

LATAM

Threat Landscape Report



Table of Contents

Executive Summary	3
Technical Details	6
Recent Dark Web Activities Targeting Entities in the Latin America Region	9
Ransomware Attack Statistics Targeting Industries in Latin America	12
Stealer Log Statistics Top Domains in the Latin America Region	20
Key Insights and Strategic Recommendations	26

Executive Summary



In recent times, as the landscape of cyber threats continues to widen and become more sophisticated on a global scale, businesses worldwide are facing an increasing risk of significant cyber attacks each day, and the LATAM region is not immune to this trend. The SOCRadar LATAM Threat Landscape Report equips organizations with an in-depth insight into the cyber threats evolving and the potential risks that are unique to their specific geographic area.

By harnessing the latest intelligence on activities of threat actors in the dark web, incidences of ransomware, and phishing operations, this report is a crucial asset for organizations aiming to craft extensive security strategies, allocate their resources more effectively, and pinpoint their cybersecurity necessities. Through its detailed investigation of cyber incidents, SOCRadar's Cyber Threat Intelligence Analysis (CTIA) Team provides thorough research on threats from the dark web, utilizes open-source intelligence, and delivers an exhaustive analysis of threats.

Top Takeaways



1,334 different threat actors targeting enterprises in the Latin America Region shared 3,561 posts on the dark web, and the most common post type was Compromised User Data Sales.

Further analysis highlights that Public Data Exposure constituted a significant portion at 46.56% of the total dark web posts. Moreover, only a small fraction of the data, 1.69%, comprised Target Attack posts, followed by Hack Announcement posts, which made up 1.32%.



The Public Administration industry emerged as the most targeted industry by threat actors, comprising 15.71% of the total.

Following closely behind were the Information Technology industry at 9.18% and the Finance and Insurance industry at 9.01%, indicating the diverse range of industries vulnerable to cyber threats.



In 2023, the Latin America region experienced 1,498 different ransomware attacks.

Among these attacks, 208 of them specifically targeted countries within Latin America. Brazil was the primary target country in 33.82% of these attacks.



Top Ransomware Groups targeting Latin American countries were LockBit 3.0, 8base and ALPHV BlackCat.

In 2023, Latin America was targeted by a total of 33 different Ransomware Groups.



Throughout 2023, Stealer Logs facilitated the compromise of critical information from thousands of Latin American users.

The critical information compromised through Stealer Logs includes data such as user ID/email address, password, credit card data, password hash, and victim IP address information.



The Latin America Region was affected by 6,048 distinct instances of phishing attacks in 2023.

While the primary focus of these phishing attacks was on the Manufacturing industry; Information Technology, Public Administration, Finance and Insurance industries were also commonly targeted.

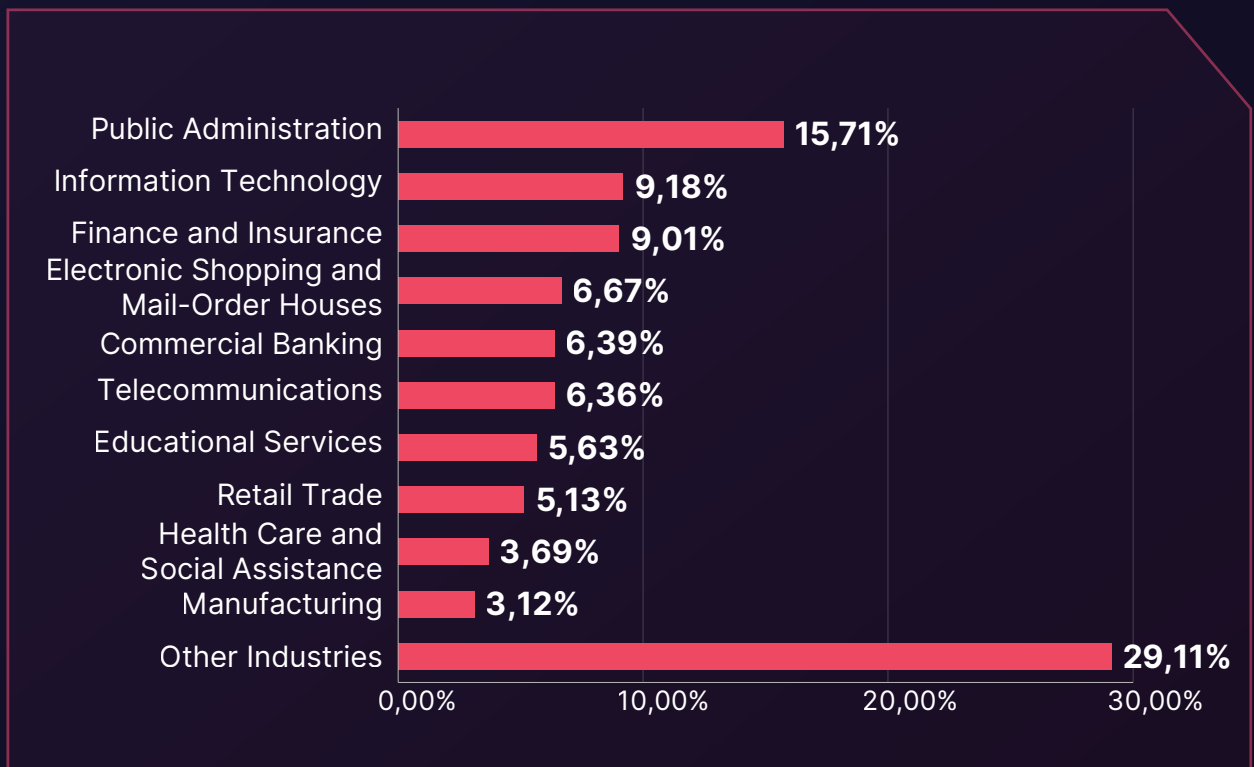
Technical Details

Dark Web Threat Statistics Targeting Industries in Latin America

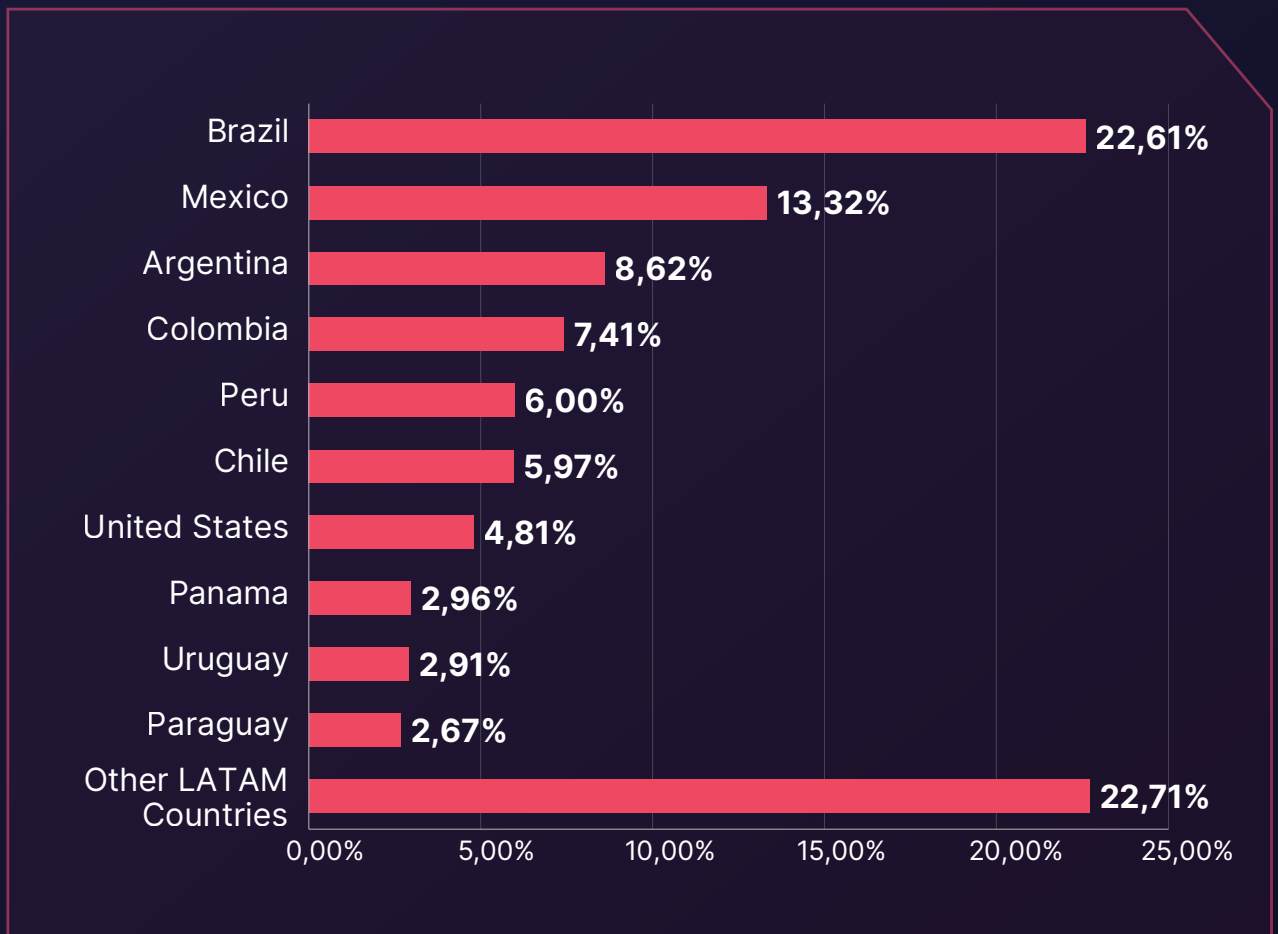
Throughout the past year, SOCRadar's Dark Web Analysts diligently monitored the dark web, identifying trends and crucial connections between enterprises in the Latin America Region and the threat actors lurking in the shadows. Over the course of 2023, enterprises faced a relentless barrage of cyber attacks. An array of threat actors sought to monetize and, at times, share the spoils of their successful cyber intrusions on dark web forums.

During this period, SOCRadar detected 3,561 dark web forum posts attributed to 1,331 distinct threat actors. The industries most frequently targeted included Public Administration, Information Technology and Finance and Insurance. Compromised user data sales dominated the dark web threat landscape.

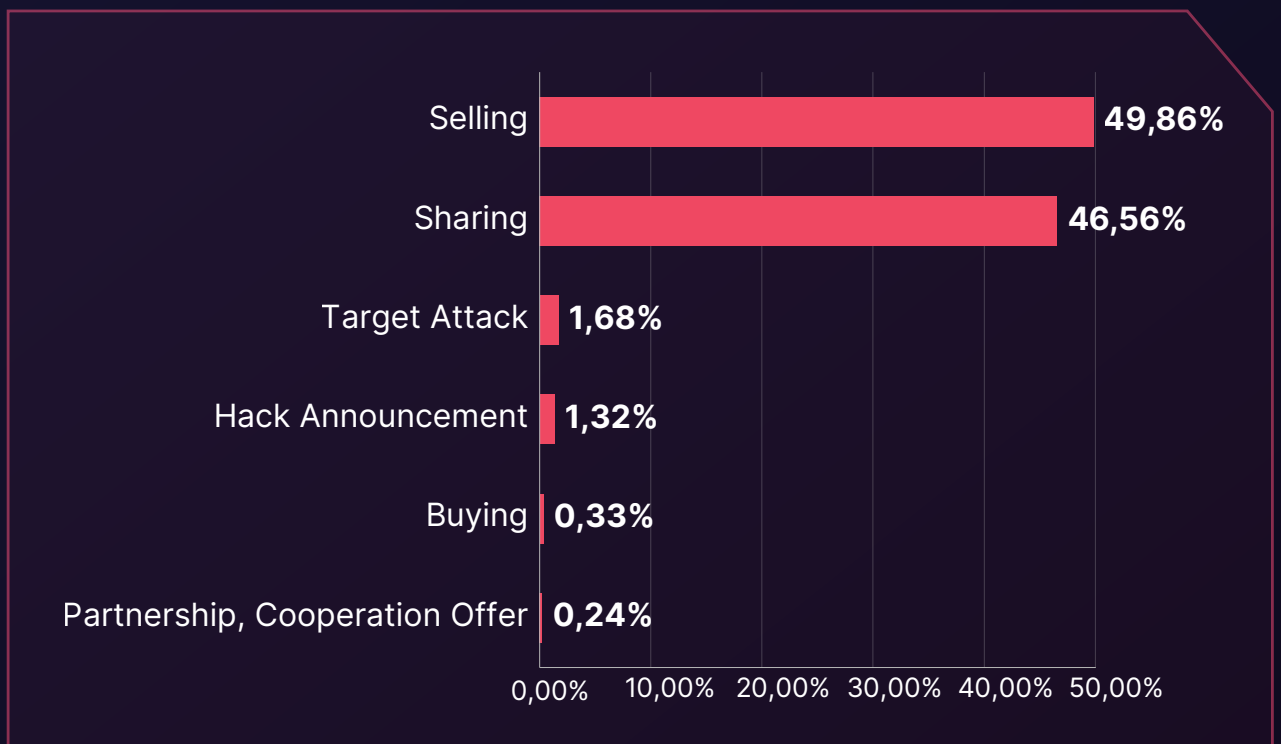
► Industry Distribution of Dark Web Threats



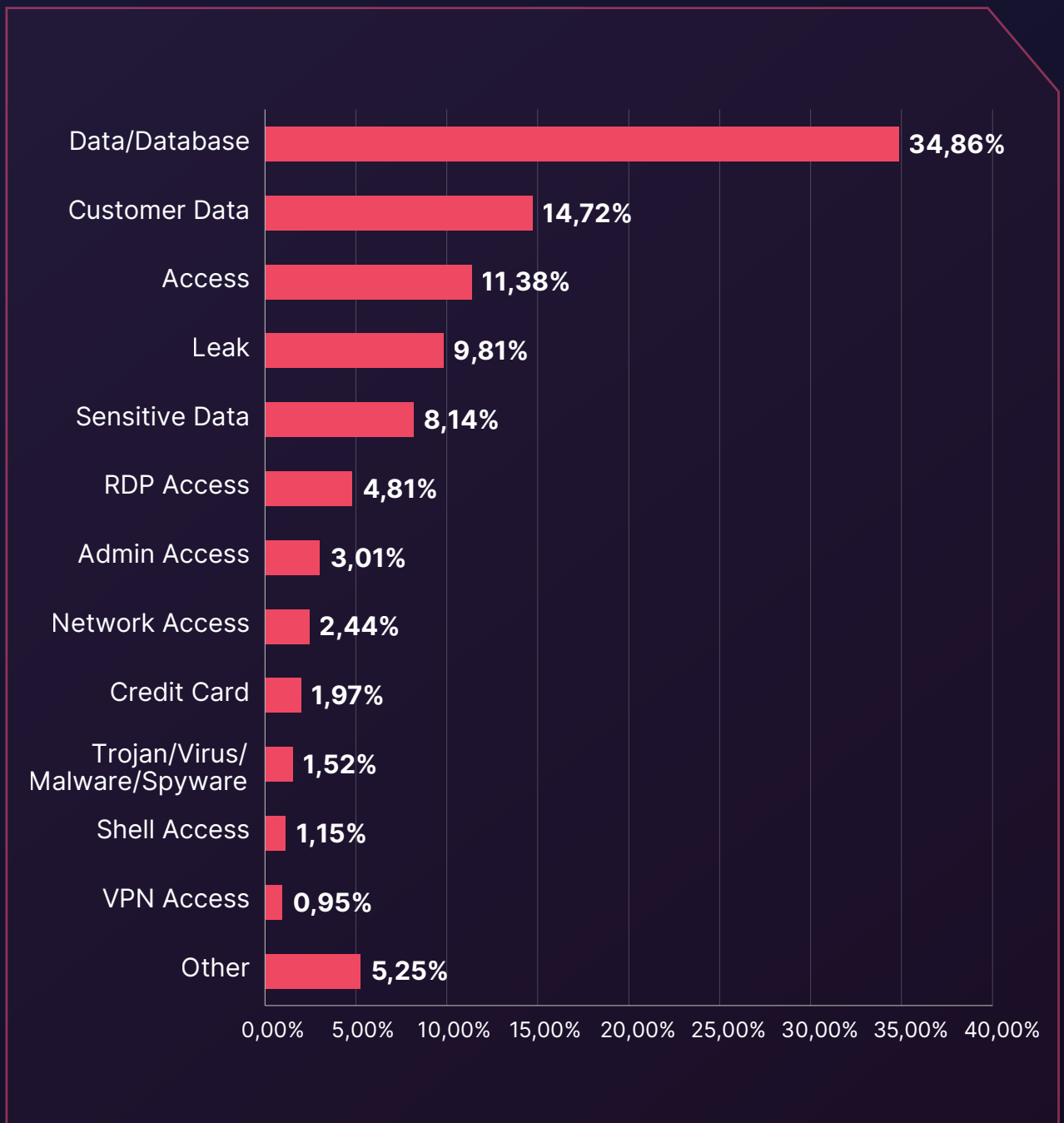
► Distribution of Dark Web Threats by Primary Target Country



► Distribution of Dark Web Threats by Threat Categories



► Distribution of Dark Web Threats by Threat Type

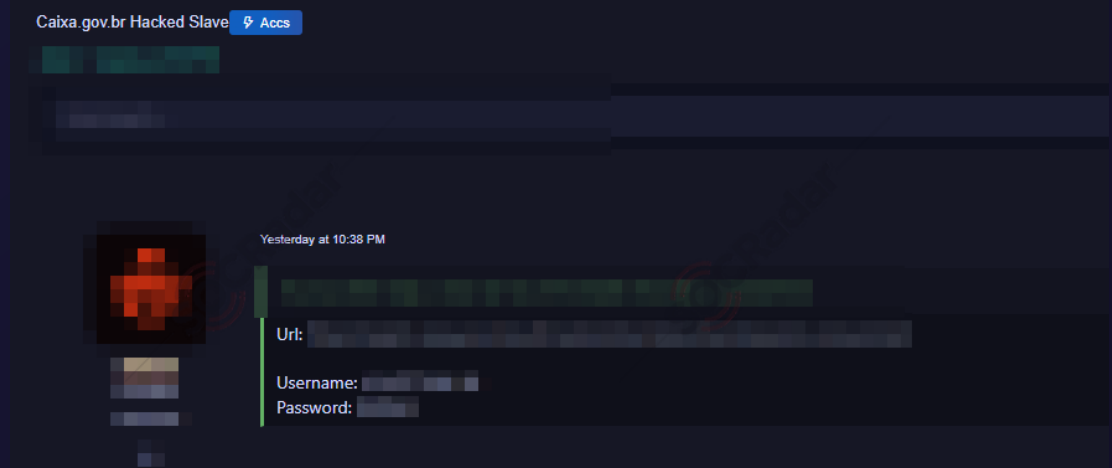


**Illuminate Dark Web Threats
for Proactive Protection**

[Try for Free](#)

Recent Dark Web Activities Targeting Entities in the Latin America Region

Customer Account of Caixa Econômica Federal is Leaked

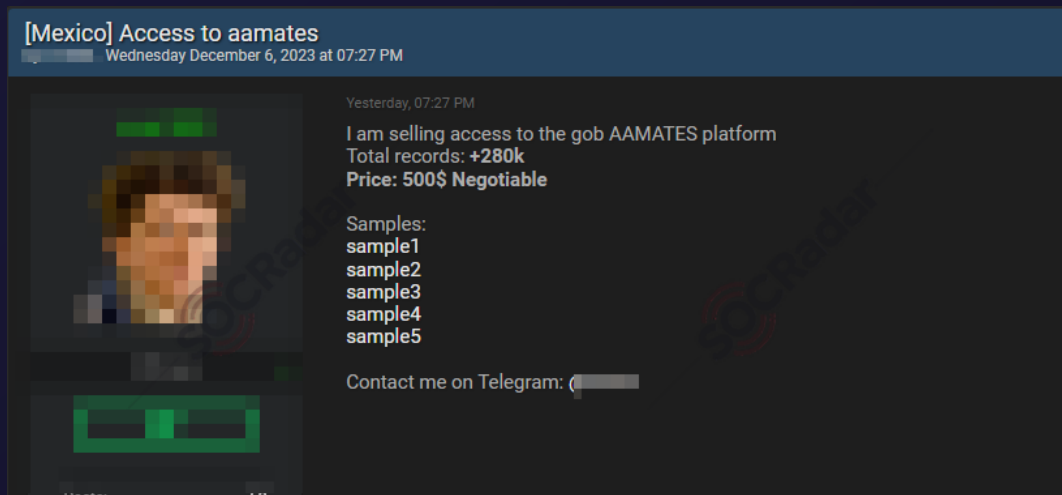


A screenshot from a dark web forum where data is being offered for sale

In a hacker forum monitored by SOCRadar, a new alleged database leak is detected for Caixa Econômica Federal, a Brazilian financial institution. The leaked data includes usernames and passwords, which pose a significant cybersecurity risk across various aspects.

Attackers can use these credentials to gain unauthorized access to customer accounts, potentially leading to financial loss, identity theft, and other malicious activities. Furthermore, the data leak can damage the reputation of Caixa Econômica Federal, eroding customer trust and confidence in the institution's ability to protect their personal and financial information.

Unauthorized Access Sale is Detected for the Health Care Administration and Management Environment

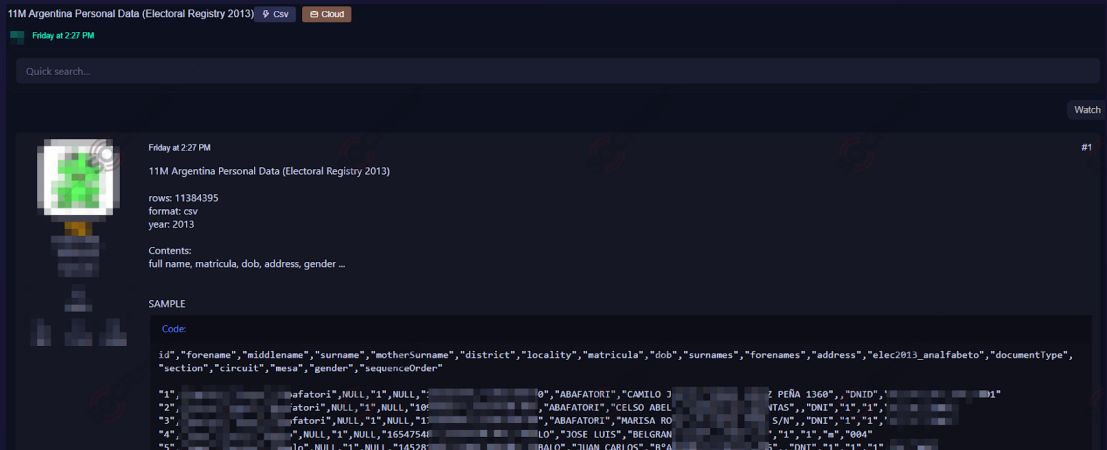


A screenshot from a dark web forum where unauthorized access information is for sale

In a hacker forum monitored by SOCRadar, an unauthorized access sale is detected allegedly belongs to Health Care Administration and Management Environment. The seller claims to have access to over 280,000 records and offers samples to potential buyers. The price for the access is mentioned as \$500 but claimed to be negotiable, via Telegram as their contact method.

The unauthorized access to the AAMATES platform could lead to a data breach, exposing the personal and sensitive information of patients and healthcare professionals. The data could be used for identity theft, fraud, or other criminal activities, resulting in financial losses for individuals and healthcare organizations, as well as reputational damage.

Data of Argentine Citizens are Leaked



A screenshot from a dark web forum where data is being offered for sale

The news article reports a data leak of 11 million Argentine citizens' personal information, including full names, addresses, dates of birth, and genders. The data is allegedly from the 2013 Electoral Registry and was detected on a hacker forum monitored by SOCRadar.

The leak exposes a significant amount of sensitive personal information, putting millions of Argentine citizens at risk of identity theft, fraud, and other cybercrimes. The data breach involves information from the Electoral Registry, raising concerns about the integrity of future elections and the potential for voter manipulation.

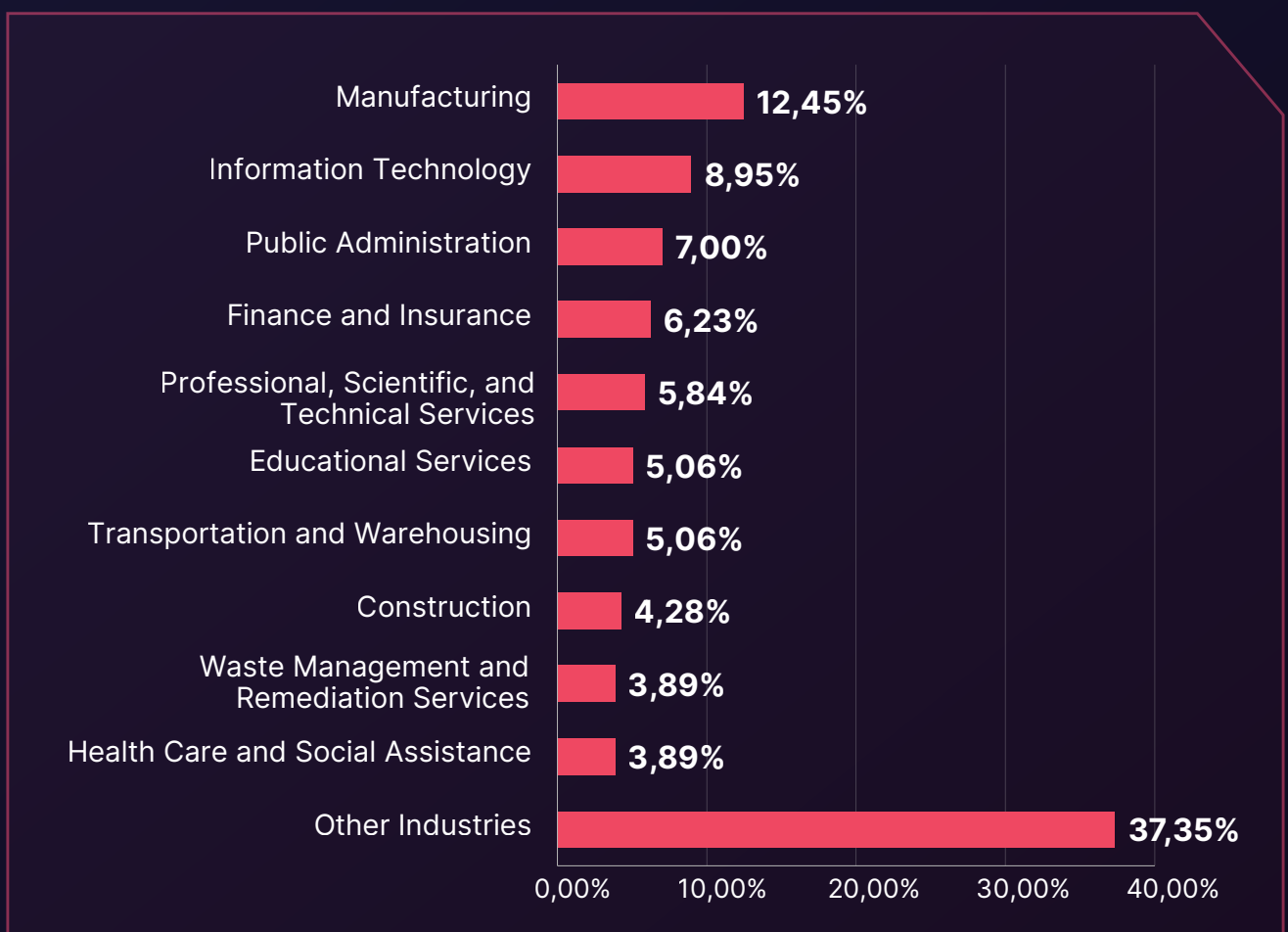
Ransomware Attack Statistics

Targeting Industries in Latin America

Ransomware attacks pose significant threats to organizations, often resulting in severe consequences such as extensive data loss and the exposure of sensitive information. SOCRadar's monitoring has identified 1,498 instances of ransomware victim notifications attributed to various ransomware threat actors and/or groups. Among these attacks, 208 of them specifically targeted countries within Latin America, with Brazil being the primary target country in 33.82% of these attacks.

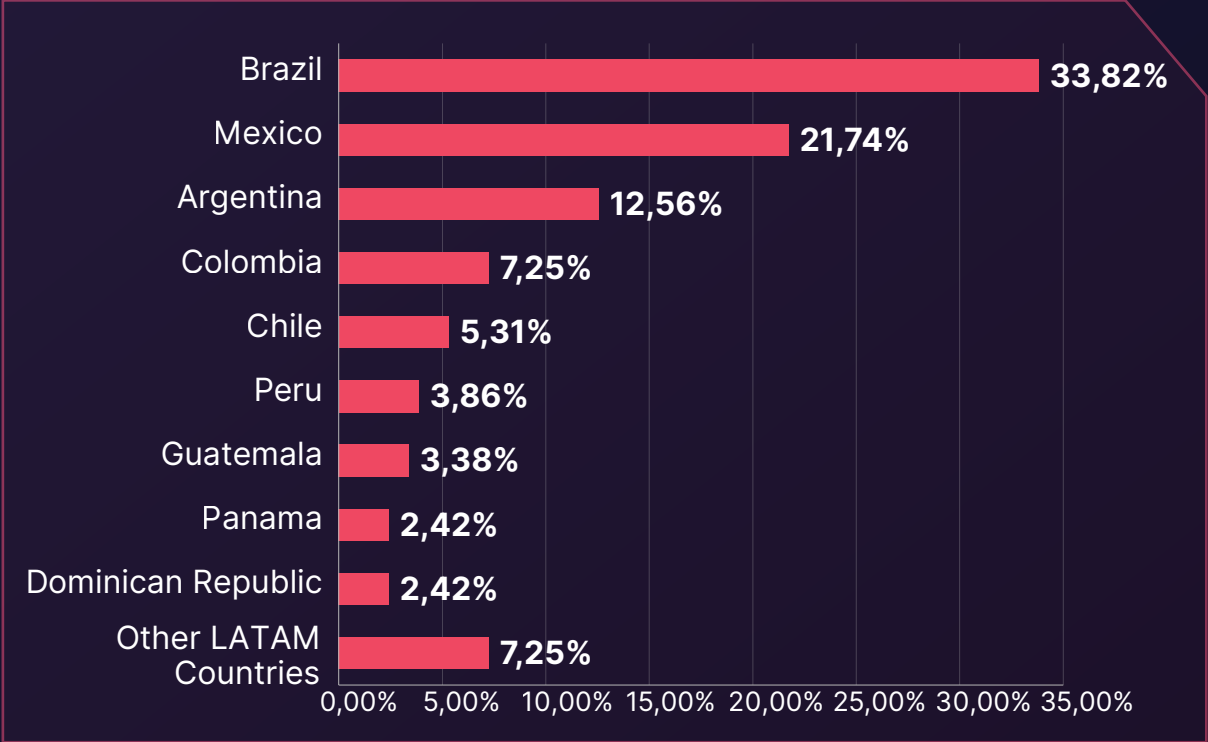
The top three active ransomware groups targeting enterprises in the Latin America Region are LockBit 3.0, 8base and ALPHV BlackCat. These attacks predominantly target Manufacturing and Information Technology industries.

► Distribution of Ransomware Attacks by Industry

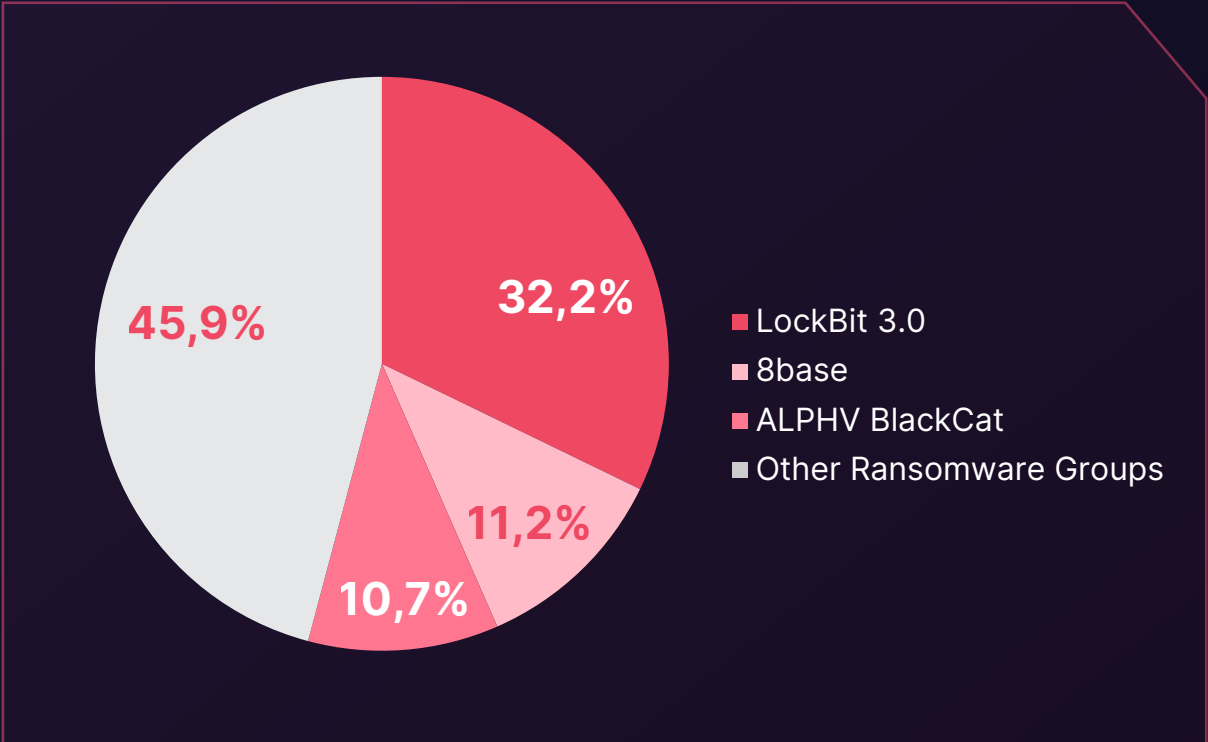


The Latin America Region experienced a total of 1,498 distinct Ransomware Attacks throughout 2023, with 208 of these incidents directly targeting countries in the region as primary targets. These attacks had far-reaching implications, impacting multiple countries simultaneously.

► **Distribution of Ransomware Attacks by Primary Target Country**



► **Top Ransomware Groups Targeting Targeting Latin America**



A Closer Look into The Top 3 Ransomware Groups

Lockbit 3.0 Ransomware Group



-Ransomware Group-	
Motivation:	Financial Gain
Target Countries:	United States, United Kingdom, Canada, Europe, Thailand, Taiwan
Target Sectors:	Manufacturing, Professional Services, IT, Healthcare, Finance, Education, Legal Services
Attack Type:	Phishing, RDP and VPN access Exploitation, Ransomware, Data Exfiltration, Double-extortion
-TTPs-	
Exploit Public-Facing Application:	T1190
Remote Desktop Protocol:	T1021.001
Data Encrypted for Impact:	T1486

LockBit 3.0, a successor to LockBit and LockBit 2.0, operates as a Ransomware-as-a-Service (RaaS) group. Since January 2020, LockBit has shifted to an affiliate-based model, employing various tactics to target businesses and critical infrastructure organizations. They are known for employing strategies like double extortion and initial access broker affiliates, as well as recruiting insiders and hosting hacker recruitment contests. With over 1,500 victim announcements on the SOCRadar platform, LockBit emerged as the most active ransomware group in 2022 following Conti's shutdown. As of the first quarter of 2023, they remain the most prolific group, boasting over 300 announced victims.

For more detailed information about the Lockbit 3.0 Ransomware Group, you can visit our [blog post](#).

8base Ransomware Group



-Ransomware Group-	
Motivation:	Financial Gain
Target Countries:	United States, Brazil, UK, Australia, Germany, Canada, Spain, Italy, Belgium
Target Sectors:	Professional Services, Manufacturing, Construction, Finance, Healthcare, Transportation
Attack Type:	RaaS, Ransomware, Double Extortion
-TTPs-	
Phishing:	Spearphishing Attachment: T1566.001
OS Credential Dumping:	T1003
Exfiltration Over C2 Channel:	T1041

8Base is a ransomware group that has been active since April 2022. Despite its relatively recent emergence, the group has rapidly gained notoriety due to its aggressive tactics and the significant number of victims it has claimed. The group primarily targets small and medium-sized businesses (SMBs) across various sectors, including business services, finance, manufacturing, and information technology.

The group's identity, methods, and motivations largely remain a mystery. However, based on its leak site and public accounts, along with the group's communications, researchers think the group's verbal style is quite similar to that of RansomHouse, a group that typically purchases already compromised data or works with data leak sites to extort victims. This has led to speculation that 8Base may be an offshoot of RansomHouse.

For more detailed information about the 8base Ransomware Group, you can visit our [blog post](#).

ALPHV BlackCat Ransomware Group



-Ransomware Group-	
Motivation:	Financial Gain
Target Countries:	United States, United Kingdom, Canada, Germany, Australia, France, Italy, Spain
Target Sectors:	Professional Services, Manufacturing, Healthcare, Finance, Information Technology
Attack Type:	Spearphishing, Stolen Credentials, RaaS, Ransomware, Triple-Extortion
-TTPs-	
User Execution: Malicious File:	T1204.002
Defacement:	T1491
Data Encrypted for Impact:	T1486

BlackCat, or ALPHV, is a ransomware group known for being the first to use Rust -a cross-platform language programming language that allows for easy malware customization for different operating systems, such as Windows and Linux- successfully. The group has been able to evade detection and successfully encrypt their victims' files by using Rust, which allows them to target multiple operating systems and bypass security controls that are not designed to analyze malware written in Rust.

For more detailed information about the ALPHV BlackCat Ransomware Group, you can visit our [blog post](#).


Think Like a Hacker, Defend Like a Pro

Request Free Access

Recent Ransomware Attacks Targeting Entities in Latin America

ALPHV BlackCat Ransomware Group Leaked The Data of LCA Consultores



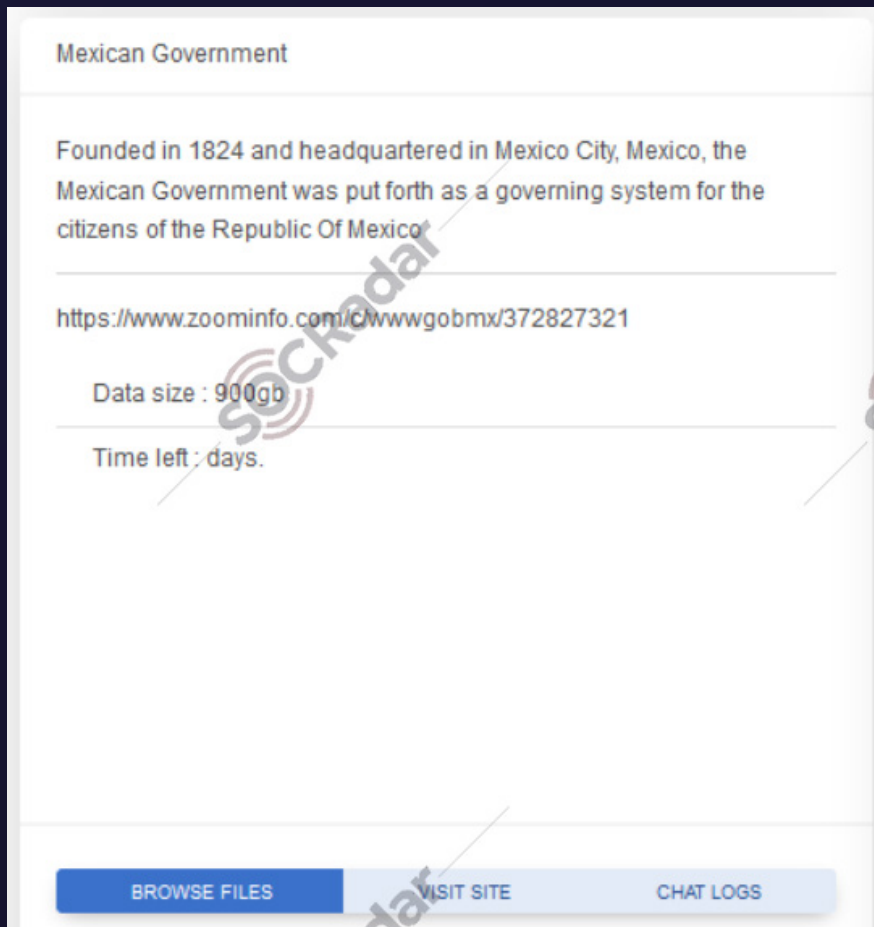
<p>LCA Consultores 11/24/2023, 12:23:17 PM</p> <p>LCA Consultores known as LCA Macroeconomia suffered cyber attack & data breach twice on 20 & 23 November no news or response from LCA Consultores</p> <p>More than 650GB of the sensitive data were exfiltrated & more than 270 clients are affected</p> <p>Sample of the data is</p> <ul style="list-style-type: none">- Internal & client databases- Confidential analytical & studies- Passports & Company sensitive documents- Wire transfers, transactions, payments, invoices, and cash receipts- NDA agreements and confidential contracts- Employees & Clients' personal & confidential data <p>Sample of the affected companies.</p>	
---	---

Threat actor claims on LCA Consultores data breach

The leaked data includes sensitive information such as internal and client databases, confidential analyses and studies, passports and company-sensitive documents, wire transfers, transactions and payments, invoices and cash receipts, NDA agreements and confidential contracts, as well as personal and confidential data of employees and clients.

The data leak of LCA Consultores poses a significant risk to the company's reputation, and customer trust. The ransom demand and potential costs associated with the data recovery and mitigation efforts can lead to substantial financial losses.

The New Ransomware Victim of LostTrust: Mexican Government



Screenshot from the LostTrust ransomware group website

In the LostTrust ransomware group website monitored by SOCRadar, a new ransomware victim was allegedly announced as Mexican Government. The ransomware group claims to have stolen 900GB of data from the Mexican Government, posing a risk of sensitive information exposure and potential disruption of government operations.

Compromised data of a government organization poses a significant risk for national security as the information in the database could be used for identity theft, targeted phishing attacks, spam or other malicious activities.

DragonForce Breach Group Leaked The Data of Dafiti Argentina



Screenshot from the DragonForce ransomware group website

In the DragonForce data breach group website monitored by SOCRadar, new data leaks detected allegedly belong to Dafiti Argentina. The leaked data includes personal information of customers, such as names, addresses, email addresses, and phone numbers, as well as financial information including credit card information.

The data leak is a major security breach that could lead to identity theft, financial fraud, and other cybercrimes. The breach of financial information on the other hand, could allow threat actors to make unauthorized purchases or access victims' bank accounts.

Stealer Log Statistics Top Domains in the Latin America Region

Throughout 2023, thousands of users' user ID/email address, password, credit card data, password hash, and victim IP address information were compromised via Stealer Logs from some of the highest traffic domains in Latin America.

The table below lists the domains associated with Latin America that have the highest traffic.

mercadolibre.com

meru.com.mx

zaxapp.com.br

ec21.com

seebiz.com

ecvv.com

terra.com.br

terra.com.mx

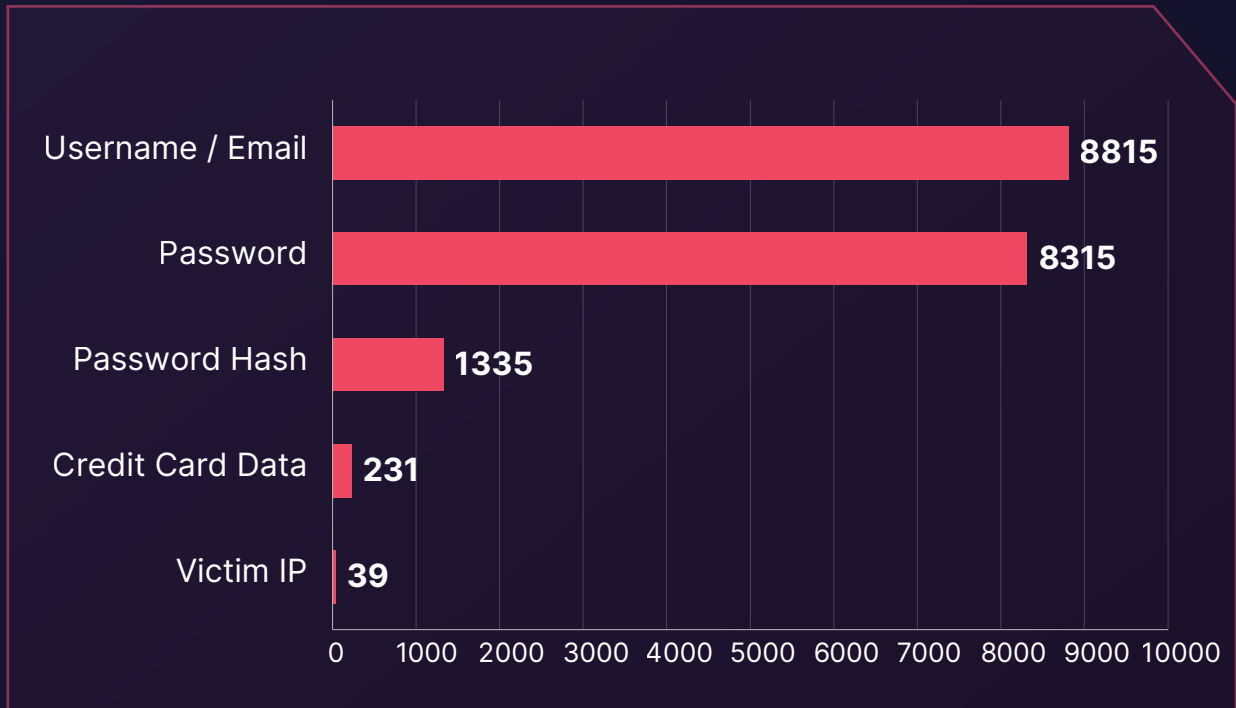
terra.cl

univision.com



The graph below showcases the distribution of the compromised user data obtained through Stealer Logs across the highest-traffic domains associated with the Latin America Region.

▶ Stealer Logs - Distribution of the Compromised Data



The data unveils a notable dissemination of compromised information, encompassing 8,815 usernames/emails, 8,315 passwords, 1,335 password hashes, 231 credit card data, and 39 compromised victim IPs, each signifying distinct instances of breach.

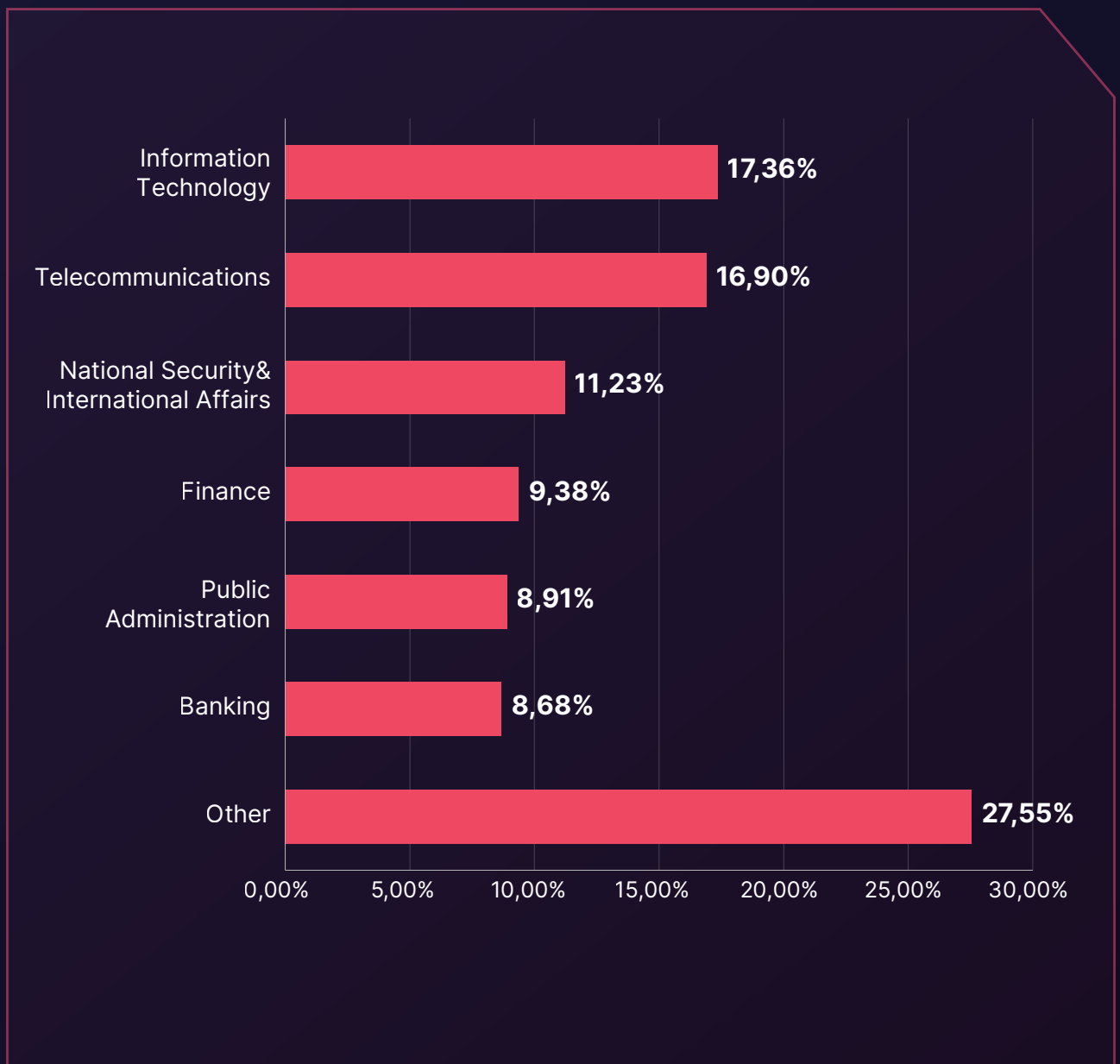
These discoveries emphasize the gravity of data compromise occurrences impacting users in the digital sphere of the Latin America Region, emphasizing the urgent necessity for strong cybersecurity protocols to efficiently alleviate such risks.

Phishing Threats Targeting Latin America

Phishing serves as an effective method to initially breach an organization's infrastructure by deceiving individuals into divulging sensitive credentials on fraudulent websites.

Typically, phishing attacks are coupled with social engineering tactics to acquire such credentials. Over the past year, enterprises in the Latin America Region has encountered 6,048 distinct instances of phishing attacks, primarily targeting the Information Technology industry.

► Phishing Attacks - Distribution by Industry



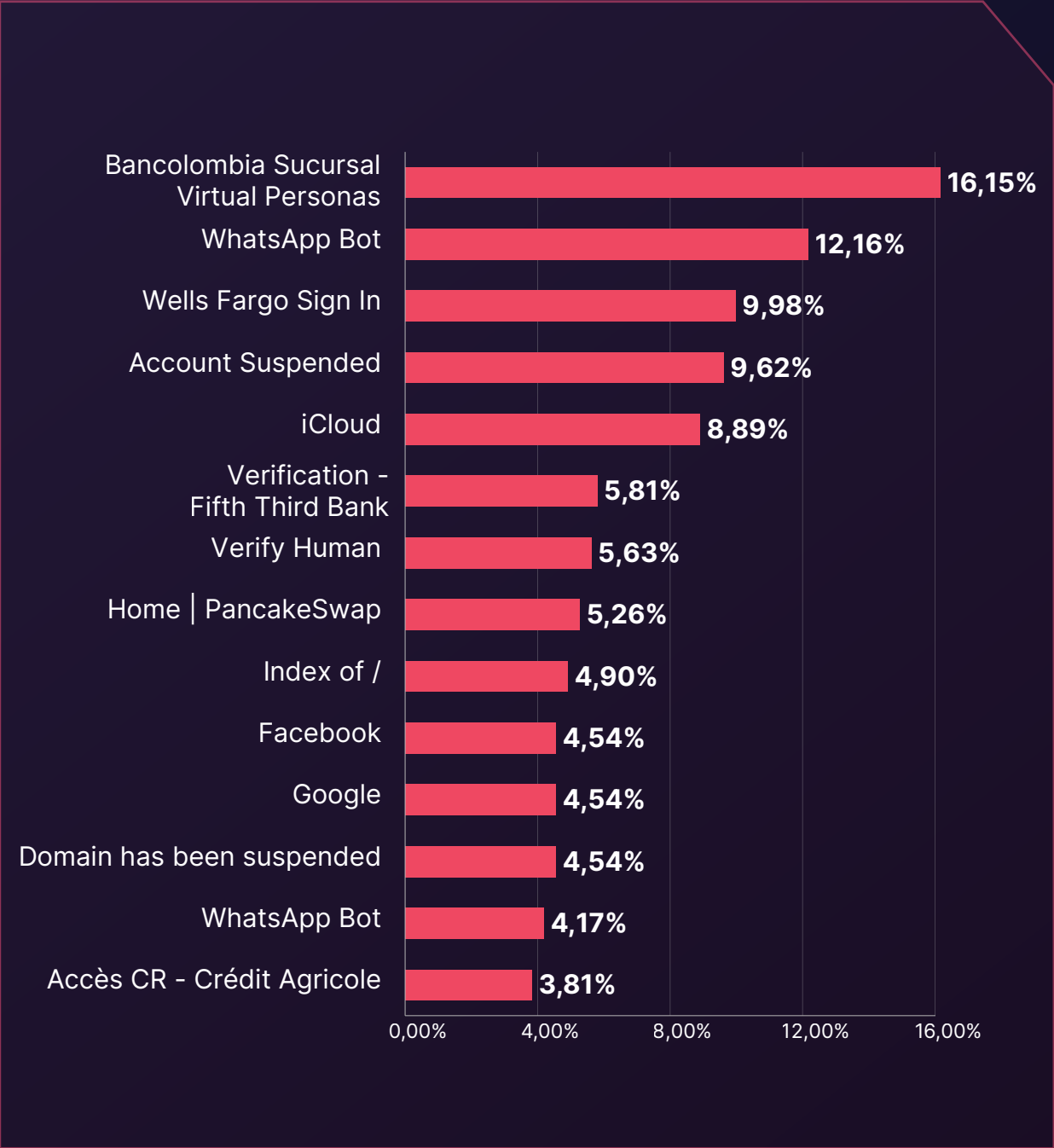
Analyzing the distribution of these attacks across countries reveals that Brazil and Argentina are the most heavily targeted, accounting for 27.60% and 21.82% of all phishing attacks, respectively. Additionally, countries such as Panama, Belize, Chile, and other Latin American countries have also been impacted by phishing attacks.

► Phishing Attacks - Distribution by Target Country



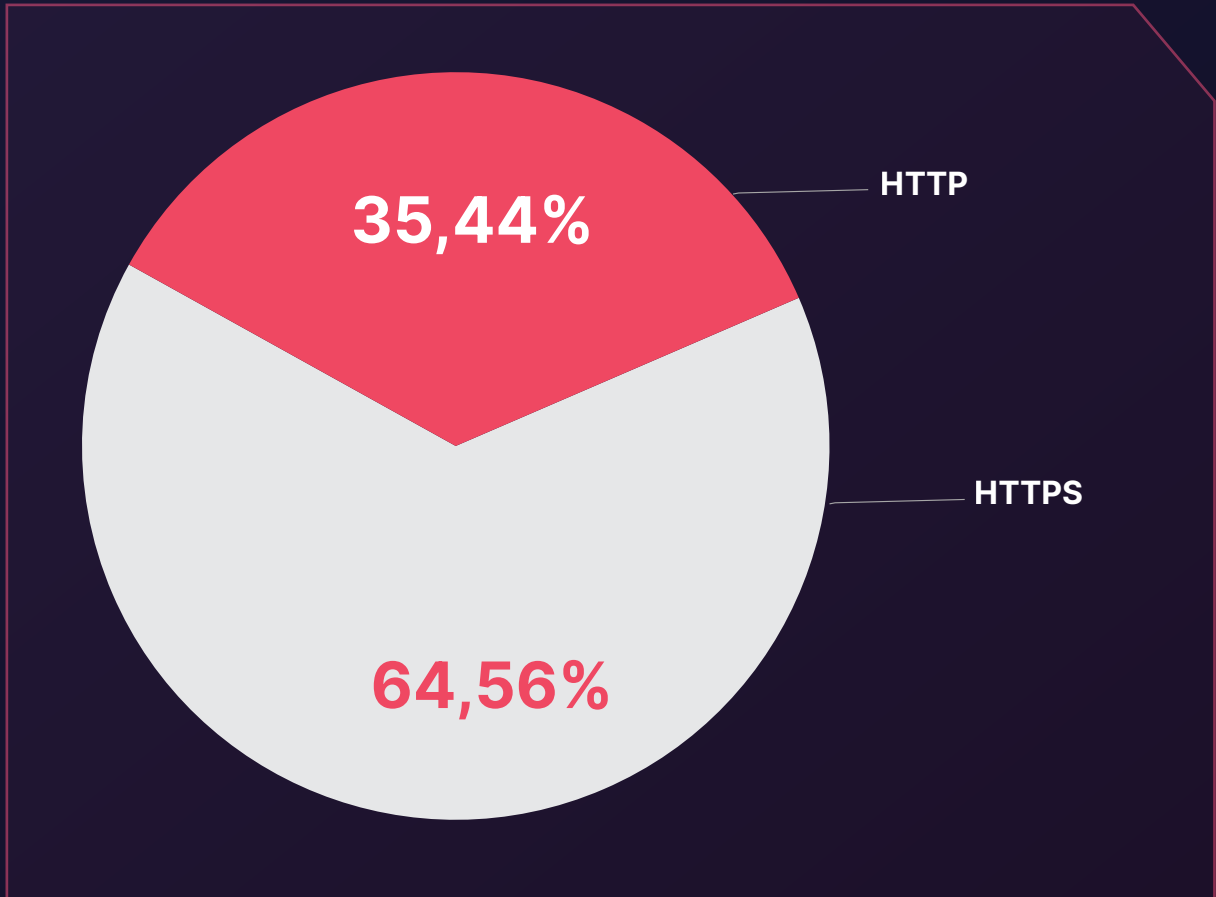
The graph below illustrates the distribution of Page Titles used by threat actors for phishing attacks. Notably, the data reveals a predominant usage of the Bancolombia Sucursal Virtual Personas page title. This insight underscores the significant focus of threat actors on mimicking legitimate login pages to deceive users into divulging sensitive information.

► **Phishing Attacks - Distribution by Phishing Page Title**



When closely examining the SSL/TLS protocols of domains prepared for phishing attacks by threat actors, we observe an increasing trend in the usage of HTTPS compared to the past.

► Phishing Attacks- Distribution by SSL/TLS Protocol



Lessons Learned: Key Insights and Strategic Recommendations

Upon reflection of the cyber threat landscape impacting organizations in the Latin America Region, several pivotal lessons and recommendations emerge. These insights, coupled with the capabilities of SOCRadar, offer a roadmap for enhancing cyber resilience and preserving operational integrity. The following are the top 5 takeaways from our analysis:

Maintain vigilance regarding the evolving cyber threat landscape:

It's evident that the cyber threat landscape is dynamically evolving, as evidenced by the surge in dark web activity related to the Latin American Region and the proliferation of ransomware incidents. Organizations must stay abreast of these developments and adapt their security strategies accordingly. Leveraging SOCRadar's Cyber Threat Intelligence provides businesses with real-time insights into emerging threats, enabling them to stay ahead of cyber adversaries.

Emphasize multi-layered security measures:

The diverse range of industries targeted by cyber threats underscores the necessity for multi-layered security measures. As demonstrated, threat actors do not discriminate based on industry, necessitating a comprehensive security approach across all industries, from Information Technology to Public Administration. SOCRadar can support this effort through proactive threat intelligence and monitoring services.

Maintain vigilance against ransomware:

Ransomware remains a significant threat, highlighting the importance of robust defenses and response plans. SOCRadar's threat intelligence capabilities enable businesses to identify potential ransomware threats and develop effective response strategies.

Educate and train employees:

Given the persistent threat of phishing attacks, continuous education and training for employees are essential. Familiarity with phishing tactics and detection methods is critical. SOCRadar's solutions can assist in this regard by identifying potential phishing domains and raising awareness of the latest phishing techniques.

Ensure defense against Stealers:

With the Latin America Region being a primary target country for Stealer Log malware infections, organizations must enhance their defenses against these malicious software. SOCRadar's advanced threat intelligence aids in detecting and mitigating Stealer threats, bolstering the overall security posture of the organization.

In conclusion, adopting a proactive, informed, and comprehensive approach to cybersecurity is paramount. By partnering with solutions such as SOCRadar, organizations in Latin America can fortify their defenses and effectively navigate the evolving cyber threat landscape.

Who is SOCRadar®?

Your Eyes Beyond

SOCRadar provides Extended Threat Intelligence (XTI) that combines: **"Cyber Threat Intelligence, Brand Protection, External Attack Surface Management, and Dark Web Radar Services."** SOCRadar provides the actionable and timely intelligence context you need to manage the risks in the transformation era.

21.000+
Free Users

Dark Web Monitoring: SOCRadar's fusion of its unique Dark Web recon technology with the human analyst eye further provides in-depth insights into financially-targeted APT groups and the threat landscape.

Protecting Customers' PII: Scan millions of data points on the surface, deep and Dark Web to accurately identify the leakage of your customers' Personally Identifiable Information (PII) in compliance with regulations.

Credit Card Monitoring: Enhance your fraud detection mechanisms with automation speed by identifying stolen credit card data on popular global black markets, carding forums, social channels, and chatters.

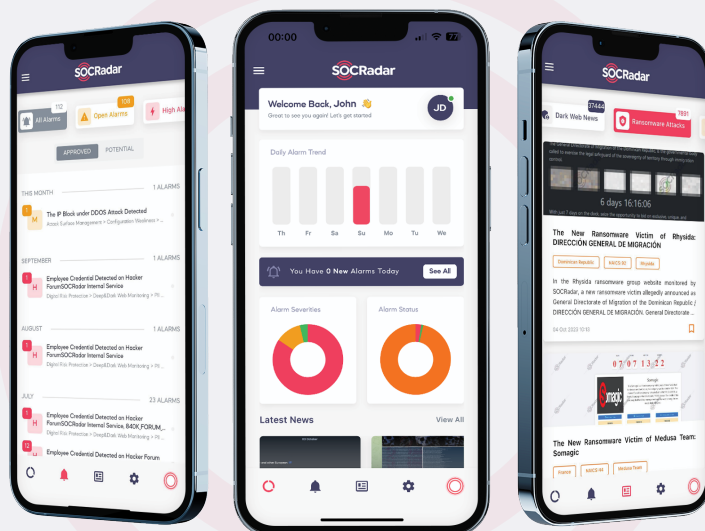
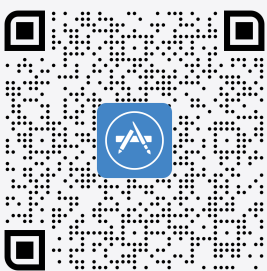
360-Degree Visibility: Achieve digital resilience by maintaining internet-facing digital asset inventory. Significantly accelerate this process by automated discovery, mapping, and continuous asset monitoring.

GET ACCESS FOR FREE

MEET THE NEW MOBILE APP

Access threat intelligence, act on-the-go, and be instantly notified of new threats. View alerts, breaking Dark Web news, and new ransomware attacks

Download on the
App Store



GET IT ON
Google Play



Gartner
Peer Insights™

