encrypt data before exfiltration
Command and Control (TA0011)	T1071.002: Application Layer Protocol: File Transfer Protocols	Uses FileZilla to communicate with C2
	T1071.001: Application Layer Protocol: Web Protocols	Uses ThunderShell to communicate via HTTP requests
	T1095: Non-Application Layer Protocol	Uses Ligolo to establish SOCKS5 or TCP tunnels from reverse connections
	T1572: Protocol Tunneling	Uses PuTTY Link (Plink) to automate SSH actions on Windows
	T1219: Remote-Access Software	Uses AnyDesk, Atera RMM, ScreenConnect, or TeamViewer for remote access
Exfiltration (TA0010)	T1567: Exfiltration Over Web Service	Uses publicly available file-sharing services to exfiltrate data
	T1567.002: Exfiltration Over Web Service: Exfiltration to Cloud Storage	Uses tools like Rclone or FreeFileSync to exfiltrate data to cloud storage (e.g., MEGA)

Tactics	Techniques	Procedures
Impact (TA0040)	T1485: Data Destruction	Deletes log files and empties the recycle bin to prevent recovery of information
	T1486: Data Encrypted for Impact	Encrypts data on target systems to disrupt availability of network resources
	T1491.001: Defacement: Internal Defacement	Changes the system's wallpaper and icons to LockBit branding
	T1490: Inhibit System Recovery	Deletes volume shadow copies to prevent system recovery
	T1489: Service Stop	Terminates processes and services to facilitate encryption and prevent recovery

IOCs:

- File hashes
- IP addresses
- Domain names
- Malicious URLs
- Ransom notes

CVEs:

- Proxy Shell: CVE-2021-34473, CVE-2021-34523, CVE-2021-31207
- Paper Cut: CVE-2023-27350
- Citrix Bleed: CVE-2023-4966 (Latest)
- CVE-2022-22279
- CVE-2021-31207, CVE-2023-4966
- CVE-2021-22986
- CVE-2018-13379
- CVE-2021-36942
- CVE-2021-20028
- CVE-2020-0787
- CVE-2022-36537

5.2.5 LockBit Technical/Tactical Recommendations

Recommendations for Critical-Attack Techniques with High Impact on Business & Data Security

The tactical recommendations below are designed to mitigate LockBit's techniques, following the MITRE ATT&CK framework. They are categorized based on the extent of their impact, with higher criticality levels indicating a greater risk, such as a potential network takeover. Therefore, these recommendations outline key considerations and actions that can be taken to mitigate the associated ATT&CK techniques.

T1133 (External Remote Services)

1. Enforce multi-factor authentication (MFA) for all remote access: Require MFA and cloud-based remote access to prevent unauthorized logins, even if credentials are compromised. Use phishing-resistant authentication methods, such as FIDO2 or certificate-based authentication. MFA significantly reduces the risk of unauthorized access.

2. Restrict remote access with network segmentation and allowlisting: Limit remote access to approved IP ranges and enforce network segmentation to isolate remote services from critical financial systems. Use Zero Trust Network Access (ZTNA) and role-based access controls (RBAC) to minimize exposure. Restricting access reduces the attack surface and limits lateral movement.

3. Monitor and log remote-access sessions for anomalies: Deploy security information and event management (SIEM) solutions to log and analyze remote-access sessions. Enable behavior-based anomaly detection to flag unusual login attempts, such as off-hours access or logins from new locations. Real-time monitoring facilitates the detection of and response to unauthorized access.

T1078 (Valid Accounts)

1. Enforce least-privilege and account segmentation: Limit account permissions based on the principle of least privilege (PoLP). Implement separate accounts for administrative and non-administrative tasks to reduce exposure. Use just-in-time (JIT) access provisioning and RBAC to minimize persistent high-privilege access. Restricting access helps mitigate the risk of account misuse.

2. Strengthen authentication and credential security: Require MFA for all privileged and sensitive accounts, prioritizing phishing-resistant methods, such as FIDO2 or certificate-based authentication. Enforce strong password policies, including length and complexity requirements, and implement password managers to reduce credential reuse. Regularly rotate credentials and disable inactive accounts to prevent unauthorized access.

3. Detect and respond to unauthorized account use: Monitor account activity using SIEM and user and entity behavior analytics (UEBA) solutions. Flag anomalous behavior, including access from new locations, excessive login attempts, or privilege escalation. Enable automated alerts and implement real-time response mechanisms to detect and contain potential account compromises.

T1566 (Phishing)

1. Implement advanced email security and filtering: Deploy secure email gateways (SEGs) and advanced phishing-protection solutions to filter out malicious emails before they reach users. Enable domain-based email-authentication protocols, such as SPF, DKIM, and DMARC, to prevent email spoofing. Use AI-driven threat detection to identify and quarantine phishing attempts in real time.

2. Conduct continuous user-awareness training and simulated phishing tests: Educate employees on recognizing phishing attempts, including social-engineering tactics, malicious attachments, and deceptive links. Regularly conduct phishing simulations to test user awareness and provide targeted training based on performance. Reinforce a culture of cybersecurity vigilance to reduce the likelihood of successful phishing attacks.

3. Deploy anti-phishing browser protections and URL analysis: Use web filtering and domain reputation services to block access to known phishing sites. Implement browser isolation for high-risk users and automatically scan URLs in emails for malicious indicators before allowing access. Encourage the use of password managers to prevent credential harvesting by auto-filling only on legitimate sites.

T1003 (OS Credential Dumping)

1. Implement credential-protection mechanisms to prevent unauthorized access to stored credentials: Configure Windows Defender Credential Guard to protect LSASS memory and prevent credential-dumping attacks. Use EDR solutions to detect suspicious access attempts targeting credential stores. Disable unnecessary administrative privileges to limit exposure to credential-dumping techniques. These protections help prevent attackers from extracting stored credentials.

2. Restrict access to sensitive system processes and enforce process auditing: Configure endpoint security solutions to monitor and block unauthorized access to LSASS and registry hives containing stored credentials. Implement process auditing to log and alert on attempts to access credential stores. Regularly review security logs and conduct forensic analysis on suspicious events. Monitoring process interactions helps detect and prevent credential-dumping attempts.

3. Deploy strong credential encryption and minimize credential storage: Use strong encryption standards for credential storage and enforce security best practices for managing secrets. Implement JIT privilege escalation to reduce persistent access to high-value accounts. Minimize password caching on endpoints to limit credential exposure. Strengthening credential storage reduces the risk of successful credential-dumping attacks.

T1486 (Data Encrypted for Impact – Ransomware)

1. Deploy robust endpoint protection and behavior-based ransomware detection: Implement next-generation antivirus (NGAV) and EDR solutions to monitor ransomware-specific behaviors, such as mass file encryption, deletion of backups, and unauthorized registry changes. Configure automatic containment of infected devices to prevent ransomware propagation. Early detection of encryption related activity helps mitigate the impact of ransomware attacks.

2. Enforce strict data-backup policies with immutable storage and offline recovery: Implement a 3-2-1 backup strategy with offline, immutable backups stored separately from production environments. Regularly test backup-restoration procedures to ensure a quick recovery from ransomware attacks. Use backup encryption and access controls to protect stored data from unauthorized modifications. Secure backups provide a critical recovery mechanism in case of ransomware infection.

3. Implement network segmentation and application allowlisting to prevent ransomware spread: Segment critical banking infrastructure from general IT environments using strict access controls and firewall policies. Deploy application allowlisting to prevent unauthorized execution of ransomware payloads. Monitor file-system changes and restrict write access to sensitive directories. Isolating critical systems reduces the attack surface and limits the impact of a ransomware outbreak.

T1567.002 (Exfiltration Over Web Service: Exfiltration to Cloud Storage)

1. Implement Data Loss Prevention (DLP) solutions to monitor and restrict unauthorized data transfers: Deploy DLP solutions to monitor, log, and block unauthorized data transfers to external cloud storage services such as Google Drive, Dropbox, and OneDrive. Configure policies to detect anomalous data movement and enforce automatic encryption of sensitive financial data before transfer. DLP solutions help prevent unauthorized exfiltration of sensitive banking data.

2. Monitor and restrict access to cloud storage services from financial institution networks: Implement firewall and proxy controls to restrict access to unauthorized cloud storage platforms. Use Secure Access Service Edge (SASE) solutions to enforce content filtering and detect suspicious data uploads. Configure alerts for high-volume data transfers and unusual access patterns indicative of exfiltration attempts. Restricting access to external storage services minimizes exfiltration risks.

3. Encrypt sensitive financial data at rest and in transit to prevent unauthorized exposure: Use strong encryption protocols (AES-256, TLS 1.2+) for all sensitive financial data stored or transmitted within the organization. Enforce strict access controls and MFA for cloud storage access. Implement logging and monitoring for cloud storage interactions to detect and investigate anomalies. Encrypting sensitive data mitigates the risk of unauthorized disclosure, even if exfiltrated.

Recommendations for High-Risk Attack Techniques with Severe Operational & Security Risks

T1547 (Boot or Logon Autostart Execution)

1. Enforce application control and prevent unauthorized persistence mechanisms: Implement application allowlisting using Windows Defender Application Control (WDAC) or AppLocker to prevent unauthorized execution of malware at system startup. Restrict administrative privileges to prevent unauthorized registry modifications, scheduled task creation, or service installations. Enforce digital signature verification to ensure only trusted applications can persist. These measures reduce the ability of attackers to establish persistence through startup mechanisms.

2. Monitor and audit system startup configurations for anomalies: Deploy EDR solutions to monitor modifications to startup locations such as the Windows registry, scheduled tasks, and service

configurations. Configure security information and event management (SIEM) alerts for unauthorized changes to auto-start entries. Regularly audit system startup settings to identify and remove suspicious persistence mechanisms. Continuous monitoring helps detect and respond to unauthorized modifications before adversaries can leverage them.

3. Harden system integrity and enforce secure boot mechanisms: Enable Secure Boot to prevent unauthorized boot modifications and ensure only trusted OS components load at startup. Implement tamper protection for critical system configurations to prevent adversaries from modifying autostart entries. Use host-based intrusion prevention systems (HIPS) to block suspicious persistence attempts. Hardening boot processes reduces the risk of malware persistence in banking terminals and ATMs.

T1484.001 (Domain Policy Modification: Group Policy Modification)

1. Implement role-based access control (RBAC) to restrict domain policy modifications: Restrict Group Policy modification privileges to a limited set of administrators. Use privileged access management (PAM) solutions to enforce just-in-time (JIT) access and prevent unauthorized changes. Regularly review and remove unnecessary administrative privileges. These measures limit the attacker's ability to manipulate security policies for lateral movement.

2. Continuously monitor and log Group Policy changes: Deploy SIEM solutions to log and alert on Group Policy modifications. Use Microsoft Advanced Threat Analytics (ATA) or Azure Sentinel to detect suspicious policy changes indicative of an attack. Regularly review domain controller logs to identify unauthorized modifications. Monitoring policy changes helps detect and respond to malicious activity before it spreads across the network.

3. Enforce secure baseline configurations and backup Group Policy objects (GPOs): Implement a secure baseline configuration using CIS benchmarks or Microsoft Security Baselines. Regularly backup Group Policy Objects (GPOs) and enable rollback capabilities to restore security settings in case of compromise. Use version control and audit logs to track changes and revert unauthorized modifications. Secure baselines and backups ensure quick recovery from malicious policy alterations.

T1562.001 (Impair Defenses: Disable or Modify Tools)

1. Implement endpoint protection with tamper-proof security controls: Deploy EDR solutions with tamper protection to prevent adversaries from disabling security tools. Restrict administrative access to security software and enforce role-based access control (RBAC) to limit modification privileges. Lock down security settings with group policies to prevent unauthorized changes. These protections prevent attackers from disabling defenses during an attack.

2. Monitor and log security tool modifications: Configure SIEM solutions to log and alert on security tool modifications, such as antivirus disabling, logging being turned off, or firewall rules being changed. Deploy host-based intrusion prevention systems (HIPS) to detect and block unauthorized attempts to modify security configurations. Regular monitoring ensures rapid detection of adversarial attempts to disable security tools.

3. Restrict execution of scripts and administrative tools used for disabling defenses: Implement PowerShell script block logging and enforce execution policies to prevent unauthorized scripts from modifying security configurations. Restrict the use of tools such as Process Hacker, GMER, and PsExec that attackers commonly use to disable security defenses. Using applications that allow listing, block execution of unauthorized security-disabling tools. These measures help maintain the integrity of security defenses.

T1046 (Network Service Discovery)

1. Limit exposure of network services through firewall and access controls: Restrict inbound and outbound traffic to essential services only using strict firewall rules. Disable unnecessary services and network protocols on critical banking infrastructure. Implement network segmentation to isolate high-value systems from general IT environments. Restricting service exposure reduces the attack surface for adversarial reconnaissance.

2. Deploy network monitoring and anomaly detection for unauthorized scans: Use intrusion detection systems (IDS) and network traffic analysis (NTA) tools to monitor for anomalous network scanning activities. Configure SIEM solutions to generate alerts on excessive network connection attempts or unusual service queries. Implement deception technology (honeypots) to detect and track attackers attempting network reconnaissance. Monitoring network activity enables early detection of threat actor reconnaissance attempts.

3. Harden network protocols and enforce strict authentication: Disable legacy protocols such as SMBv1 and enforce TLS encryption on all network communications. Implement mutual authentication for sensitive network services to prevent unauthorized access. Require certificate-based authentication for remote administrative services. Strengthening network security protocols makes service discovery more difficult for attackers.

T1082 (System Information Discovery)

1. Restrict access to system and hardware information: Configure group policies to prevent non-administrative users from accessing system information commands such as systeminfo, wmic, and tasklist. Disable remote access to system enumeration tools on banking endpoints. Prevent adversaries from collecting detailed information about financial institution infrastructure.

2. Deploy endpoint monitoring to detect suspicious discovery activities: Use EDR solutions to monitor and alert on system enumeration commands executed by unauthorized users. Configure SIEM rules to log and flag attempts to access system details. Detecting reconnaissance activity early helps prevent further exploitation.

3. Enforce strict access controls for system management tools: Restrict administrative access to system management utilities such as PowerShell, WMI, and Task Scheduler. Use just-in-time (JIT) privilege escalation to grant temporary access only when necessary. Regularly audit access logs for unusual queries against system information databases. These measures limit an attacker's ability to gather intelligence on banking infrastructure.

T1021.001 (Remote Services: Remote Desktop Protocol – RDP)

1. Restrict RDP access with strong authentication and network segmentation: Implement MFA for all RDP connections. Restrict RDP access using firewalls, allowing only pre-approved IP addresses. Use virtual desktop infrastructure (VDI) with brokered authentication to limit direct exposure of RDP services. Enforcing strict access controls reduces unauthorized remote access attempts.

2. Monitor and log RDP session activity to detect unauthorized access: Enable logging for RDP sessions, capturing successful and failed connection attempts. Configure SIEM solutions to generate alerts for anomalous RDP usage, such as logins from unusual locations or repeated failed attempts. Implement behavioral analytics to detect compromised RDP sessions. Continuous monitoring helps detect unauthorized remote access attempts.

3. Harden RDP settings and implement session security controls: Configure RDP to use network level authentication (NLA) to prevent unauthorized access before authentication. Enforce TLS encryption for all RDP traffic. Use time-based access controls to limit RDP access to predefined maintenance windows. Regularly review RDP session logs to identify suspicious activity. Hardening RDP configurations reduces the risk of unauthorized access and lateral movement.

Recommendations for Indirect Impact Attach Techniques Used for Lateral Movement & Evasion

T1059.003 (Windows Command Shell – Executes scripts to automate malicious actions in financial systems)

1. Restrict execution of unauthorized command-line scripts and commands: Implement application allowlisting using Windows Defender Application Control (WDAC) or AppLocker to block unauthorized execution of cmd.exe and batch scripts. Enforce PowerShell script block logging and execution policies to prevent malicious scripts from running. Limit access to command-line interpreters for non-administrative users. Restricting command shell execution prevents adversaries from automating malicious actions within financial systems.

2. Monitor and log suspicious command-line activity: Deploy EDR solutions to track command-line usage and detect suspicious scripts executing system modifications. Configure SIEM alerts to flag unusual shell commands such as net user, taskkill, or reg add. Proactively monitoring shell activity allows security teams to detect and mitigate unauthorized script execution.

3. Enforce strict access controls on administrative command execution: Implement JIT privilege escalation to restrict access to administrative command-line interfaces. MFA is required for privileged sessions using cmd.exe or PowerShell. Log all administrative shell activities for forensic analysis. These measures limit adversaries' ability to execute malicious scripts and maintain persistence in banking systems.

T1072 (Software Development Tools – Utilized to compile and execute malicious code within banking environments)

1. Restrict installation and execution of unauthorized development tools: Use application allowlisting to prevent unauthorized execution of compilers, scripting environments, and development

frameworks within banking networks. Limit installation permissions for tools such as Visual Studio, GCC, and Python to authorized users only. Blocking unapproved software development tools reduces the risk of adversaries compiling and executing malicious code.

2. Monitor developer tool usage for anomalies: Deploy endpoint monitoring solutions to track the execution of software development tools and identify unauthorized usage. Configure SIEM rules to generate alerts when suspicious code compilation or execution occurs outside approved development environments. Continuous monitoring ensures rapid detection of adversarial use of development tools.

3. Enforce strict code execution policies in financial systems: Digital signature verification is required for all executables and scripts before execution. Implement sandboxing for unverified code execution to prevent direct interaction with production systems. Use EDR to analyze the behavior of compiled binaries before allowing execution. Enforcing execution controls mitigates the risk of malicious code being deployed in banking networks.

T1110 (Brute Force – Attempts to crack banking credentials for unauthorized access)

1. Enforce strong password policies and account lockout mechanisms: Require complex passwords with a minimum length of 12-15 characters and enforce automatic password expiration. Implement account lockout policies after multiple failed login attempts to prevent brute-force attacks. Use password blacklisting to prevent the use of standard or easily guessed passwords. Strong authentication policies significantly reduce the effectiveness of brute-force attacks.

2. Deploy anomaly detection for login attempts and implement multi-factor authentication (MFA): Use behavioral analytics to detect abnormal login activity, such as repeated failed attempts from a single IP address. Implement MFA for all privileged accounts and remote access points to prevent unauthorized access even if credentials are compromised. Anomaly detection and MFA create multiple layers of defense against brute-force attacks.

3. Restrict external access to authentication portals and enforce geofencing rules: Limit access to authentication systems using IP whitelisting and geofencing to block login attempts from high-risk regions. Use identity threat detection tools to analyze authentication requests for signs of automated brute-force attempts. Restricting access to authentication portals minimizes exposure to credential stuffing and password brute-forcing.

T1572 (Protocol Tunneling – Conceals malicious network traffic to bypass security controls)

1. Implement deep packet inspection (DPI) to detect and block tunneling activity: Deploy network intrusion detection and prevention systems (IDS/IPS) with DPI capabilities to analyze encrypted traffic for protocol tunneling signatures. Use threat intelligence feeds to update detection rules for known tunneling tools. DPI ensures that unauthorized protocol tunneling attempts are identified and blocked before reaching critical systems.

2. Restrict outbound network connections to only approved protocols and services: Configure firewalls to block unauthorized outbound connections using protocols commonly leveraged for tunneling, such as ICMP, DNS, and HTTP over non-standard ports. Implement strict egress filtering policies to limit external communications to pre-approved domains and IP addresses. Reducing unauthorized outbound traffic minimizes the effectiveness of tunneling techniques.

3. Monitor network traffic for anomalies indicative of tunneling attempts: Use network traffic analysis (NTA) tools to detect irregular data transfer patterns, such as encrypted payloads over unexpected ports. Configure SIEM solutions to generate alerts when suspicious tunneling behaviors are detected. Continuous monitoring helps security teams identify and respond to adversarial attempts to bypass security controls.

T1071.002 (Application Layer Protocol: File Transfer Protocols – Used for staging and transferring stolen financial data)

1. Restrict unauthorized use of file transfer protocols: Block unauthorized FTP, SFTP, and HTTP file transfers using network firewalls and web proxies. Limit outbound file transfers to pre-approved cloud storage and internal repositories. For auditing purposes, authentication is required for all file transfers and log activity. Restricting file transfer protocol usage prevents adversaries from exfiltrating financial data.

2. Monitor and log file transfer activities for suspicious behavior: Deploy security monitoring tools to track large or unexpected file transfers from financial systems. Configure SIEM alerts for high-volume uploads to external servers or anomalous transfer patterns. Regularly auditing file transfer logs helps detect data exfiltration attempts before they result in financial losses.

3. Encrypt sensitive financial data at rest and in transit to prevent unauthorized access: Enforce end-to-end encryption for all file transfers using secure protocols such as SFTP, TLS, and IPsec. Implement data loss prevention (DLP) solutions to automatically detect and block the transfer of sensitive banking data to unauthorized destinations. Encryption and DLP policies ensure financial data remains secure even if it is exfiltrated.

T1219 (Remote Access Software – Enables attackers to maintain persistent control over compromised banking systems)

1. Block unauthorized remote access tools and restrict remote desktop access: Use application allowlisting to prevent execution of unauthorized remote access tools such as TeamViewer, AnyDesk, and VNC. Disable remote desktop access (RDP) on critical financial systems unless explicitly required. Restrict remote access to VPN-only connections with MFA enforcement. Blocking unauthorized remote access tools reduces the attack surface for persistent control.

2. Continuously monitor and log remote access sessions: Deploy endpoint monitoring solutions to track all remote access sessions and detect unusual login behaviors. Use behavioral analytics to identify anomalies, such as remote sessions originating from unusual geolocations or during non-business hours. Logging and monitoring remote access activities help detect persistent adversary presence.

3. Enforce network segmentation and limit remote access privileges: Isolate remote access services from core banking networks using network segmentation. Implement just-in-time (JIT) access provisioning to grant temporary remote access only when necessary. Use privilege access management (PAM) solutions to enforce strict session recording and auditing for all remote connections. Segmentation and privilege restrictions prevent attackers from leveraging remote access tools for lateral movement.

5.3 Mispadu

Mispadu is a highly sophisticated banking trojan that poses a significant threat to the financial sector, particularly in LATAM. Originally discovered in 2019, Mispadu has since expanded its reach beyond its initial targets in Brazil and Mexico to include other LATAM countries and even European nations.[217] [218]

The trojan's effectiveness in targeting financial institutions stems from its multi-stage infection strategy and stealthy nature. Mispadu primarily focuses on Spanish and Portuguese-speaking users, making it particularly dangerous for banks and credit unions in LATAM.[219] [220] Its ability to bypass numerous endpoint protection solutions, including many well-known anti-virus products, has allowed it to infiltrate a wide range of industries, with the financial sector being a primary target.[221]

Mispadu's impact on the financial sector is substantial:

- **Credential theft:** The trojan steals banking credentials, credit card information, and other sensitive financial data using keylogging and screen capture techniques.[222]
- **Cryptocurrency targeting:** Mispadu monitors for cryptocurrency wallet addresses and can replace them with attacker-controlled addresses, potentially redirecting transactions.[223]
- **Widespread infections:** In one campaign, Mispadu affected numerous government websites and online banking platforms across Chile, Mexico, and Peru, compromising hundreds of financial institutions.[224]

A notable example of Mispadu's effectiveness was a campaign that targeted users with fake discount coupons, demonstrating the trojan's ability to adapt its social engineering tactics to lure victims.[225] This adaptability, combined with its focus on LATAM financial institutions, makes Mispadu a persistent and evolving threat to the region's banking sector. To evade detection, the malware uses advanced techniques like obfuscation, sandbox detection, and geofencing. Morphisec's intelligence reports reveal that Mispadu's final payload was delivered through a decrypted AutoIT script, which loads the trojan into memory. Hackers have been using weaponized PDF files for distribution,

[217] https://blog.morphisec.com/mispadu-infiltration-beyond-latam
[218] https://www.feedzai.com/blog/
[219] https://www.feedzai.com/blog/
[220] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/mispadu-banking-trojan-resurfaces
[221] https://blog.morphisec.com/mispadu-infiltration-beyond-latam
[222] https://www.feedzai.com/blog/
[223] https://www.feedzai.com/blog/
[224] https://www.metabaseq.com/threat/mispadu-banking-trojan/
[225] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/mispadu-banking-trojan-resurfaces

and Mispadu is known for stealing browser and email passwords and actively monitoring user activity. Initially targeting Latin America, it now affects Europe, stealing credentials through phishing emails and malicious.[226]

5.3.1 Mispadu's Methods and Exploitation of LATAM Infrastructure

The Mispadu campaign's methods are strategically tailored to exploit the unique vulnerabilities present in LATAM's regulatory, legal, and IT ecosystems. One primary factor is the lack of stringent cybersecurity regulations and inconsistent enforcement across the region, which provides a low-risk environment for cyber criminals. By targeting regions with weak cybersecurity awareness, Mispadu ensures that phishing email campaigns achieve higher success rates, as users are less likely to recognize and report malicious activity.[227] Furthermore, outdated systems and software prevalent in LATAM organizations make it easier for the malware to exploit known vulnerabilities, such as those in CMS platforms like WordPress.

Mispadu capitalizes on insufficient incident response capabilities within the region, ensuring prolonged undetected operations. The adoption of anti-analysis measures and multi-layered infection chains not only improves evasion but also exploits the limited forensic and mitigation capabilities of regional cybersecurity teams. The geographically targeted approach, filtering victims by system language settings, ensures that only intended demographics are affected, thereby increasing the efficiency and profitability of the campaigns. Finally, by leveraging the Windows SmartScreen bypass, Mispadu circumvents built-in protections, exploiting the lack of technical maturity and reliance on default security configurations in many LATAM organizations. These strategies highlight the trojan's effectiveness in exploiting the regulatory and technical gaps of the region to sustain its malicious operations.

5.3.2 Tactics, Techniques, and Procedures

Mispadu employs a sophisticated array of TTPs designed to maximize its effectiveness as a banking trojan. Its infection campaigns often begin with social engineering through phishing emails, distributing malicious HTML pages, or password-protected PDF attachments that entice users into executing the malware.[228] The trojan also leverages malicious advertisements and compromised legitimate websites, including vulnerable WordPress-based platforms, to serve as Command and Control (C2) servers for payload delivery.[229] Additionally, Mispadu adopts multi-stage infection chains, using obfuscated scripts and loaders such as AutoIT and VBScript to deliver its final payload, which is a hallmark of its operational complexity.

To evade detection, Mispadu employs anti-analysis techniques, including virtual machine detection and language checks, to ensure the malware only executes in environments matching the targeted victim profile. It also utilizes fake certificates to disguise the malware and bypass security defenses.[230] The malware includes functionality for credential theft, employing backdoors that allow it to capture keystrokes, take screenshots, and display fake browser overlays to extract sensitive information. Moreover, Mispadu leverages the dual-C2 infrastructure and advanced techniques like the exploitation of the Windows SmartScreen vulnerability (CVE-2023-36025) to bypass security warnings, ensuring its payloads are delivered stealthily and effectively.[231]

[226] https://www.morphisec.com/blog/mispadu-infiltration-beyond-latam/
[227] https://blog.morphisec.com/mispadu-infiltration-beyond-latam
[228] https://blog.morphisec.com/mispadu-infiltration-beyond-latam
[229] https://www.metabaseq.com/threat/mispadu-banking-trojan/
[230] https://www.feedzai.com/blog/
[231] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/mispadu-banking-trojan-resurfaces

5.3.3 Mispadu Tactics, Techniques, and Procedures

Tactics	Techniques	Procedures
Reconnaissance (TA0043)	NA	NA
Resource Development (TA0042)	NA	NA
Initial Access (TA0001)	T1566.001: Phishing	Spam campaigns, the victim is led to the payload by a malicious link or attachment
	T1190: Exploit Public-Facing Application	Exploit a weakness in an Internet-facing host or system to initially access a network.
Execution (TA0002)	T1204.002: User Execution Malicious File: Malware	Executes when the user opens malicious attachments or files downloaded from compromised websites.
Persistence (TA0003)	T1053.005: Scheduled Task/Job	Employs scheduled tasks to maintain persistence on infected systems.
Privilege Escalation (TA0004)	T1055: Process Injection T1055.012: Process Hollowing T1055.013: Process Doppelganging	Injects its payload into legitimate processes to avoid detection.
Defense Evasion (TA0005)	T1036: Masquerading	Masquerades as a discount coupon
	T1027: Obfuscated Files or Information T1027.013: Encrypted/Encoded File	Uses obfuscation and encryption to evade detection by security tools, including anti-analysis and sandbox detection.
Credential Access (TA0006)	T1555: Credentials from Password Stores T1555.003: Credentials from Web Browsers	Obtains credentials from mail clients and web browsers.
	T1003: OS Credential Dumping T1003.008: etc/password and etc/shadow	Uses tools like WebBrowserPassView and MailPassView to steal passwords from browsers and email clients.
	T1056: Input Capture T1056.001: Keylogging T1056.003: Web Portal Capture	Captures keystrokes and screenshots to steal credentials and sensitive data.
Discovery (TA0007)	T1082: System and Information Discovery T1083: File and Directory Discovery	Extracts the version of the operating system, computer name and language ID.
Lateral Movement (TA0008)	NA	NA
Collection (TA0009)	T1113: Screen Capture	Contains a command to take screenshots.
	T1005: Data from Local System	Collects credentials, browser history, and system information from the victim's machine.

Tactics	Techniques	Procedures
Command and Control (C2) (TA0011)	T1573: Encrypted Channel Command and Control (C2)	Communicates with C2 servers using HTTPS or other encrypted channels for data exfiltration and command execution.
	T1102: Web ServiceT1102.002: Bidirectional Communication	Uses an existing, legitimate external Web service as a means for relaying data to/from a compromised system.
	T1105: Ingress Tool Transfer	Transfer tools or other files from an external system into a compromised environment.
Exfiltration (TA0010)	T1041: Exfiltration Over C2 Channel	Sends the data it collects to its C&C server.
	T1567: Exfiltration Over Web Service	Uses an existing, legitimate external Web service to exfiltrate data rather than their primary command and control channel
Impact(TA0040)	NA	

Mispadu IOCs

- Mispadu exfiltrates stolen data, including credentials and system information, via encrypted C2 channels.
- Hashes: 72e83b133a9e4cecd21fdb47334672f6, e5967a8274d40e0573c28b664670857e IP addresses: 104.238.182.44, 140.82.47.181
- Domain: germogenborya.top, russk22.icu, germogenborya.at

Other Mispadu IOCs

- SHA256 C++ dropper non-obfuscated version
- dbb2e294a65eb3fa1bbe1a25c2baf352a01250d567cfa953d4f942c2b5f08e53
- SHA256 C++ dropper obfuscated version
- d56863d940d5ccd1922bbbdf65471c493701e3b10be5c522851c8efbdaeb9fae
- SHA256.NET dropper
- ac97f893f8243db3c5ccfbc89d83b97534c1b73d0289ccb61bfb2c035f539126
- SHA256HTA dropper
- f873062ff206ad60cb4b790c2ba83624c510f15dbc4905d5c96668f87999c16a
- SHA256D2 downloader
- 7b6444e5be24ce95cdcac357cf20ddc77abda142a16202ab3677b7d29a1e0da3
- SHA256 payload version 96
- 78e3e51ddeac0519d434a8b192bae61bbaa278154a9511676c8a58079d95beb5
- SmokeBot download URL that served Mispadu
- http[:]//84.54.50[.]102/FX_432661.exe
- SmokeBot download URL that served a Rhadamanthys payload connected to Mispadu
- http[:]//amx55[.]xyz/rh111.exe

Mispadu CVE: CVE-2023-3602
5.3.3 Mispadu Mitigations

Reconnaissance (TA0043)

- Monitor network traffic for suspicious scanning activities using IDS/IPS.
- Deploy honeypots to detect early reconnaissance attempts.

Resource Development (TA0042)

Monitor domain registrations and look for spoofed domains mimicking your organization.
Use threat intelligence feeds to track adversary infrastructure.

Initial Access (TA0001)

T1566.001: Phishing
- Implement email security solutions (DMARC, DKIM, SPF).
- Conduct employee security awareness training on phishing threats.
- Use sandboxing for email attachments to detect malicious content.

T1190: Exploit Public-Facing Application
- Perform regular vulnerability scanning and patching of internet-facing applications.
- Implement Web Application Firewalls (WAFs) to detect and block exploit attempts.

Execution (TA0002)

T1204.002: User Execution - Malicious File
- Enable application whitelisting to restrict unauthorized execution.
- Use EDR tools to identify suspicious execution.

Persistence (TA0003)

T1053.005: Scheduled Task/Job
- Audit scheduled tasks regularly and restrict user privileges.
- Use PowerShell logging to detect abnormal script execution.

Privilege Escalation (TA0004)

T1055: Process Injection (including T1055.012 and T1055.013)
- Enable Windows Defender Credential Guard to prevent credential theft.
- Use behavior-based detection for injected processes.

Defense Evasion (TA0005)

T1036: Masquerading
- Deploy heuristic-based detection for disguised malware.
- Analyze file metadata for anomalies in timestamps and signatures.

T1027: Obfuscated Files or Information

- Implement automated malware analysis in a sandbox environment.
- Enable real-time file integrity monitoring for unexpected changes.

Credential Access (TA0006)

T1555: Credentials from Password Stores
- Disable password autocomplete in browsers and applications.
- Enforce MFA for critical systems.

T1003: OS Credential Dumping
- Monitor Windows Event Logs for abnormal LSASS access attempts.
- Disable unencrypted credential storage in OS configurations.

T1056: Input Capture (Keylogging, Web Portal Capture)
- Deploy behavior-based keylogger detection.
- Enforce least privilege access to prevent unauthorized software installations.

Discovery (TA0007)

T1082: System and Information Discovery
- Restrict system information access using Group Policy settings.
- Monitor command-line activity for reconnaissance attempts.

Collection (TA0009)

T1113: Screen Capture
- Implement DLP solutions to monitor and restrict unauthorized screenshots.
- Use virtual desktops to limit malware persistence.

T1005: Data from Local System
- Enforce data encryption at rest and in transit.
- Deploy file integrity monitoring to detect unauthorized data access.

Command and Control (TA0011)

T1573: Encrypted Channel
- Monitor network traffic for unusual encrypted connections.
- Implement SSL/TLS decryption and inspection where feasible.

T1102: Web Service
- Block known malicious domains using threat intelligence feeds.
- Deploy anomaly detection to identify irregular data traffic.

T1105: Ingress Tool Transfer
- Restrict file downloads from unknown external sources.
- Use content filtering solutions to block unauthorized transfers.

Exfiltration (TA0010)

T1041: Exfiltration Over C2 Channel
- Implement DLP controls to monitor outbound data flows.
- Detect data exfiltration patterns using network analytics.

T1567: Exfiltration Over Web Service
- Block unauthorized external file transfers via web proxies.
- Implement API monitoring to detect abnormal data movements.

Impact (TA0040)
- Implement ransomware protection with endpoint rollback capabilities.
- Use network segmentation to limit the spread of malware.

5.4 Horabot

Horabot is a sophisticated malware that has been designed to target spanish-speaking users, mainly across Latin American countries. Horabot uses multi-modular techniques to steal sensitive information and spreads itself further, focusing on Latin American systems. Based on the evidence gathered by Cisco Talos, there are patterns revealing the highly targeted attacks in these regions where cybersecurity measures are not as robust.[232]

Horabot was first observed as a significant threat in late 2020, identified by Cisco's Talos team as part of a phishing campaign with tax-related themes to entice victims.[233] Horabot targets individuals and businesses in Mexico, Uruguay, Brazil, Venezuela, Argentina, Guatemala and Panama.[234] These malware campaigns typically disguise themselves as legitimate emails from the tax agencies, presenting users with a malicious HTML attachment that upon clicking redirects the users to a malicious HTML application. The phishing emails use Spanish as their primary language which aligns with the target region and utilizes regional tax deadlines to trick the users into clicking on the malicious attachments and increase the infection rate.[235]

Primary Targets and Sectors:

- The main target entities of Horabot are from the following sectors: accounting, construction, engineering, wholesale distribution, and investments.[236]
- By nature, organizations in these industries would generally be more susceptible to phishing as they often engage in transactional emails.[237]

5.4.1 Capabilities and Malware Functionality

Horabot utilizes banking trojan and spam tools and is deployed at different stages of the infection.

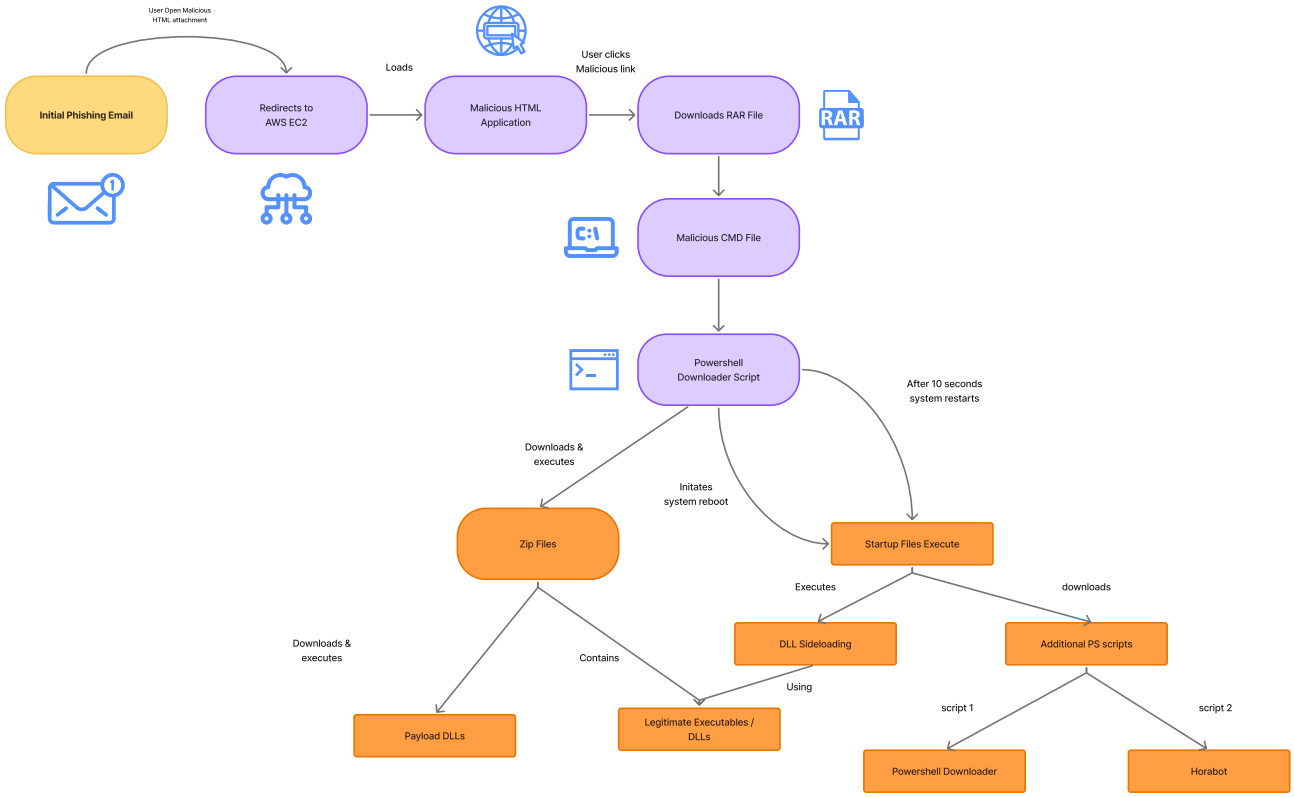
- The banking trojan fetches sensitive information related to banking login credentials, information about operating systems, keystrokes, one-time passwords and soft tokens from banking

232 https://blog.talosintelligence.com/new-horabot-targets-americas/
233 https://blog.talosintelligence.com/new-horabot-targets-americas/
234 https://blog.talosintelligence.com/new-horabot-targets-americas/
235 https://www.welivesecurity.com/2019/08/01/banking-trojans-amavaldo/
236 https://blog.talosintelligence.com/new-horabot-targets-americas/
237 https://www.welivesecurity.com/2019/08/01/banking-trojans-amavaldo/

applications. This functionality directly exploits the security protocols of Latin American financial institutions, placing user accounts at risk and enabling unauthorized access to funds.[238]

- The role played by the spam tool is to compromise Yahoo, Gmail, and Outlook accounts to harvest and exfiltrate the email addresses of the target's contacts. Once these addresses are harvested, the malware sends phishing emails using the victim's legitimate email account and organization's server, increasing the emails' credibility and decreasing the likelihood of detection.[239]

Figure 7: Attack Flowchart



[238] https://blog.talosintelligence.com/new-horabot-targets-americas/
[239] https://blog.talosintelligence.com/new-horabot-targets-americas/

5.4.2 Correlation Between Horabot and Mispadu

Horabot and Mispadu have striking similarities in their TTPs, and both frequently target Latin American organizations. Some similarities that have been observed are:

- Both malware families have been targeting financial institutions and users in Latin America who speak Spanish, through mostly phishing attacks that involve HTML-based malicious payloads that initiate multi-step infection chains.
- They leverage the MITRE ATT&CK techniques T1204.001 (User Execution: Malicious Link) and T1566 (Phishing), enabling them to propagate efficiently through social engineering tactics designed to evade detection on legitimate email servers
- Horabot and Mispadu commonly employ obfuscation techniques and payload encryption, evading static signature-based detections on endpoint solutions.
- Both malwares implement geolocation filters to target Spanish- and Portuguese-speaking regions. Hardcoded Spanish keywords and financial institution names align with their focus on Latin America, especially Mexico and Brazil.

5.4.3 Horabot Tactics, Techniques & Procedures

Tactics	Techniques	Procedures
Resource Development (TA0042)	T1584: Compromise Infrastructure	Compromise third-party infrastructure that can be used during targeting.
	T1584.005: Compromise Infrastructure: Botnet	Compromise numerous third-party systems to form a botnet that can be used during targeting.
Initial Access (TA0001)	T1566: Phishing	Send phishing messages to gain access to victim systems.
	T1566.001: Phishing: Spear Phishing Attachment	Send spear phishing emails with a malicious attachment in an attempt to gain access to victim systems.
	T1190: Exploit Public-Facing Application	Attempt to exploit a weakness in an Internet-facing host or system to initially access a network.
	T1078: Valid Accounts	Obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion.
Execution (TA0002)	T1059: Command and Scripting Interpreter	Abuse command and script interpreters to execute commands, scripts, or binaries.
	T1059.001: Command and Scripting Interpreter: PowerShell	Abuse PowerShell commands and scripts for execution.
	T1204: User Execution	Rely upon specific actions by a user in order to gain execution.
	T1204.001: User Execution: Malicious Link	Rely upon a user clicking a malicious link in order to gain execution.
	T1106: Native API	Interact with the native OS application programming interface (API) to execute behaviors.

Tactics	Techniques	Procedures
Persistence (TA0003)	T1574: Hijack Execution Flow	Execute their own malicious payloads by hijacking the way operating systems run programs.
	T1574.002: Hijack Execution Flow: DLL Side-Loading	Execute their own malicious payloads by side-loading DLLs.
	T1547.001: Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Achieve persistence by adding a program to a startup folder or referencing it with a Registry run key.
	T1547.009: oot or Logon Autostart Execution: Shortcut Modification	Create or modify shortcuts that can execute a program during system boot or user login.
Defense Evasion (TA0005)	T1036: Masquerading	Attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools.
	T1027: Obfuscated Files or Information	Attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit.
	T1497: Virtualization/Sandbox Evasion	Employ various means to detect and avoid virtualization and analysis environments.
	T1070.004: Indicator Removal: File Deletion	Delete files left behind by the actions of their intrusion activity.
Credential Access (TA0006)	T1056.001: Input Capture: Keylogging	Log user keystrokes to intercept credentials as the user types them.
	T1003: OS Credential Dumping	Attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password.
Discovery (TA0007)	T1082: System Information Discovery	Attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture.
	T1083: File and Directory Discovery	Enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system.
Lateral Movement (TA0008)	T1534: Internal Spear Phishing	The malware uses a spam tool to exfiltrate the contact's email address and sends targeted phishing email
Collection (TA0009)	T1113: Screen Capture	Attempt to take screen captures of the desktop to gather information over the course of an operation.
Impact (TA0040)	T1657: Financial Theft	The threat actor group exfiltrated the banking login credentials of the victim to access their bank accounts and cause financial loss

IOCs:

Domain Names

- tributaria[.]website
- facturacionmarzo[.]cloud
- m9b4s2[.]site
- wiqp[.]xyz
- ckws[.]info
- amarte[.]store

IP Addresses

- 139[.]177[.]193[.]74
- 185[.]45[.]195[.]226
- 216[.]238[.]70[.]224
- 51[.]38[.]235[.]152
- 137[.]220[.]53[.]87
- 212[.]46[.]38[.]43
- 191[.]101[.]2[.]101

URLs

- hxxps[://]tributaria[.]website/
- hxxps[://]tributaria[.]website/ESP/12/151222/UP/UP
- hxxps[://]tributaria[.]website/A/08/150822/AU/TST/INDEX[.]PHP?LIST
- hxxps[://]tributaria[.]website/a/09/01092022/au/tst/index[.]php?list
- hxxps[://]tributaria[.]website/a/08/150822/up/up
- hxxps[://]tributaria[.]website/esp/12/151222/up/up
- hxxps[://]tributaria[.]website/a/W_/X\\W_YY/au/au
- hxxps[://]tributaria[.]website/a/08/150822/au/au
- hxxp[://]tributaria[.]website:443/
- hxxps[://]tributaria[.]website/A/08/150822/AU/AU
- hxxps[://]tributaria[.]website/esp/12/151222/au/au
- hxxp[://]139[.]177[.]193[.]74/a/08/150822/au/adjuntos_0703[.]html
- hxxp[://]139[.]177[.]193[.]74/esp/12/151222/au/adjuntos_0703[.]html
- hxxp[://]139[.]177[.]193[.]74/a/08/150822/au/logs/index[.]php?CHLG
- hxxp[://]139[.]177[.]193[.]74/
- hxxp[://]139[.]177[.]193[.]74/a/08/150822/au/tst/index[.]php?list
- hxxp[://]139[.]177[.]193[.]74/a/08/150822/au/adjuntos_2102[.]html
- hxxp[://]139[.]177[.]193[.]74/09/01092022/au/adjuntos_2102[.]html
- hxxp[://]139[.]177[.]193[.]74/a/08/150822/au/adjuntos_0102[.]htm
- hxxp[://]139[.]177[.]193[.]74:443/
- hxxps[://]facturacionmarzo[.]cloud/m/archivos[.]pdf[.]html
- hxxps[://]facturacionmarzo[.]cloud/e/archivos[.]pdf[.]html

Malicious Batch scripts

- 63535100bbc1ba8ce9afb5883a59a4138e95c8e33a4585b8285ea7a39e0ead3e
- 720c126f372b68ff79ef13bd1ae6fc9a6aef10669269490d7e8fb589d7d49064
- ffd43b32655fc6f1e1c10f88660b68e2c2ad7da271b0f2e3eda70ccdcb3bcee4

Powershell Downloader

- aaf456575c8761f3af9b61e015282d9162325ed09b699732bf65b53ae7b7d252

Banking Trojan

39194718b460ea174784f6a7edbccd1e3324fe1043be806927cece7a86f15611
474b25badb40f524a7b2fe089e51eb7dbafd2e3e03a9f6750f72055d05b13d76

Spam Tool

07f7575af922da1aea5aa26436a3cfcd91b419bbf31d77bf6c9d921290bc04da

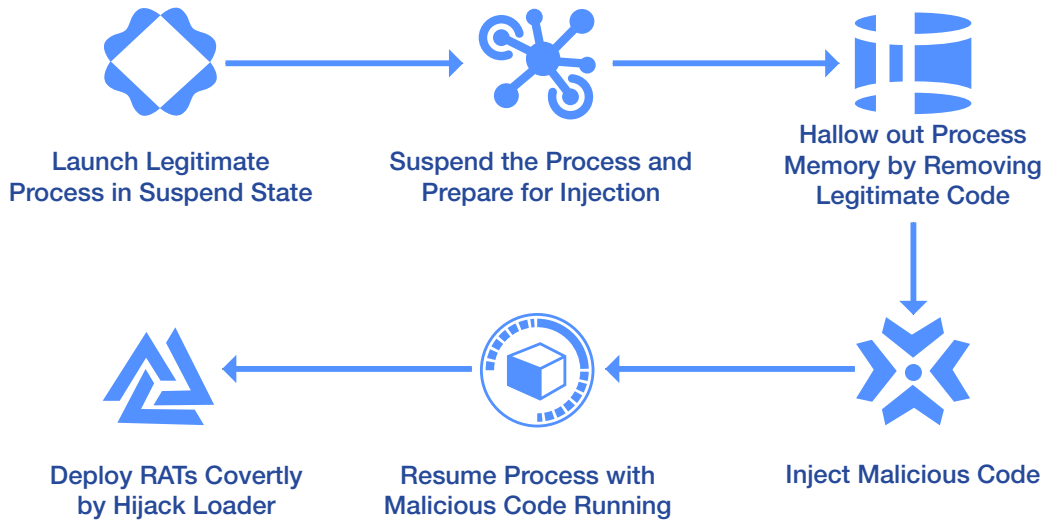
5.5 Blind Eagle

5.5.1 Relevant Threat Actor Activity

Blind Eagle (APT-C-36) is a sophisticated Latin American threat actor known for cyber espionage operations that impact sectors including government, finance, and energy in Colombia, Ecuador, Chile, and Panama.[240] Active since at least 2018, Blind Eagle consistently leverages spear-phishing campaigns, impersonating legitimate regional institutions to deliver remote access trojans (RATs).[241] These attacks exploit human vulnerabilities through deceptive emails with malicious links or attachments.

Blind Eagle's activities showcase their adaptability and extensive knowledge of Latin America's institutional structures. The group's increasing technical sophistication includes techniques like process hollowing, a stealthy code injection method that helps them evade detection and maintain persistent access. In process hollowing, Blind Eagle begins by launching a legitimate process in a suspended state, then "hollows out" its memory by removing the legitimate code. They then inject their own malicious code, often in the form of Remote Access Trojans such as QuasarRAT or AsyncRAT, into this emptied memory space. Once the process resumes, it runs the attacker's code while retaining its original, trusted name. This camouflages the malicious activity, as the process appears legitimate to endpoint detection systems. Additionally, they use custom malware loaders, such as Hijack Loader, to deploy Remote Access Trojans covertly, maintaining remote control over infected devices and continuously adjusting tactics to avoid detection. The straightforward flow chart is shown in Figure 8.

Figure 8: Blind Eagle's Attack Activity



[240] https://securelist.com/blindeagle-apt/113414/
[241] https://research.checkpoint.com/2023/blindeagle-targeting-ecuador-with-sharpened-tools/

The impact on financial institutions has been substantial, as Blind Eagle's espionage and credential theft campaigns have disrupted critical systems and compromised sensitive information. Studies indicate that Latin America has experienced a notable rise in cybercrime costs, with the financial sector bearing the brunt. According to the Organization of American States (OAS) and the Inter-American Development Bank (IDB), Latin American cyber incidents cost the region an estimated $90 billion annually, a significant portion of which impacts financial institutions due to espionage and credential theft campaigns.[242] By capturing browser data, often through keylogging and screen-capturing trojans, Blind Eagle can siphon financial credentials, directly compromising the security of financial institutions in the region. This persistent cybersecurity threat underscores the critical need for FIs to enhance their defenses to keep pace with Blind Eagle's evolving tactics.

5.5.2 Background

Blind Eagle is a cyber-espionage group concentrated in Latin America, particularly targeting Colombia and Ecuador's high-value government and financial sectors.[243] Their primary method of exploitation begins with spear-phishing emails that disguise malware as official communications. These emails carry attachments or links designed to deploy RATs like QuasarRAT and AsyncRAT on victim systems, allowing Blind Eagle full remote access.

QuasarRAT and AsyncRAT are popular tools for groups like Blind Eagle due to their accessibility and adaptability—both are open-source and easily customizable, making them highly versatile for specific espionage needs. Additionally, these RATs offer powerful capabilities such as keylogging, screen capturing, and data exfiltration, allowing attackers to capture sensitive information and monitor user behavior effectively. Their built-in evasion techniques, including encryption and obfuscation, enable them to bypass traditional antivirus software, which is essential for the sustained covert access needed in targeted espionage campaigns. These factors make QuasarRAT and AsyncRAT highly effective tools in Blind Eagle's operations against financial and governmental institutions.

5.5.3 Correlation

Blind Eagle's tactics share some overlap with other Latin American-focused threat actors, such as their use of spear-phishing and remote access trojans (RATs) for credential theft and espionage. The spear-phishing approach is a common technique, used by numerous threat actors to infiltrate organizations through trusted regional personas. However, Blind Eagle's unique characteristics lie in their extensive use of process injection, particularly process hollowing, and their custom malware delivery tools, like Hijack Loader, which are less frequently observed among other threat actors. The combination of RAT deployment with advanced stealth techniques allows Blind Eagle to maintain a persistent presence in critical systems, posing significant challenges to detection and removal. Unlike more generalized attackers, their operations are highly tailored to the LATAM region, with phishing emails that incorporate detailed knowledge of local government and financial systems, adding to their effectiveness and uniqueness.

5.5.4 Recommendations

- Email Filtering: Implement robust filtering to catch spear-phishing indicators like spoofed domain names and unusual attachments, reducing the likelihood of phishing emails reaching employees.

- Endpoint Detection and Response (EDR): Strengthen EDR solutions to detect process injection activities, such as process hollowing, enhancing visibility, and enabling a swift response to threats.

- Local Threat Intelligence: Develop intelligence focused on LATAM threat actors to identify attack patterns and anticipate tactics used by groups like Blind Eagle, allowing for proactive defense strategies.

- Workforce Training: Conduct regular phishing drills and establish a dedicated spam reporting channel for IT/Security, helping employees recognize phishing attempts and alerting IT to potential threats in real-time.

5.5.5 Techniques, Tactic and Procedures

Blind Eagle employs a distinctive set of TTPs that combine spear-phishing, sophisticated process injection, and custom malware loaders to target LATAM's high-value sectors. Their campaigns begin with spear-phishing emails, often tailored to local government or financial entities, tricking recipients into downloading or opening malicious attachments. These attachments commonly deploy RATs like QuasarRAT and AsyncRAT, tools enabling Blind Eagle to remotely monitor, control, and extract sensitive data.

[242] https://publications.iadb.org/publications/english/document/2020-Cybersecurity-Report-Risks-Progress-and-the-Way-Forward-in-Latin-America-and-the-Caribbean.pdf
[243] https://www.zscaler.com/blogs/security-research/blindeagle-targets-colombian-insurance-sector-blotchyquasar

The group's unique TTPs include advanced process injection techniques such as process hollowing, allowing malware to run within legitimate applications' memory spaces. This technique is critical to Blind Eagle's strategy, as it allows their malware to blend into legitimate system processes, reducing the likelihood of detection by conventional security tools and endpoint defenses.

Another notable TTP is their use of the Hijack Loader, a custom-built malware loader that delivers RATs more covertly by masking its functions. This loader adapts to a target's defense system, aiding in both initial evasion and ongoing access. Their sophisticated, regionally focused approach also leverages local knowledge to enhance the believability of their phishing campaigns, strengthening their initial foothold in high-value targets. Blind Eagle selects victims based on potential data value and criticality within LATAM's infrastructure. Their persistence techniques and adaptability in RAT deployment reflect a deliberate, long-term strategy aimed at extracting data while remaining undetected, posing an enduring threat to the cybersecurity landscape of LATAM.

Tactics	Techniques	Procedures
Resource Development	T1583.001	BlindEagle uses DDNS services to create third-level domains. Those domains serve as C2.
Resource Development	T1586.002	BlindEagle controlled a Google Drive folder owned by a Colombian, regional, administration organization.
Resource Development	T1587.001	BlindEagle is operating BlotchyQuasar, which may be considered a customized variant of QuasarRAT.
Resource Development	T1608.001	BlindEagle staged a BlotchyQuasar sample on a compromised and publicly available Google Drive folder.
Initial Access	T1566.002	BlindEagle attempted to gain initial access to the victim's system by using a phishing email including a link to download BlotchyQuasar malware.
User Execution	T1204.002	BlindEagle renamed the BlotchyQuasar sample to be consistent with the phishing email lure and push the victim to manually execute the malware.

Tactics	Techniques	Procedures
User Execution	T1204.001	BlindEagle's attack chain starts with the victim clicking on a link included in the email body and in the attached PDF file.
Initial Access	T1566	Blind Eagle is delivered via a phishing email containing the link to retrieve the password-protected archive.
Persistence	T1547.001	Persistence is achieved via the Registry Run Keys / Startup folder
Execution	T1059.001	The VBS script spawns PowerShell to execute Ande Loader
Defense Evasion, Privilege Escalation	T1055.012	Blind Eagle is using process hollowing to inject the final payload

DNS

- hXXps://pastebin[.]com/raw/XAfmb6xp
- edificiobaldeares.linkpc[.]net
- equipo.linkpc[.]net
- perfect5.publicvm[.]com
- perfect8.publicvm[.]com
- rxms.duckdns[.]org:57832
- njnjnjs[.]duckdns.org
- 91.213.50[.]74

Hashes

- a73057824a65a5ac982e298a80febf61
- bd4505316254f00329431fb8b2888643
- d2fc372302180fbabe18c425aa4a0a72
- c944cb638364c74431bf1dbe7dd329ff
- 64e6ad512eff12e971efdd8979086c5c
- a1f5091ad4e12f922a8e760e0980ab66
- ad578125b337168c976ff5e7e1b190b8
- e21b4c9d9da81deea2381f9b988b0f99
- 07f661aeeb0774f0cb84b0a5e970c2a5
- c4a946903cc9e9a84763ac1731cdd7dd
- 75a40cc019c39e3c2800fb2fe5aba1d3
- 0fa40788b75896a452398b6a49cc62b6
- 59a4f7aed1e3a0718592fb536e987a1d
- 456211df625002df378cf0f4af9d1a6f
- 0f35306ad4fede9a9ba0276a5e788138
- 6044b126afb86682b4a3440e2924c079
- b432e8ff5797fbaf5808d95d46524647
- a31ff54f33ced7b4180f87afb18185a7
- e3239ac16c6fe9c99d6fac0867121a88
- 2784a9fc64d244b14e7d8e4d03f41265
- 3125ae6b1462b0b48dc06bc47d8ddbc7
- b83f6c57aa04dab955fadcef6e1f4139
- a68cac786b47575a0d747282ace9a4c75e73504d
- ec2dd6753e42f0e0b173a98f074aa41d2640390c163ae77999eb6c10ff7e2edd
- 18eb0a413b80a548d2b615e11fc580cd

5.5.6 Blind Eagle Mitigations

Initial Access

- **T1566.001** – Spearphishing Attachment
  - **Mitigation:**
    - » Implement email security gateways with advanced phishing detection.
    - » Train users to identify phishing attempts, including suspicious attachments.
    - » Enable attachment sandboxing to detect malicious payloads before delivery.

Execution

- **T1204.001 – Malicious Link in Email**
- **T1204.002 – Malicious File Execution**
  - **Mitigation:**
    - » Enable application whitelisting to prevent unauthorized execution.
    - » Use safe browsing solutions that flag malicious links before clicking.
    - » Enforce attachment scanning with behavior-based analysis.
- **T1059.001 – Command and Scripting Interpreter: PowerShell**
- **T1059.003 – Command and Scripting Interpreter: Windows Command Shell**
- **T1059.005 – Command and Scripting Interpreter: Visual Basic**
  - **Mitigation:**
    - » Restrict PowerShell and scripting languages via Group Policy.
    - » Enable PowerShell logging (Script Block Logging) to monitor suspicious scripts.
    - » Disable macro execution in Office applications unless necessary.

Persistence

- **T1053.005 – Scheduled Task**
  - **Mitigation:**
    - » Monitor and restrict user permission to create scheduled tasks.
    - » Regularly audit Task Scheduler logs to detect unauthorized jobs.
- **T1547.001 – Registry Run Keys / Startup Folder**
  - **Mitigation:**
    - » Restrict write access to registry keys used for persistence.
    - » Monitor autorun registry entries and startup items for suspicious modifications.
    - » Defense Evasion
- **T1218.009 – Signed Binary Proxy Execution: Regsvr32**
- Mitigation:
    - » Restrict execution of regsvr32.exe if not required.
    - » Use application control (Microsoft Defender ASR rules, AppLocker).
    - » Monitor child processes spawned by regsvr32.exe for anomalies.


****
1010
10101
10101
10
0101
0101010
101010
1010101
1010101

6 Strategic Recommendations for Cybersecurity in Latin America's Financial Sector

6.1 Implement Regional-Specific Security Controls

Financial institutions should adopt security controls tailored to regional banking architectures and threats.

- Establish dedicated threat intelligence teams analyzing region-specific malware and attack patterns (MITRE ATT&CK, NIST SP 800-53).
- Invest in local threat-hunting capabilities and collaboration with regional security researchers (ISO 27001, NIST 800-150).
- Conduct red team exercises reflecting local attack vectors and regulatory requirements (NIST 800-115).

6.2 Establish Financial Sector CSIRT Networks

- Develop sector-specific incident response teams modeled after Colombia's financial CSIRT (ISO 27035, NIST 800-61).
- Foster national and regional collaboration through public-private partnerships.
- Implement structured information-sharing protocols for real-time threat intelligence.

6.3 Strengthen Cross-Border Incident Response

- Standardize incident response frameworks across jurisdictions (NIST 800-61, ISO 27035).
- Establish direct partnerships with regional CERTs and international law enforcement.
- Conduct multi-jurisdictional tabletop exercises to test response readiness.

6.4 Strengthen Human-Centric Security Awareness

- Implement role-specific cybersecurity training and phishing simulations (NIST 800-50, ISO 27002).
- Enforce strong authentication measures, including MFA and secure credential hygiene (NIST 800-63, ISO 27001).
- Foster a security-first culture to mitigate social engineering risks.

6.5 Secure Digital Transformation & Access Control

- Integrate Zero Trust Architecture (NIST SP 800-207) to enforce least privilege access.
- Implement adaptive MFA and biometric authentication (ISO 27001, NIST 800-63B).
- Upgrade outdated systems with secure-by-design principles to meet regulatory standards.

6.6 Enhance Third-Party Risk Management & Monitoring

- Establish continuous vendor risk assessments and compliance checks (ISO 27036, NIST 800-161).
- Enforce contractual security requirements aligned with global cybersecurity standards.
- Strengthen real-time threat monitoring and automated incident detection.

6.7 Harmonize Reporting Requirements

- LATAM should adopt the CRI Profile to streamline regulatory compliance, enhance cyber resilience, and unify risk management under a standardized framework.[244]
- Develop a regional cybersecurity framework with standardized reporting protocols (ISO 29147, NIST 800-61).
- Mandate breach disclosure timelines similar to Brazil's LGPD.
- Establish a unified cybersecurity authority to oversee reporting and response efforts.

6.8 Enhance Information Sharing

- Create a secure platform for cross-border threat intelligence sharing.
- Strengthen public-private partnerships for coordinated response (NIST 800-150, ISO 27010).
- Develop cooperation agreements for rapid response to transnational cyber threats.

6.9 Strengthen Cybersecurity Infrastructure

- Allocate 2-3% of GDP to cybersecurity initiatives (OECD cybersecurity recommendations).
- Enforce strong encryption standards and MFA across critical sectors (NIST 800-175, ISO 27001).
- Develop national cybersecurity strategies prioritizing critical infrastructure protection.

6.10 Improve Cybersecurity Education and Workforce Development

- Launch industry-specific cybersecurity education programs (NIST NICE framework, ISO 27021).
- Conduct regular cybersecurity drills to test resilience (NIST 800-84).
- Establish certification programs to build a skilled workforce.

[244] https://cyberriskinstitute.org/the-profile/

6.11 Strengthen Regulatory Frameworks

- Enforce comprehensive data protection laws where lacking (ISO 27701, GDPR, NIST Privacy Framework).
- Implement stricter penalties for non-compliance with breach reporting.
- Regularly update cybersecurity regulations to align with emerging threats and technologies.

6.12 Foster International Collaboration

- Participate in global cybersecurity forums to exchange best practices (ENISA, ITU Global Cybersecurity Index).
- Strengthen cooperation with international law enforcement to combat cybercrime (Budapest Convention on Cybercrime).
- Seek technical assistance from countries with advanced cybersecurity capabilities.

These measures, aligned with international best practices, will strengthen Latin America's financial sector against emerging cyber threats, fostering resilience and trust in the region's digital economy.

7 Appendix

7.1 Segmented Data

These Threat IDs commonly referred as Techniques are the commonalities between all three threat actors.

CLOP Data for MITER

Recon: tactics

mitre:T1592	T1592	MitreAttackIdentifier
mitre:T1589.002	T1589.002	MitreAttackIdentifier
mitre:T1589.001	T1589.001	MitreAttackIdentifier
mitre:T1589	T1589	MitreAttackIdentifier
mitre:T1590	T1590	MitreAttackIdentifier
mitre:TA0043	TA0043	MitreAttackIdentifier

Resource Development:

mitre:T1586	T1586	MitreAttackIdentifier

Initial Access:

mitre:T1190	T1190	MitreAttackIdentifier
mitre:T1133	T1133	MitreAttackIdentifier
mitre:T1566	T1566	MitreAttackIdentifier
mitre:T1078.003	T1078.003	MitreAttackIdentifier
mitre:T1091	T1091	MitreAttackIdentifier
mitre:TA0001	TA0001	MitreAttackIdentifier

Execution:

mitre:T1059	T1059	MitreAttackIdentifier
mitre:T1059.001	T1059.001	MitreAttackIdentifier
mitre:T1059.003	T1059.003	MitreAttackIdentifier
mitre:T1106	T1106	MitreAttackIdentifier
mitre:T1053.003	T1053.003	MitreAttackIdentifier
mitre:T1053.005	T1053.005	MitreAttackIdentifier
mitre:T1204.002	T1204.002	MitreAttackIdentifier
mitre:T1047	T1047	MitreAttackIdentifier

Persistence:

mitre:T1098	T1098	MitreAttackIdentifier
mitre:T1547.001	T1547.001	MitreAttackIdentifier
mitre:T1037.004	T1037.004	MitreAttackIdentifier
mitre:T1136	T1136	MitreAttackIdentifier
mitre:T1543.002	T1543.002	MitreAttackIdentifier
mitre:T1133	T1133	MitreAttackIdentifier
mitre:T1574.002	T1574.002	MitreAttackIdentifier

mitre:T1053.003	T1053.003	MitreAttackIdentifier
mitre:T1053.005	T1053.005	MitreAttackIdentifier
mitre:T1505	T1505	MitreAttackIdentifier
mitre:T1505.001	T1505.001	MitreAttackIdentifier
mitre:T1505.003	T1505.003	MitreAttackIdentifier
mitre:T1078	T1078	MitreAttackIdentifier
mitre:T1078.003	T1078.003	MitreAttackIdentifier

Privilege Escalation:

mitre:T1548.002	T1548.002	MitreAttackIdentifier
mitre:T1098	T1098	MitreAttackIdentifier
mitre:T1547.001	T1547.001	MitreAttackIdentifier
mitre:T1037.004	T1037.004	MitreAttackIdentifier
mitre:T1543.002	T1543.002	MitreAttackIdentifier
mitre:T1068	T1068	MitreAttackIdentifier
mitre:T1574.002	T1574.002	MitreAttackIdentifier
mitre:T1053.003	T1053.003	MitreAttackIdentifier
mitre:T1053.005	T1053.005	MitreAttackIdentifier
mitre:T1078.003	T1078.003	MitreAttackIdentifier
mitre:T1078	T1078	MitreAttackIdentifier

Defense Evasion:

mitre:T1222.002	T1222.002	MitreAttackIdentifier
mitre:T1497.001	T1497.001	MitreAttackIdentifier
mitre:T1078.003	T1078.003	MitreAttackIdentifier
mitre:T1078	T1078	MitreAttackIdentifier
mitre:T1218.007	T1218.007	MitreAttackIdentifier
mitre:T1218.010	T1218.010	MitreAttackIdentifier
mitre:T1218.011	T1218.011	MitreAttackIdentifier
mitre:T1553.002	T1553.002	MitreAttackIdentifier
mitre:T1112	T1112	MitreAttackIdentifier
mitre:T1070.002	T1070.002	MitreAttackIdentifier
mitre:T1574.002	T1574.002	MitreAttackIdentifier
mitre:T1140	T1140	MitreAttackIdentifier
mitre:T1622	T1622	MitreAttackIdentifier
mitre:T1548.002	T1548.002	MitreAttackIdentifier

Credential Access:

mitre:T1003.001	T1003.001	MitreAttackIdentifier
mitre:T1552.007	T1552.007	MitreAttackIdentifier

Discovery:

mitre:T1622	T1622	MitreAttackIdentifier
mitre:T1083	T1083	MitreAttackIdentifier
mitre:T1135	T1135	MitreAttackIdentifier
mitre:T1057	T1057	MitreAttackIdentifier
mitre:T1012	T1012	MitreAttackIdentifier
mitre:T1082	T1082	MitreAttackIdentifier

Lateral Movement:

mitre:T1021	T1021	MitreAttackIdentifier
mitre:T1021.001	T1021.001	MitreAttackIdentifier
mitre:T1021.002	T1021.002	MitreAttackIdentifier
mitre:T1021.004	T1021.004	MitreAttackIdentifier
mitre:T1021.006	T1021.006	MitreAttackIdentifier
mitre:T1091	T1091	MitreAttackIdentifier

Collection:

mitre:T1005	T1005	MitreAttackIdentifier

C&C:

mitre:T1071.001	T1071.001	MitreAttackIdentifier
mitre:T1573.001	T1573.001	MitreAttackIdentifier
mitre:T1105	T1105	MitreAttackIdentifier
mitre:T1104	T1140	MitreAttackIdentifier
mitre:T1571	T1571	MitreAttackIdentifier

Exfiltration:

mitre:T1041	T1041	MitreAttackIdentifier
mitre:T1052.001	T1052.001	MitreAttackIdentifier
mitre:T1567.002	T1567.002	MitreAttackIdentifier

Impact:

mitre:T1485	T1485	MitreAttackIdentifier
mitre:T1486	T1486	MitreAttackIdentifier
mitre:T1565	T1565	MitreAttackIdentifier
mitre:T1496	T1496	MitreAttackIdentifier
mitre:T1489	T1489	MitreAttackIdentifier

MITER Mobile:

mitre:T1406.002	T1406.002	MitreAttackIdentifier

LockBit Data for MITER

1. Recon:
2. Resource Development:
3. Initial Access:

mitre:T1190	T1190	MitreAttackIdentifier
mitre:T1078	T1078	MitreAttackIdentifier

4. Execution:

mitre:T1059	T1059	MitreAttackIdentifier

5. Persistence:

mitre:T1543	T1543	MitreAttackIdentifier

6. Privilege Escalation:
7. Defense Evasion:

mitre:T1562	T1562	MitreAttackIdentifier

8. Credential Access:

mitre:T1003	T1003	MitreAttackIdentifier

9. Discovery:

mitre:T1087	T1087	MitreAttackIdentifier

10. Lateral Movement:

mitre:T1021.001	T1021.001	MitreAttackIdentifier

11. Collection:

mitre:T1560	T1560	MitreAttackIdentifier

12. C&C:
13. Exfiltration:
14. Impact:

mitre:T1486	T1486	MitreAttackIdentifier

Mispadu Data for MITER

1. Recon:
2. Resource Development:
3. Initial Access:

mitre:T1566	T1566	MitreAttackIdentifier
mitre:T1566.001	T1566.001	MitreAttackIdentifier
mitre:T1190	T1190	MitreAttackIdentifier

4. Execution:

mitre:T1204	T1204	MitreAttackIdentifier
mitre:T1204.002	T1204.002	MitreAttackIdentifier

5. Persistence:
6. Privilege Escalation:

mitre:T1055.012	T1055.012	MitreAttackIdentifier
mitre:T1055.013	T1055.013	MitreAttackIdentifier

7. Defense Evasion:

mitre:T1036	T1036	MitreAttackIdentifier
mitre:T1027	T1027	MitreAttackIdentifier

8. Credential Access:

mitre:T1056.001	T1056.001	MitreAttackIdentifier
mitre:T1056.003	T1555.003	MitreAttackIdentifier

9. Discovery:

mitre:T1082	T1082	MitreAttackIdentifier
mitre:T1083	T1083	MitreAttackIdentifier

10. Lateral Movement:
11. Collection:

mitre:T1005	T1005	MitreAttackIdentifier
mitre:T1113	T1113	MitreAttackIdentifier

12. C&C:

mitre:T1573	T1573	MitreAttackIdentifier
mitre:T1105	T1105	MitreAttackIdentifier
mitre:T1102.002	T1102.002	MitreAttackIdentifier

13. Exfiltration:

mitre:T1041	T1041	MitreAttackIdentifier
mitre:T1567	T1567	MitreAttackIdentifier

Horabot Data for Miter

1. Recon:
2. Resource Development:

mitre:T1584	T1584	MitreAttackIdentifier
mitre:T1584.005	T1584.005	MitreAttackIdentifier

3. Initial Access:

mitre:TA0001	TA0001	MitreAttackIdentifier
mitre:T1566	T1566	MitreAttackIdentifier
mitre:T1566.001	T1566.001	MitreAttackIdentifier
mitre:T1190	T1190	MitreAttackIdentifier
mitre:T1078	T1078	MitreAttackIdentifier

4. Execution:

mitre:TA0002	TA0002	MitreAttackIdentifier
mitre:TA1059	TA1059	MitreAttackIdentifier
mitre:T1059.001	T1059.001	MitreAttackIdentifier
mitre:T1204	T1204	MitreAttackIdentifier
mitre:T1204.001	T1204.001	MitreAttackIdentifier
mitre:T1106	T1106	MitreAttackIdentifier

5. Persistence:

mitre:TA0003	TA0003	MitreAttackIdentifier
mitre:T1574	T1574	MitreAttackIdentifier
mitre:T1574.002	T1574.002	MitreAttackIdentifier
mitre:T1547.009	T1547.009	MitreAttackIdentifier
mitre:T1547.001	T1547.001	MitreAttackIdentifier

6. Privilege Escalation:

mitre:TA0004	TA0004	MitreAttackIdentifier

7. Defense Evasion:

mitre:TA0005	TA0005	MitreAttackIdentifier
mitre:T1036	T1036	MitreAttackIdentifier
mitre:T1027	T1027	MitreAttackIdentifier
mitre:T1497	T1497	MitreAttackIdentifier
mitre:T1070	T1070	MitreAttackIdentifier
mitre:T1070.004	T1070.004	MitreAttackIdentifier

8. redential Access:

mitre:T1056.001	T1056.001	MitreAttackIdentifier
mitre:T1003	T1003	MitreAttackIdentifier
mitre:T1083	T1083	MitreAttackIdentifier

9. Discovery:

mitre:TA0007	TA0007	MitreAttackIdentifier
mitre:T1082	T1082	MitreAttackIdentifier

10. Lateral Movement:
11. Collection:

mitre:TA0009	TA0009	MitreAttackIdentifier
mitre:T1115	T1115	MitreAttackIdentifier
mitre:T1113	T1113	MitreAttackIdentifier

12. C&C:

mitre:TA0011	TA0011	MitreAttackIdentifier

13. Exfiltration:
14. Impact:

mitre:TA0040	TA0040	MitreAttackIdentifier

7.2 Definitions

Tactics, Techniques, and Procedures: The most common behaviors, strategies, and methods used by attackers to develop and execute cyber-attacks on financial institutions.[245]

Phishing: Phishing is a type of pf cyber-attack where the attacker uses various techniques to lure victims to reveal their personal or business-related information. Various types of phishing include:

1. Spear Phishing: Spear phishing is a type of attack in which individuals from organizations are targeted, usually through a malicious link prompting them to reveal login credentials. This leads to unauthorized third-party access to the company's data.

2. Whaling: Whaling is a phishing attack targeting C-level executive members/ employees to reveal sensitive information.[246]

3. Smishing: Smishing is a type of attack where the attacker sends malicious or fraudulent messages/ links through messages, and in most cases, people are lured into revealing usernames, passwords, etc.

4. Vishing: Voice Phishing is commonly known as Vishing. Here, attackers make fraudulent calls representing organizations and lure them into revealing their data using manipulation.

Malware: This is malicious software or a program or just a tiny piece of code which exploits a vulnerability.

Ransomware: A malicious software that encrypts a victim's data and demands a ransom for decryption. Often delivered through phishing emails or exploited vulnerabilities.

Fileless Malware: Malware that operates without installing any files on the infected system, making detection difficult.

Spyware: Software that secretly monitors a user's online activity to collect sensitive information.

Adware: A type of spyware that displays unwanted advertisements to the user.[247]

Trojans: Malicious programs disguised as legitimate software, often downloaded through social engineering tactics.[248]

Worms: Self-replicating malware that spreads rapidly across networks, potentially damaging files or installing additional malware.

Rootkits: Software that provides an attacker with stealthy, persistent control over a compromised system.

Mobile Malware: Malicious software specifically designed to target mobile devices, often delivered through malicious apps or compromised networks.

Exploits: Software or code that takes advantage of vulnerabilities in operating systems or applications to gain unauthorized access.[249]

Scareware: Malware that attempts to frighten users into believing their systems are infected, often promoting fake antivirus software.

Keyloggers: Software that records keystrokes entered on a device, potentially capturing sensitive information.

Botnets: Networks of compromised devices controlled by an attacker to launch various malicious activities.

Malspam: Spam emails containing malicious attachments or links designed to deliver malware.

Wiper Attacks: Malware designed to permanently delete or corrupt data on targeted systems, often used in cyberwarfare or hacktivism.

DOS/DDOS: Denial-of-Service (DoS) attacks are cyber attacks aimed at disrupting a network, server, or website by overwhelming traffic. This can render the target inaccessible to legitimate users. Distributed Denial-of-Service (DDoS) attacks are a more sophisticated variant of DoS attacks. They involve coordinating multiple compromised systems (known as bots) to launch simultaneous attacks on a target, amplifying the Impact and making it more difficult to defend against.

Injection Attacks: Injection attacks are a type of cyber attack where malicious code is inserted into a vulnerable application or system. This can lead to a variety of harmful consequences, including unauthorized access, data theft, and system disruption.[250]

[245] https://www.nextias.com/ca/current-affairs/14-09-2023/cybercrime-investigation-tool)
[246] https://es.cryoserver.com/blog/how-to-avoid-phishing-scams/
[247] https://top10antivirus.site/the-intricacies-of-spyware-a-breakdown-of-their-invasive-techniques/
[248] https://softwarelab.org/best-antivirus-with-firewall/
[249] https://www.mobiletracker.org/law-enforcement-implications-in-hacking-mobile-devices_wpg_881/
[250] https://www.securityjourney.com/post/owasp-top-10-injection-attacks-explained

Common Types of Injection Attacks:

- **SQL Injection:** Exploiting vulnerabilities in SQL queries to execute unauthorized commands.
- **Command Injection:** Executing arbitrary commands on the operating system through vulnerable input parameters.
- **Cross-Site Scripting (XSS):** Injecting malicious scripts into web pages to steal user data or hijack sessions.[251]
- **XML Injection:** Exploiting vulnerabilities in XML processing to inject malicious XML code.
- **LDAP Injection:** Injecting malicious LDAP queries to gain unauthorized access to directory services.

7.3 Common Vulnerabilities, Exposures, and Indicators of Compromise

The most common glossary of classified vulnerabilities in financial institutions has been analyzed and evaluated based on the threat level of the vulnerability. Managing vulnerabilities and threats is crucial for financial institutions due to the sensitive nature of the data they handle.[252] Here are some commonly used glossaries and frameworks for classified vulnerabilities and indicators of compromise (IoCs).

Common Vulnerabilities and Exposures (CVE):

- A standardized list of publicly known cybersecurity vulnerabilities.
- Each CVE entry includes an identification number, a description, and references to related security advisories.
- Financial institutions use CVE to track and assess vulnerabilities in their systems.
- Common Vulnerability Scoring System (CVSS):
- A framework for assessing the severity of vulnerabilities.[253]
- It assigns a score based on exploitability and Impact, helping institutions prioritize their response.
- National Vulnerability Database (NVD):
- A U.S. government repository of vulnerability management data, including CVE entries, CVSS scores, and additional metadata.
- Widely used by financial institutions for vulnerability assessment and management.
- Financial Services Information Sharing and Analysis Center (FS-ISAC):[254]
- Provides threat intelligence and vulnerability information specifically tailored for the financial sector.
- Shares indicators of compromise and threat intelligence to help financial institutions protect themselves.

MITRE ATT&CK Framework:

- Provides a knowledge base of adversary tactics and techniques based on real-world observations.[255]
- Used by financial institutions to understand and defend against sophisticated attack methods.

7.4 Indicators of Compromise (IOCs)

- File Hashes: Unique values representing files that might be used to detect malicious activity.
- IP Addresses: Addresses associated with known malicious activities.
- URLs/Domains: Attackers use web addresses to control malware or exfiltrate data.
- Email Addresses: Addresses involved in phishing or other email-based attacks.

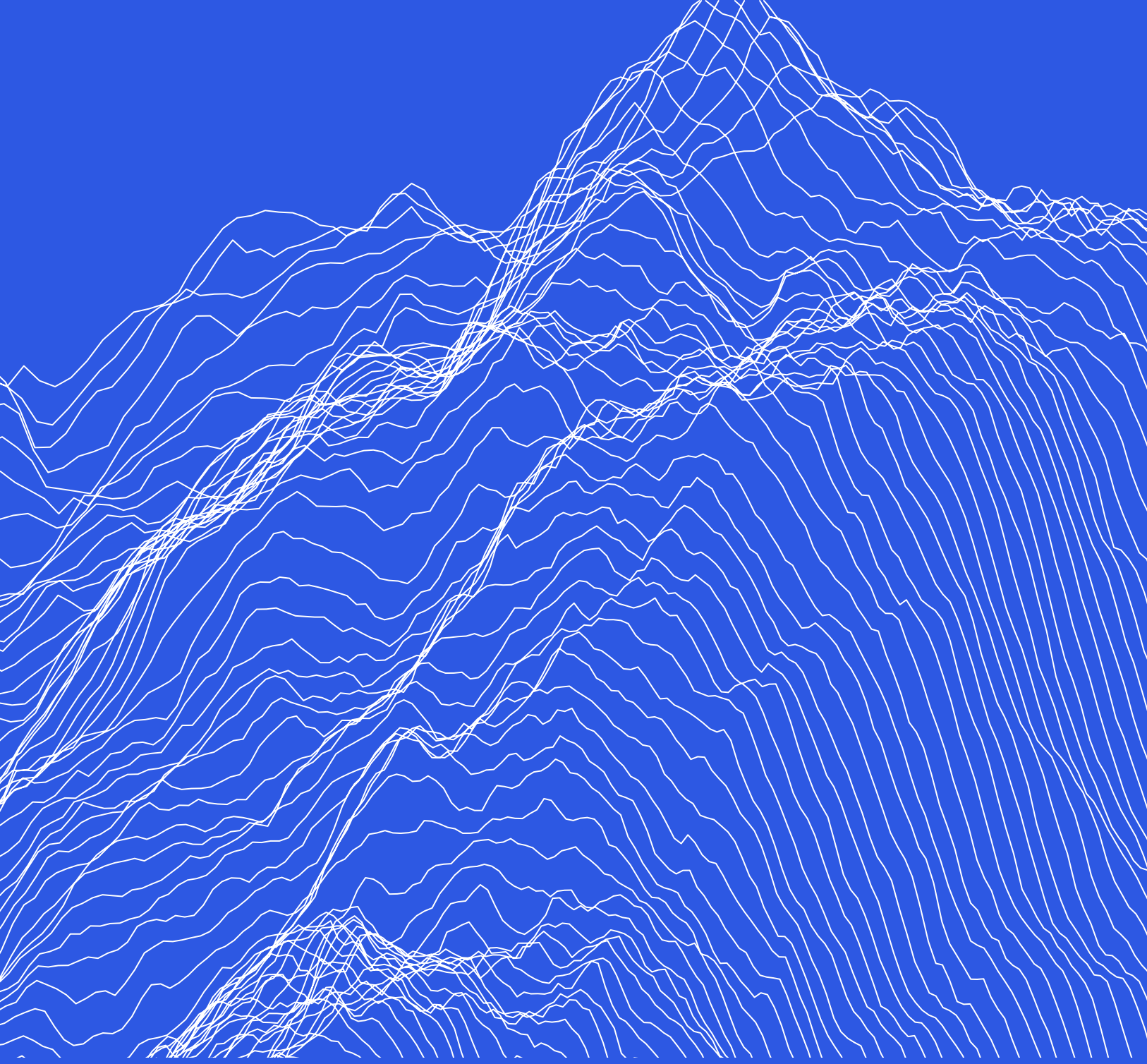
These tools and frameworks help financial institutions effectively manage and mitigate cybersecurity threats, ensuring the protection of their sensitive data.

7.5 Forensic Evidence

The top three forensic evidence of potential intrusions on a host system or network for Financial Institutions.[256]

- Privilege Escalation: This indicates that an attacker has gained higher-level access than initially intended, allowing them to execute more damaging actions.
- Lateral Movement: This shows that an attacker has moved from one compromised system to another within the network, potentially spreading malware or gaining access to sensitive data.
- Exfiltration of Data: This is the most critical sign of a successful intrusion, as it means that sensitive data has been stolen and may be used for malicious purposes.

[251] https://datapacket.net/website-security/
[252] https://neovera.com/cybersecurity-outlook-for-financial-institutions/
[253] https://hadrian.io/blog/tag/security-solutions
[254] https://www.ibm.com/reports/threat-intelligence
[255] https://nsarchive.gwu.edu/media/29421/ocr
[256] https://core.ac.uk/download/346450152.pdf



DIGI
AMERICAS