LATAM

Regional Threat Landscape Report

SOCRadar®
Your Eyes Beyond

socradar.io

SOCRadar®
Your Eyes Beyond

Table of Contents

Executive Summary

Top Takeaways

Brazil remains the primary target across all threat types, accounting for 30.98% of dark web mentions, 30.28% of ransomware attacks, and 51.25% of phishing incidents.

Public Administration is the most targeted sector, leading in both dark web threats (18.57%) and phishing attacks (16.99%), highlighting persistent focus on government systems.

Data theft dominates cybercrime in the region, with 64.78% of dark web threat types involving stolen data and over 2.68 million exposed credentials from stealer logs.

Ransomware activity is fragmented, with RansomHub (14.25%) and Akira (9.65%) being the most active known groups, but 70.61% of incidents are attributed to “Other.”

Stealer logs reveal indiscriminate data harvesting, with credentials from popular domains like globo.com and mercadolibre captured simply because users accessed them on infected devices.

65% of phishing attacks use HTTPS, showing that a secure connection is no longer a sign of legitimacy.

Technical Details

This report based on data collected between May 2024 and May 2025

In the following chapters, you will be reading about the various aspects of the cyber threat landscape around the LATAM region.

In the Dark Web Threats chapter, we will be covering the news and developments from Dark Web Forums, Telegram channels, Discord groups and so on. These are areas where threat actors with various skill sets come together, discuss, share tools and publish their alleged cyber attacks.

In the Ransomware Threats chapter you will find detailed information about ransomware actors targeting LATAM, their detailed profiles and the necessary data that summarizes the ransomware activities.

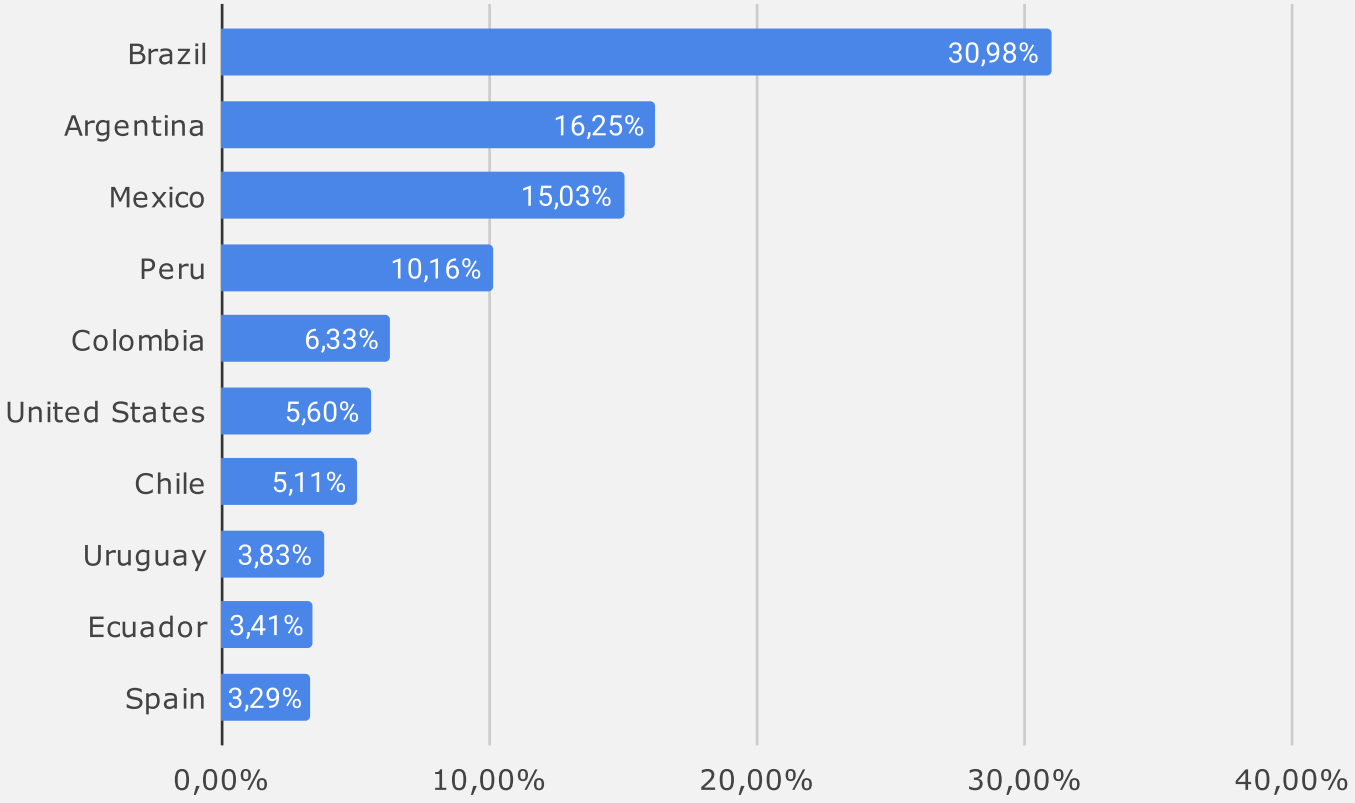
Stealer Logs Statistics chapter is all about stealer malware and the data around leaked credentials. These days, hackers don't hack, they log in. It is important to make sure that employee credentials are not compromised.

The Phishing Threats chapter will show you how threat actors target various organizations with fake websites. By examining the data here, you can take the necessary steps to prevent your employees from falling into threat actors' traps.

And lastly, the DDoS Attack Statistics shows you the latest information about the intensity of DDoS attacks and how threat actors target organizations to disrupt their operations.

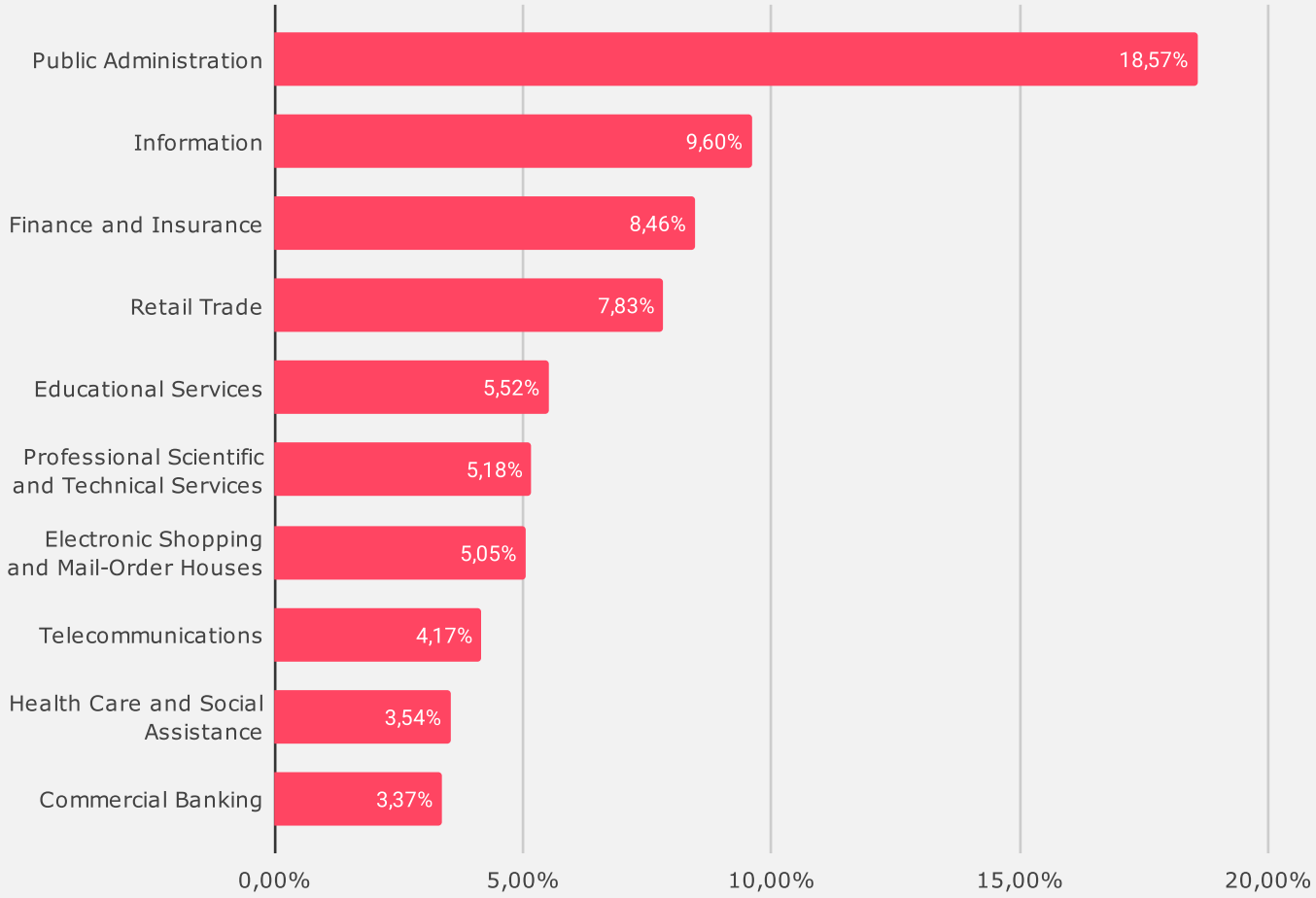
Dark Web Threats

Distribution of Dark Web Threats by Country



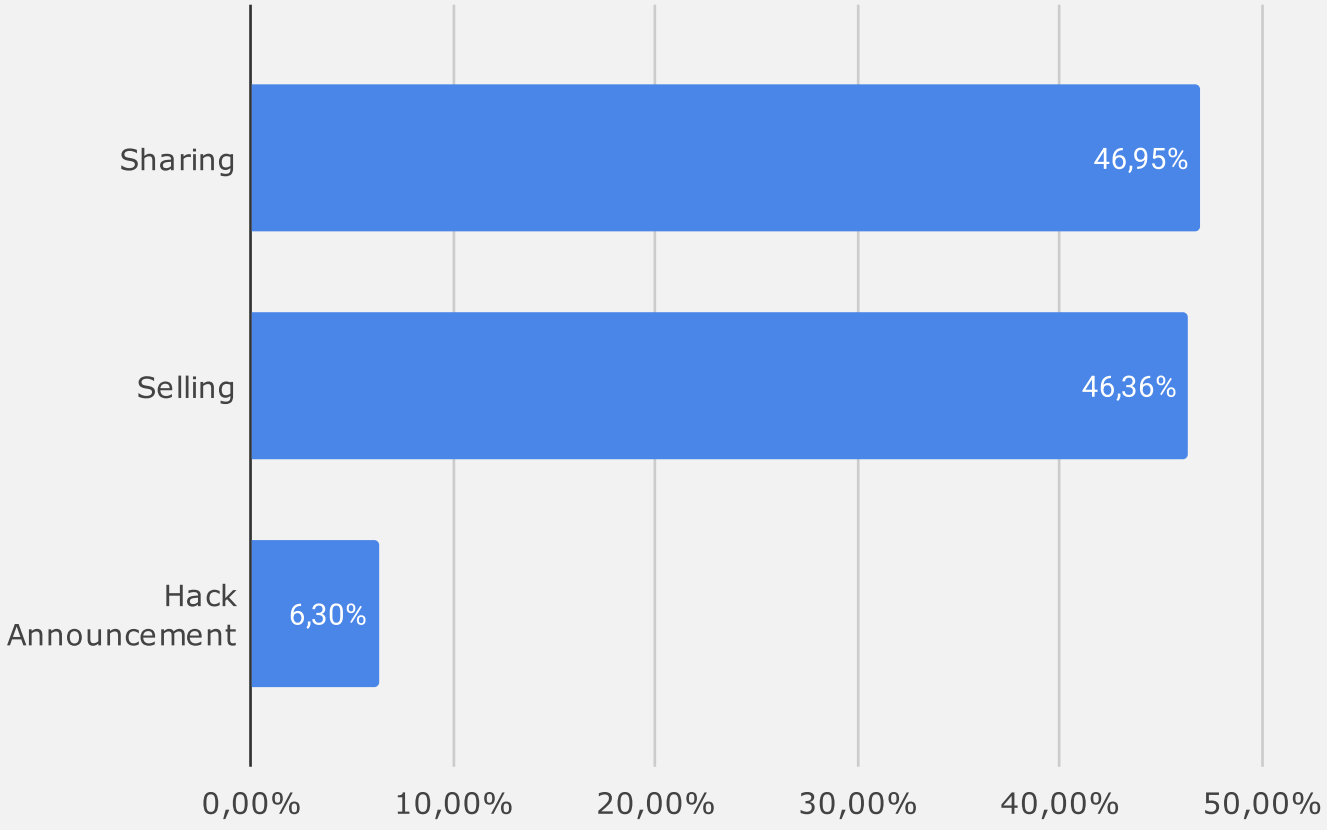
The data reveals Brazil as the most targeted country in the LATAM region, accounting for nearly 31% of dark web activity, double that of the next highest, Argentina (16.25%). Mexico and Peru follow, showing that larger economies tend to attract more cybercriminal attention. Interestingly, non-LATAM countries like the United States (5.60%) and Spain (3.29%) also appear, due to regional linkages and incidents impacting several branches or locations of one organization. The focus on Brazil suggests persistent threat actor interest, possibly due to its economic size and digital footprint.

Distribution of Dark Web Threats by Industry



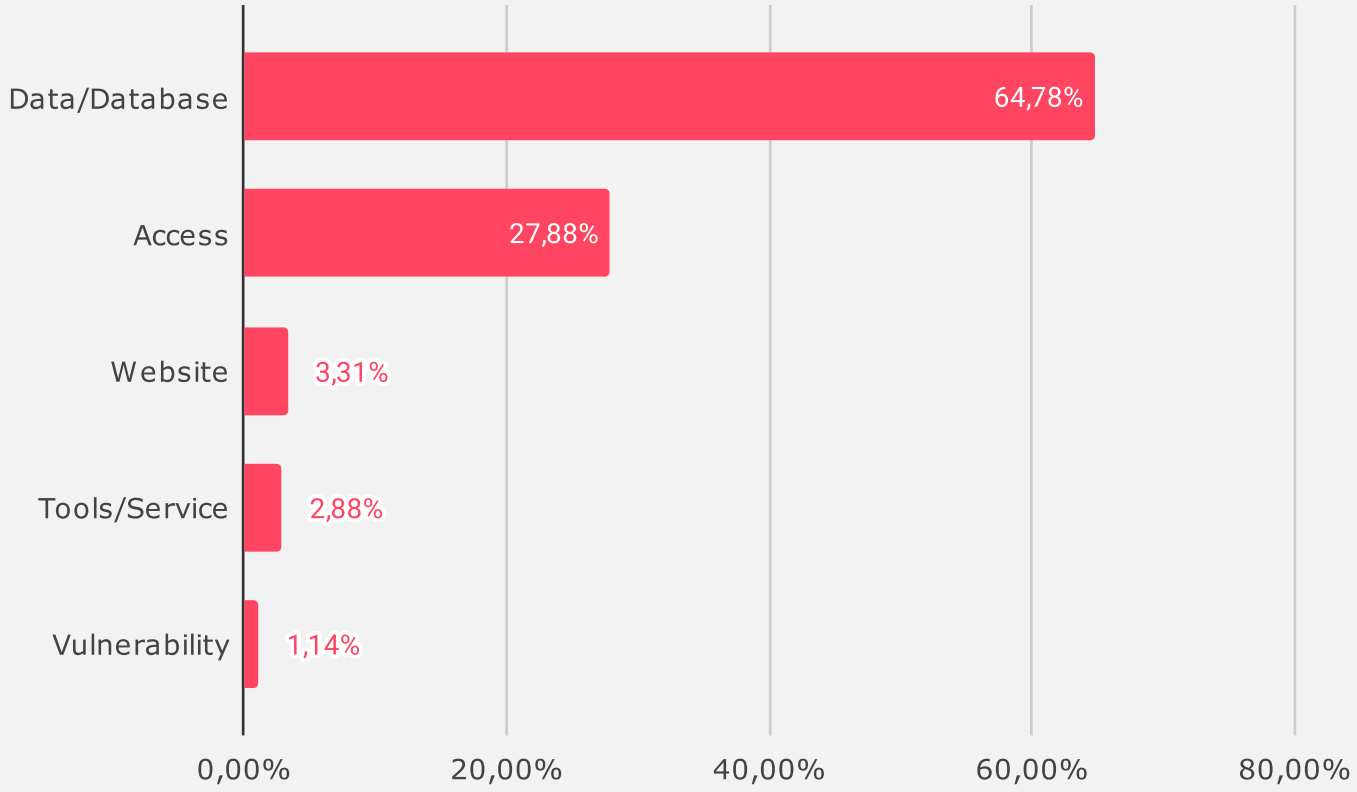
Public Administration is the most targeted sector in LATAM, comprising 18.57% of dark web threats, highlighting cybercriminal interest in government systems, possibly for data theft or disruption. The Information and Finance sectors follow, reflecting their high-value digital assets and sensitive data. Retail and e-commerce (Electronic Shopping and Mail-Order Houses) also feature prominently, indicating risks related to customer data and payment systems. The presence of Educational and Health sectors suggests broader targeting across less secure but data-rich environments. Overall, the threat landscape spans both critical infrastructure and commercial sectors.

Distribution of Dark Web Threats by Threat Categories



The data shows that nearly all dark web threats fall into two primary categories: Sharing (46.95%) and Selling (46.36%). This indicates that most malicious activity involves the distribution or commercialization of stolen data, tools, or access. Hack Announcements account for just 6.30%, suggesting that while some actors publicize breaches, the majority focus on operational gains rather than reputation. The close split between Sharing and Selling highlights a dual motive landscape, community engagement and profit.

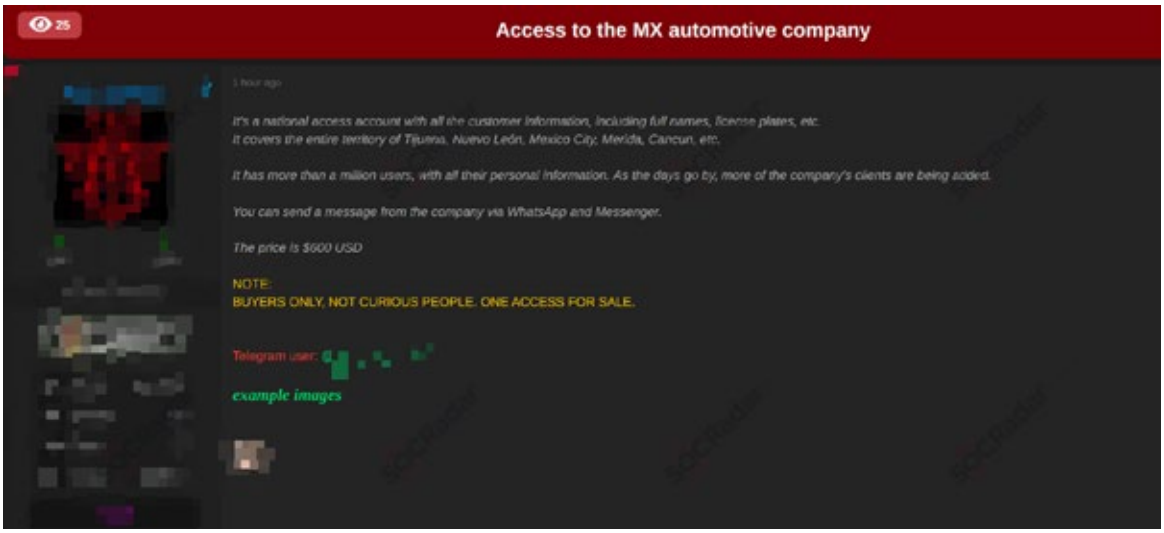
Distribution of Dark Web Threats by Threat Types



Data and database-related threats dominate the dark web landscape at 64.78%, indicating a strong focus on exfiltrating and distributing sensitive information. Access threats follow at 27.88%, suggesting significant demand for unauthorized entry points into systems or networks. Website compromises (3.31%), malicious tools/services (2.88%), and vulnerabilities (1.14%) are far less frequent, highlighting that attackers prioritize tangible assets like data and credentials over exploits or technical resources. The trend points to data as the primary commodity driving underground activity.

Recent Dark Web Activities Targeting the Entities in LATAM

Massive Data Access Sale Targeting Mexican Transportation or Mobility Service



SOCRadar has identified a post on a hacker forum advertising unauthorized access to a major digital service operating across Mexico, likely in the transportation, mobility, or public service sector.

The access is national in scope, covering key regions such as Tijuana, Nuevo León, Mexico City, Mérida, and Cancún. The dataset includes personal information of over one million users, including full names, license plates, and more. The seller claims that additional user data is being added over time, suggesting ongoing access or data extraction.

Notably, the access reportedly allows the attacker to send messages to users through official communication channels like WhatsApp and Messenger, indicating a deep compromise of internal systems.

Leaked Voter Database Targeting Mexican Citizens Surfaces on Hacker Forum

An alleged data leak targeting the public sector in Mexico has surfaced on a hacker forum. The post claims to offer a database containing personal information of voters from the state of Nuevo León. The leaker criticized the circulation of outdated data and stated this dataset is more recent and valuable.

Alleged Data Breach Targets Paraguay's Agricultural Sector

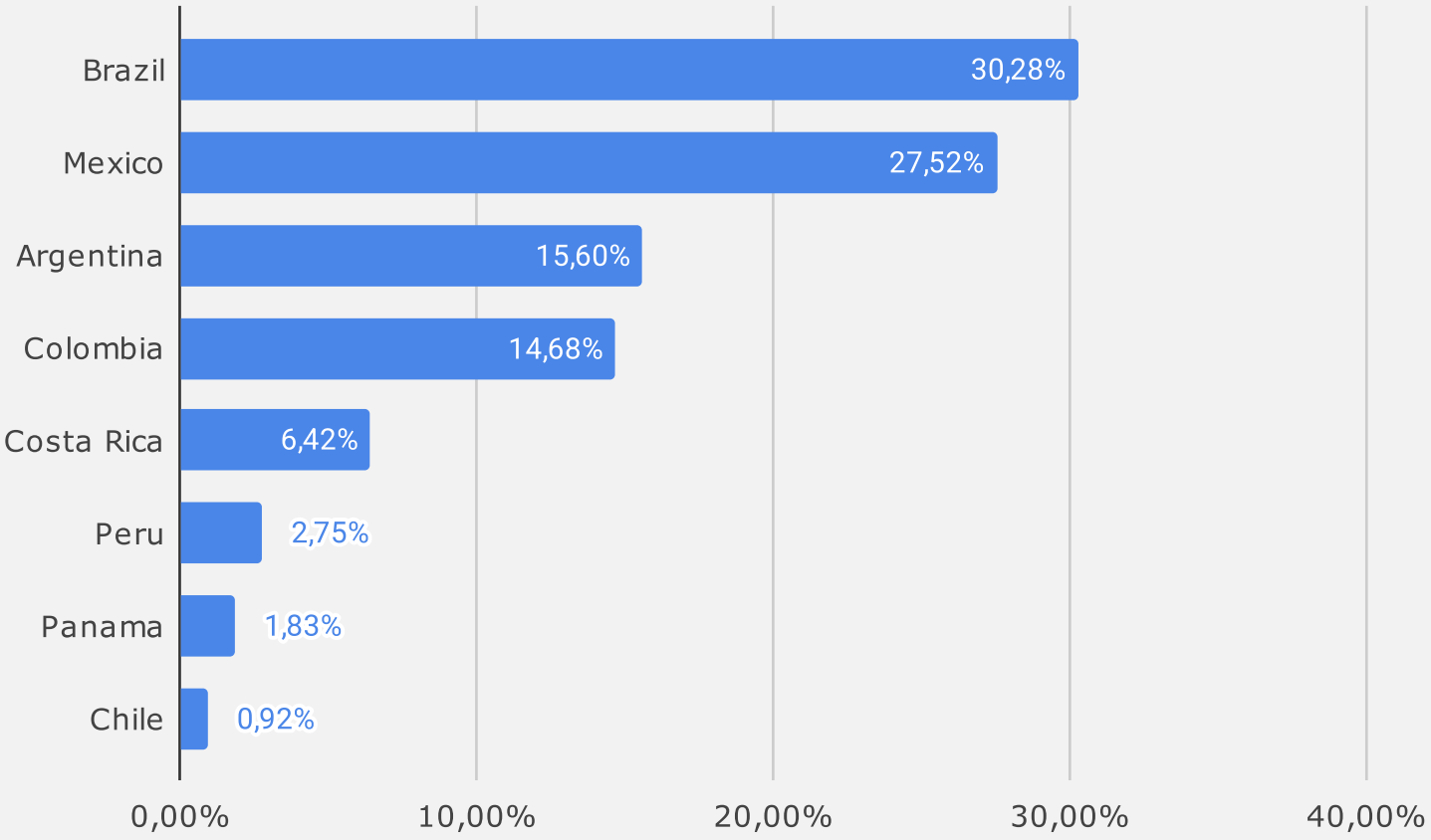
The threat actor shared what they claim is a list of suppliers linked to Paraguay's Ministry of Agriculture, along with additional files in CSV format. Although the original source link appears to be inactive, credentials were included in the post.

The actor also issued a warning directed at Paraguay's national technology and communications institution, criticizing its cybersecurity posture and claiming unauthorized access to internal systems.

This incident highlights the increasing threat landscape facing government agencies in Latin America's agricultural and public sector infrastructure.

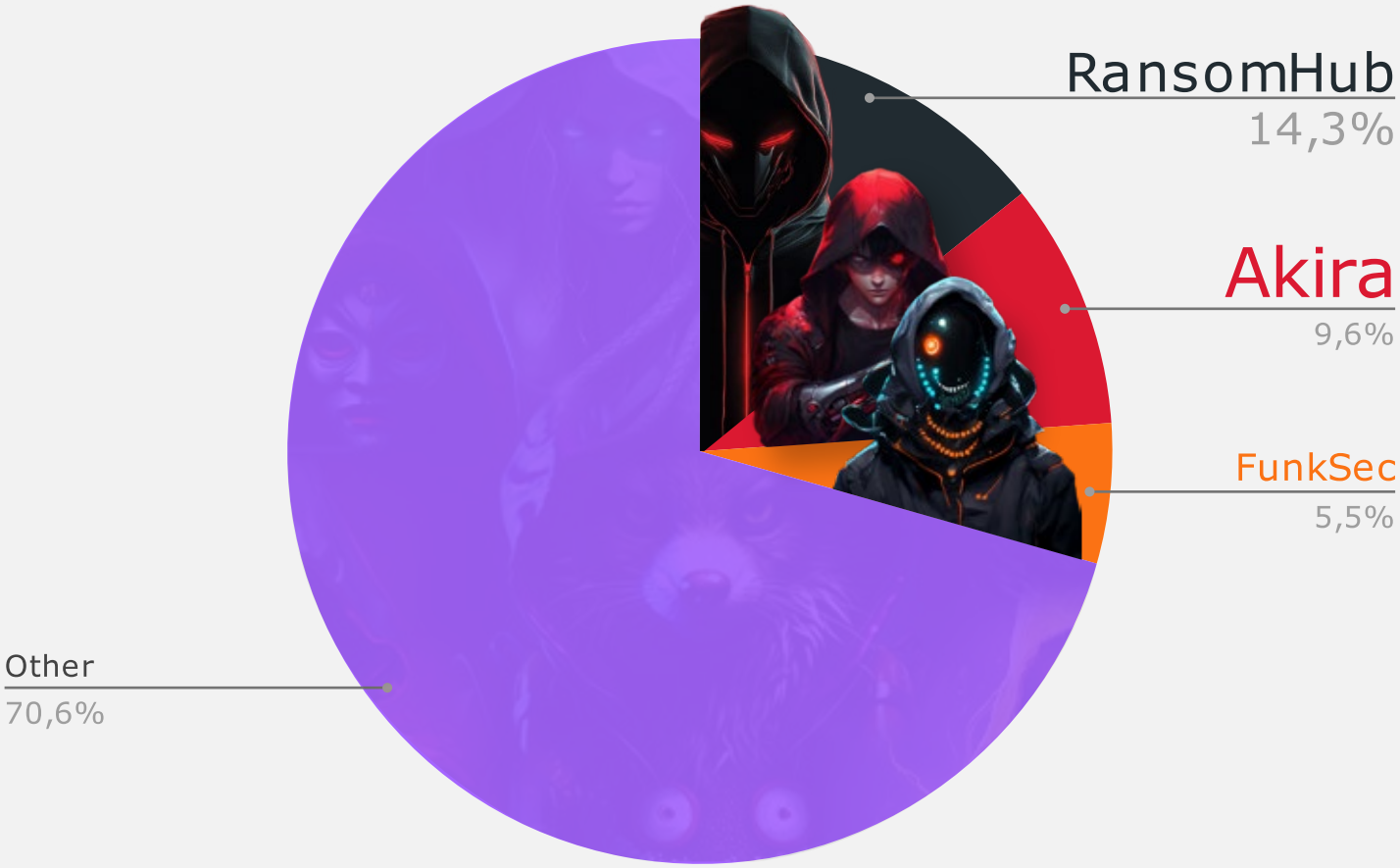
Ransomware Threats

Distribution of Ransomware Attacks by Country



Brazil (30.28%) and Mexico (27.52%) account for over half of ransomware attacks in LATAM, indicating that larger economies face greater targeting, due to broader digital infrastructure and higher potential payouts. Argentina and Colombia also show notable exposure, while countries like Chile and Panama report minimal incidents. The concentration in top economies suggests attackers prioritize regions where disruption or data theft may yield significant leverage or financial gain.

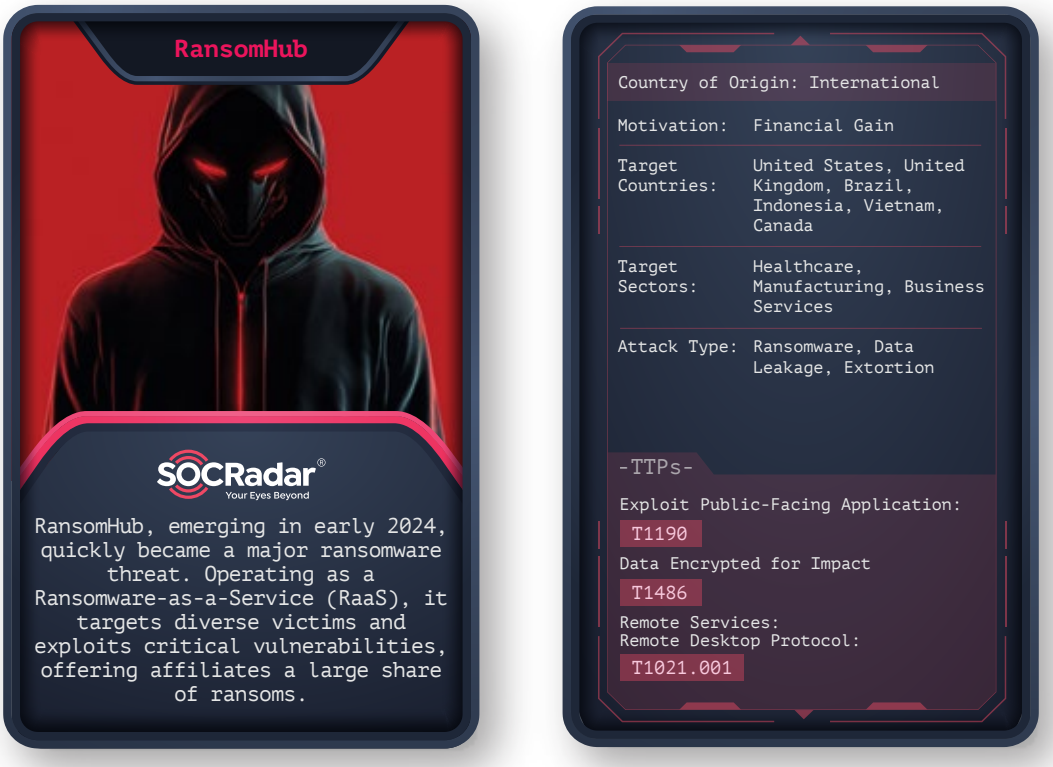
Top Ransomware Groups Targeting LATAM



RansomHub (14.3%) and Akira (9.65%) are the most active known ransomware groups targeting LATAM, with FunkSec trailing at 5.48%. However, a significant majority of incidents (70.61%) fall under “Other,” indicating a highly fragmented threat landscape with many lesser-known or emerging groups. This diversity complicates attribution and suggests that LATAM remains a target-rich environment for both established and new ransomware actors.

A Closer Look into The Top 3 Ransomware Groups

RansomHub



As stated on the group's About page, RansomHub is comprised of hackers from various locations united by a common goal of financial gain. The gang explicitly mentions prohibiting attacks on specific countries and non-profit organizations. In February 2024, RansomHub posted its first victim, the Brazilian company YKP.

The gang's website states that they refrain from targeting CIS, Cuba, North Korea, and China. While they suggest a global hacker community, their operations notably resemble a traditional Russian ransomware setup. Their stance on Russian-affiliated nations and the overlap in targeted companies with other Russian ransomware groups are also worth noting.

You can visit our *blog post* for more detailed information about RansomHub.

Akira

Since its discovery in early 2023, Akira ransomware has evolved from a seemingly ordinary addition to the ransomware landscape to a significant threat affecting many businesses and critical infrastructure entities. This evolution and the unique aesthetic of its leak site and communications have drawn attention to its operations.

The ransom group employs a double extortion strategy, first exfiltrating data and then encrypting devices within the targeted network. Payment is then demanded not only for decrypting files but also for preventing the exposure of leaked data.

The Akira ransomware group frequently demands hefty ransoms, primarily targeting large enterprises across North America, Europe, and Australia. The malware typically spreads through targeted threat campaigns using phishing emails or exploiting software vulnerabilities, focusing on industries such as education, finance, manufacturing, and healthcare.

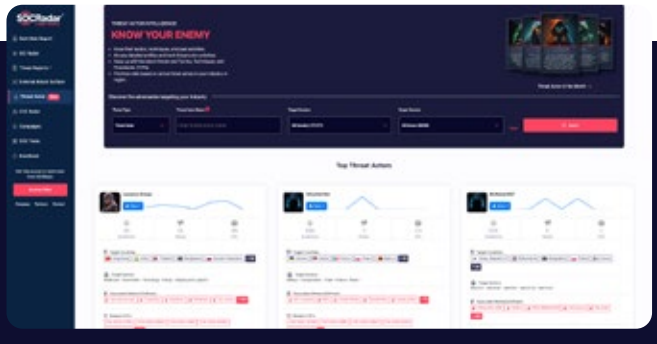
You can visit our *blog post* to read the rest of the threat actor profile.

FunkSec

FunkSec, a new ransomware group, emerged in December 2024 and claimed responsibility for attacks on multiple victims. By the time of writing the number of victims reached 129. The group appears to be involved in both hacktivism and ransomware, with members likely inexperienced and seeking recognition.

Researchers suggest that the file-encrypting malware, written in Rust, was likely developed by an inexperienced malware creator from Algeria with the assistance of AI. The developer also uploaded parts of the ransomware's source code online. Operating under the Ransomware-as-a-Service (RaaS) model, FunkSec engages in double extortion, threatening to release stolen data to coerce victims into paying the ransom.

You can visit our *blog post* to read the rest of the threat actor profile.



Threat Actor Intelligence Module

SOCRadar enhances cybersecurity measures with its *Threat Actor Intelligence Module*, which features advanced Threat Actor Tracking capabilities for organizations that want to stay ahead of cyber threats in real time.

Recent Ransomware Attacks Targeted Entities in LATAM

Brazilian Educational and Healthcare Institution Listed by Rhysida Ransomware Group

On the Rhysida ransomware group's leak site monitored by SOCRadar, a new alleged victim has been listed from the education and healthcare sector in Brazil. The affected institution, located in Cachoeiro de Itapemirim, Espírito Santo, was originally established in 1969 as a local center for higher education. Over time, it expanded its role to provide both educational and medical services to the surrounding community.

Brazilian Educational and Healthcare Institution Listed by Rhysida Ransomware Group

On the Rhysida ransomware group's leak site monitored by SOCRadar, a new alleged victim has been listed from the education and healthcare sector in Brazil. The affected institution, located in Cachoeiro de Itapemirim, Espírito Santo, was originally established in 1969 as a local center for higher education. Over time, it expanded its role to provide both educational and medical services to the surrounding community.

Medusa Ransomware Targeted a Mobile Phone Company in Venezuela

The mobile phone company was founded in 1995. The number of subscribers of the company is more than 5,000,000, and the number of employees is more than 1,100 people.

Stealer Log Statistics

What is a Stealer?

A stealer is a specialized form of malware engineered to exfiltrate sensitive information from infected devices. Stealers operate covertly, maintaining persistence while methodically collecting valuable data. Modern stealers can harvest credentials from browsers, extract cryptocurrency wallet information, capture authentication cookies and collect system information.

What are Stealer Logs?

Stealer logs are the compiled datasets of stolen information from infected devices. These logs typically contain:

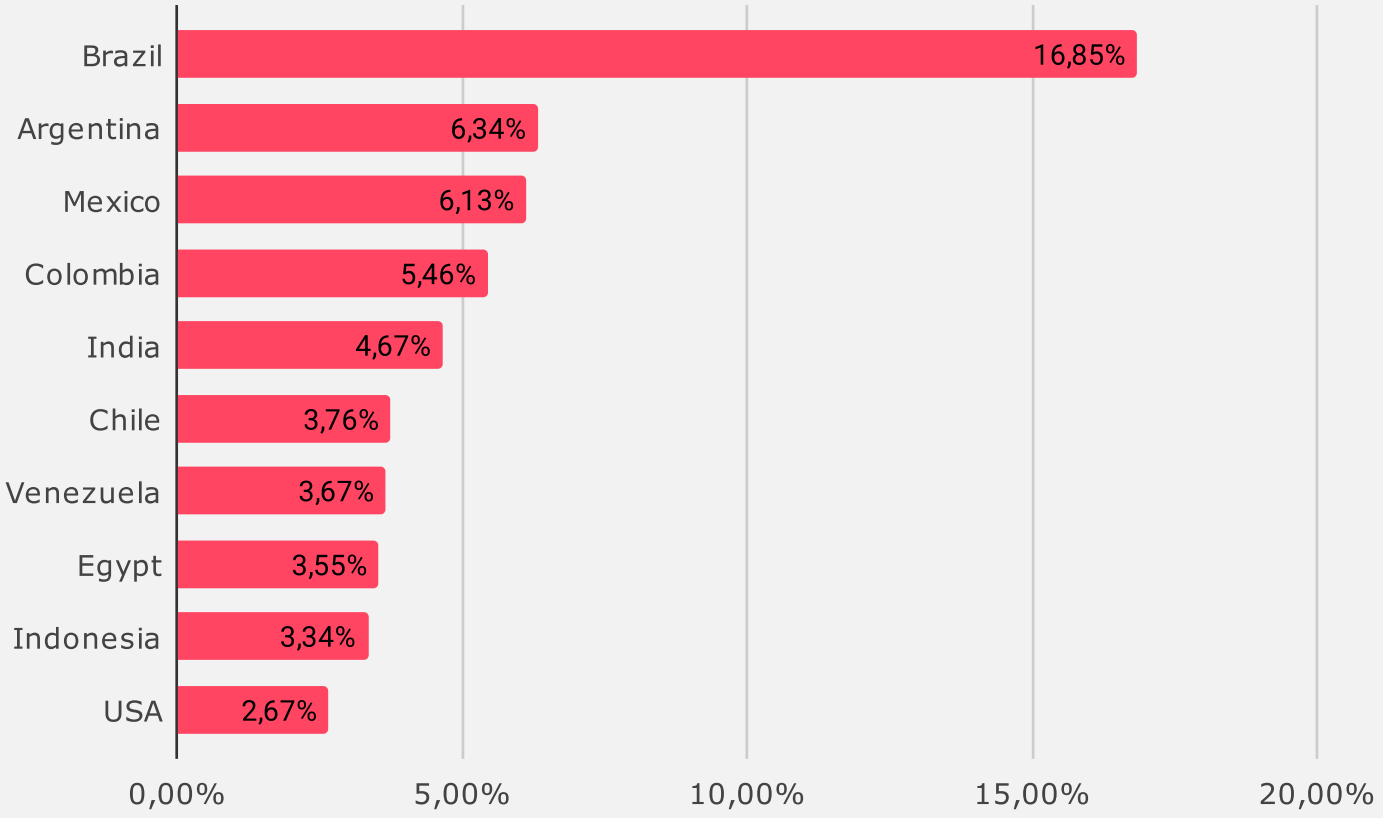
- Browser-saved credentials (usernames and passwords)
- Session cookies and authentication tokens
- Cryptocurrency wallet information and private keys
- Personal information including names, addresses, phone numbers
- Financial data such as credit card information
- System information including hardware specifications, installed software, and IP addresses
- Corporate access credentials including VPN, email, and cloud service logins

Once collected, these logs are either transmitted to command-and-control servers controlled by the threat actors or stored locally for retrieval. Threat actors then either use these logs themselves or sell them on underground marketplaces.

Stealer Log Statistics: Most Visited Domains in LATAM

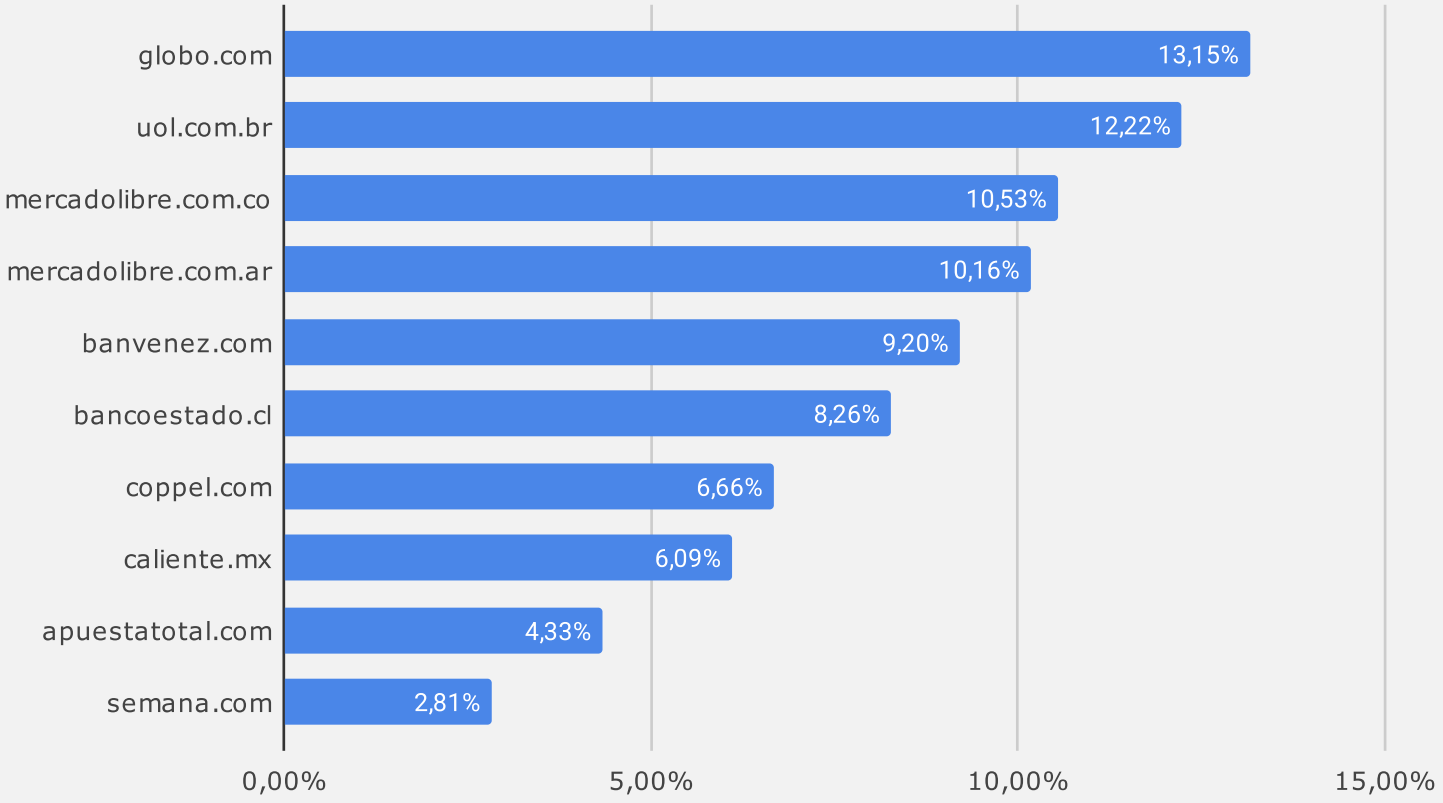
Most Visited Domains		
ecuabet.com	mercadolibre.com.ar	infobae.com
abc.com.py	uol.com.br	caliente.mx
apuestatotal.com	biobiochile.cl	betcha.pa
montevideo.com.uy	semana.com	leercapitulo.co
2001online.com	ultimahora.com	laprensa.hn
conflictnations.com	futbollibres.pe	librefutbol.su
koptical.net	elpais.com.uy	crhoy.com
ucr.ac.cr	banvenez.com	livebyoptimum.com
prensalibre.com	mercadolibre.com.co	pr.gov
diez.hn	bancoestado.cl	paryajlakay.com
coppel.com	globo.com	conectate.com.do

Stealer Logs - Distribution of the Compromised Data by Victim Countries



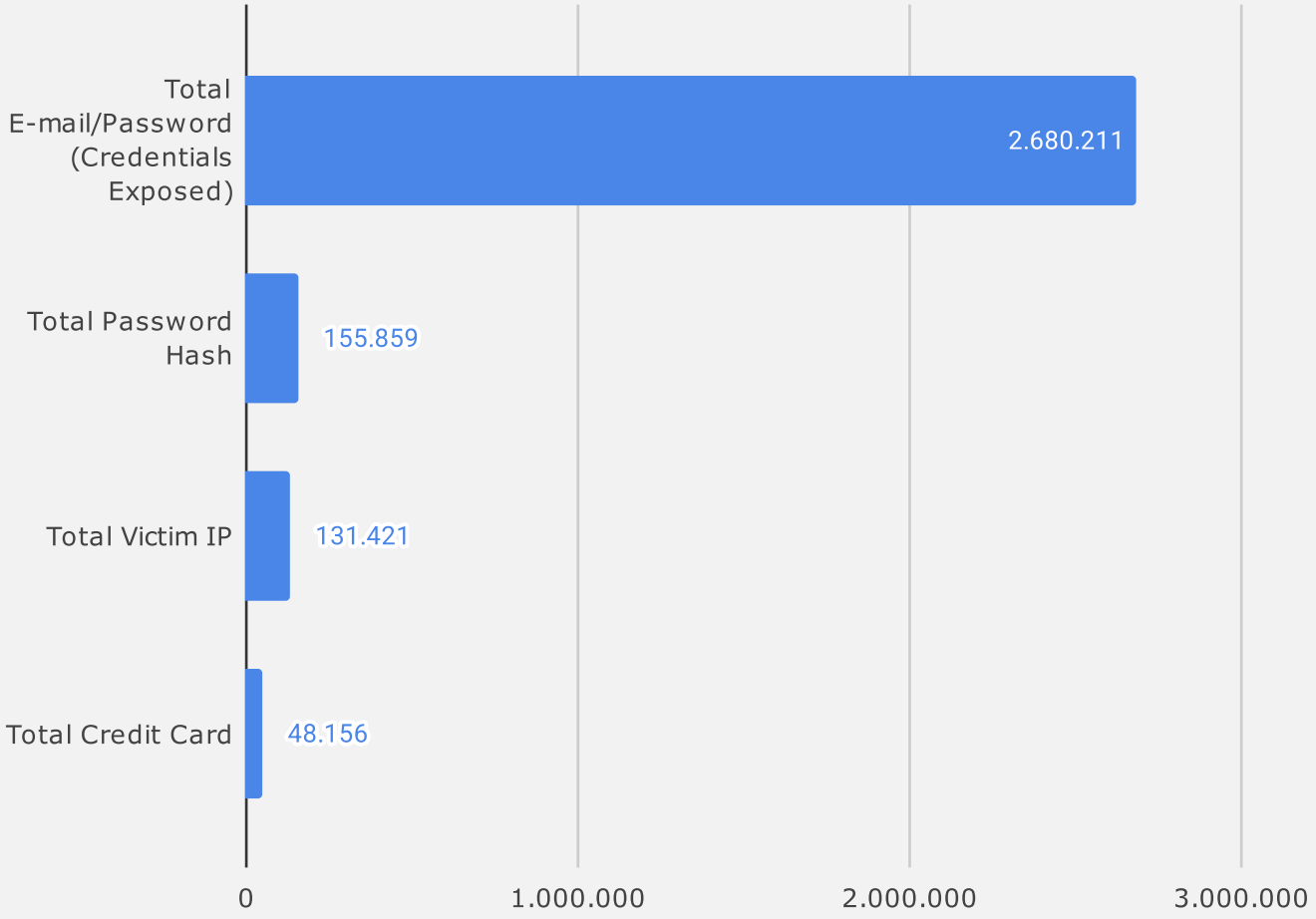
Brazil stands out as the primary source of compromised data in stealer logs, with 16.85% of the observed cases, far exceeding other countries in LATAM. Argentina, Mexico, and Colombia also show notable victimization, reflecting a broader regional exposure to infostealer malware. Interestingly, non-LATAM countries such as India, Egypt, and Indonesia appear in the top 10, indicating global reach. The presence of the USA (2.67%) may reflect spillover effects or indiscriminate targeting. Overall, the data highlights Brazil as a consistent high-risk zone, and reinforces the global scope and indiscriminate nature of stealer campaigns.

Stealer Logs - Distribution of the Compromised Data by Domains

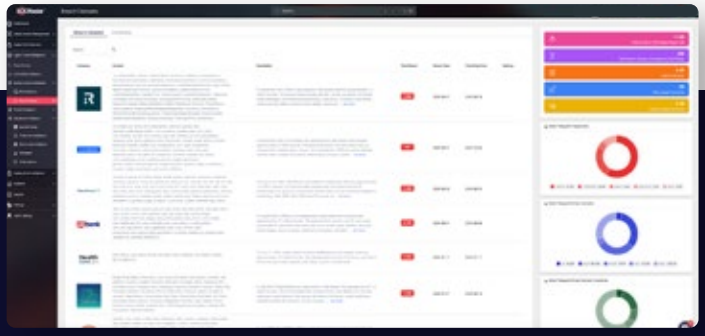


The presence of credentials linked to domains like globo.com (13.15%) and uol.com.br (12.22%) in stealer logs reflects the popularity of these services. It shows that users had stored or accessed these platforms on compromised devices. The inclusion of retail (coppel.com) and gambling domains (caliente.mx, apuestatotal.com) indicates a broader threat landscape. These trends underscore the value cybercriminals place on credentials for high-traffic, locally trusted services in LATAM.

Stealer Logs - Distribution of the Compromised Data



The stealer logs reveal a substantial volume of compromised data, with over 2.68 million exposed email and password combinations. Additionally, 155,859 password hashes were collected, suggesting attempts to store credentials securely were still vulnerable. The presence of 131,421 unique victim IP addresses highlights the broad geographic spread of infections. Notably, 48,156 stolen credit card records point to a significant financial threat. These figures underscore the scale and impact of stealer malware, which silently extracts sensitive data from infected devices without targeting specific users or platforms.

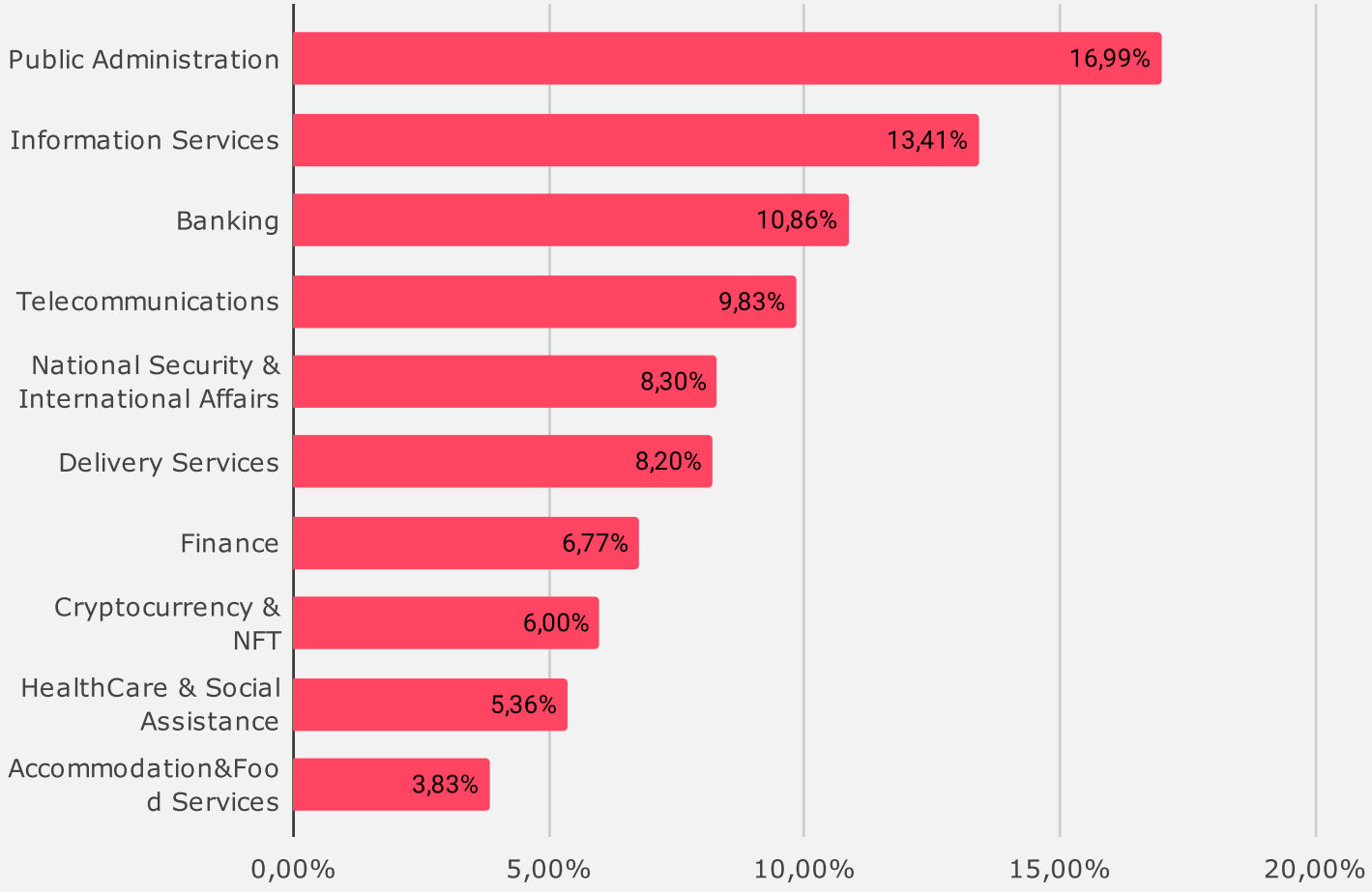


SOCRadar's Identity & Access Intelligence Module

SOCRadar's Identity & Access Intelligence Module can detect stealers on your devices and identify their location, facilitating a secure working environment. Changing passwords without eliminating stealers is insufficient to secure your organization, as it will only provide new passwords to threat actors.

Phishing Threats

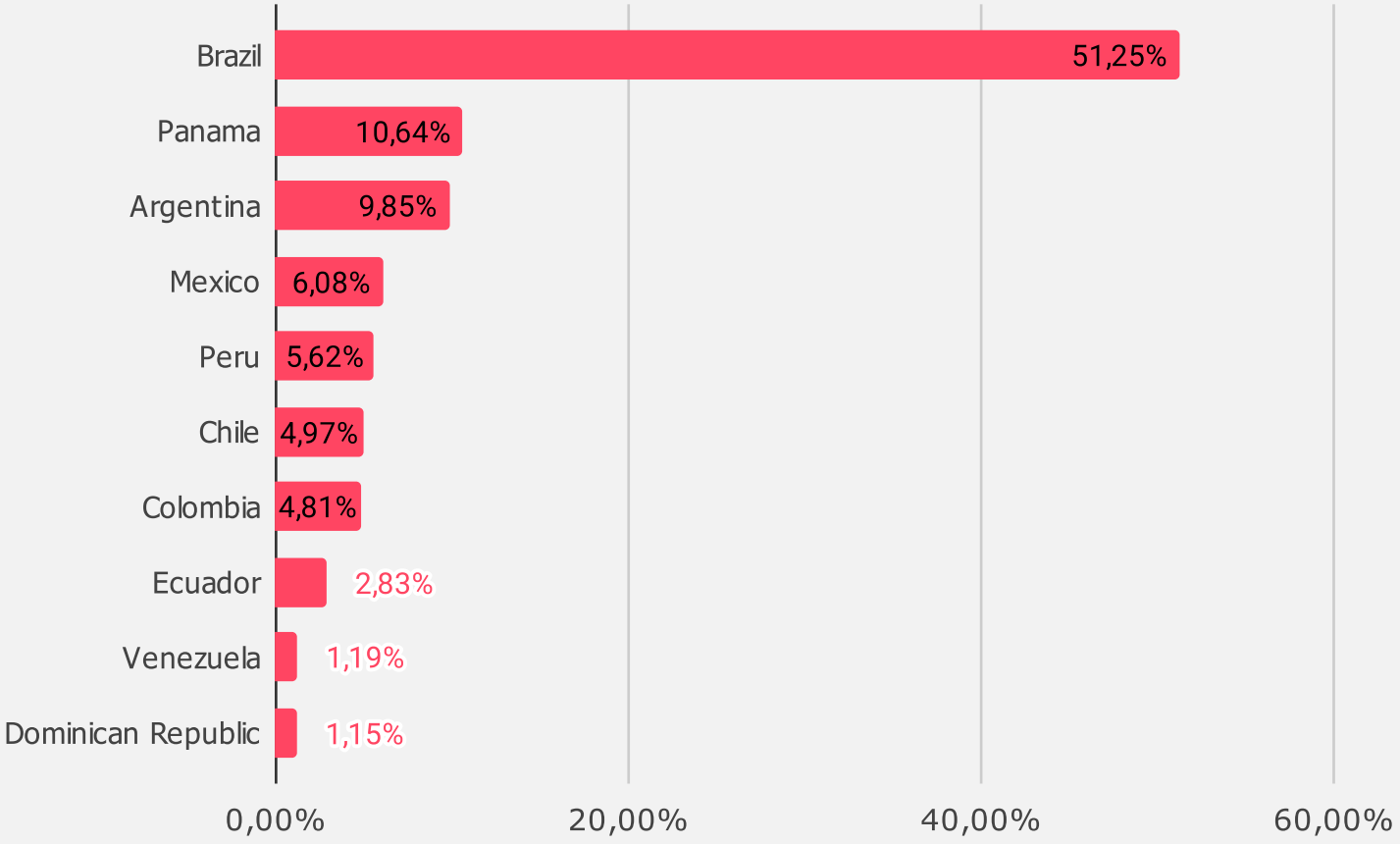
Phishing Attacks - Distribution by Industry



Phishing attacks are most frequently observed in the Public Administration sector (16.99%), indicating persistent attempts to exploit government-related systems and personnel. Information Services (13.41%) and Banking (10.86%) follow closely, reflecting the high value of data and financial access in these industries. Notably, sectors like Telecommunications, National Security, and Delivery Services also face substantial exposure, suggesting attackers are targeting both infrastructure and logistical networks. Another reason for Delivery Services might be related to the fast paced nature of this business where users are required to answer phone calls, use confirmation codes and on certain occasions share more sensitive personal information. The presence of Cryptocurrency & NFT (6.00%) highlights growing interest in digital assets.

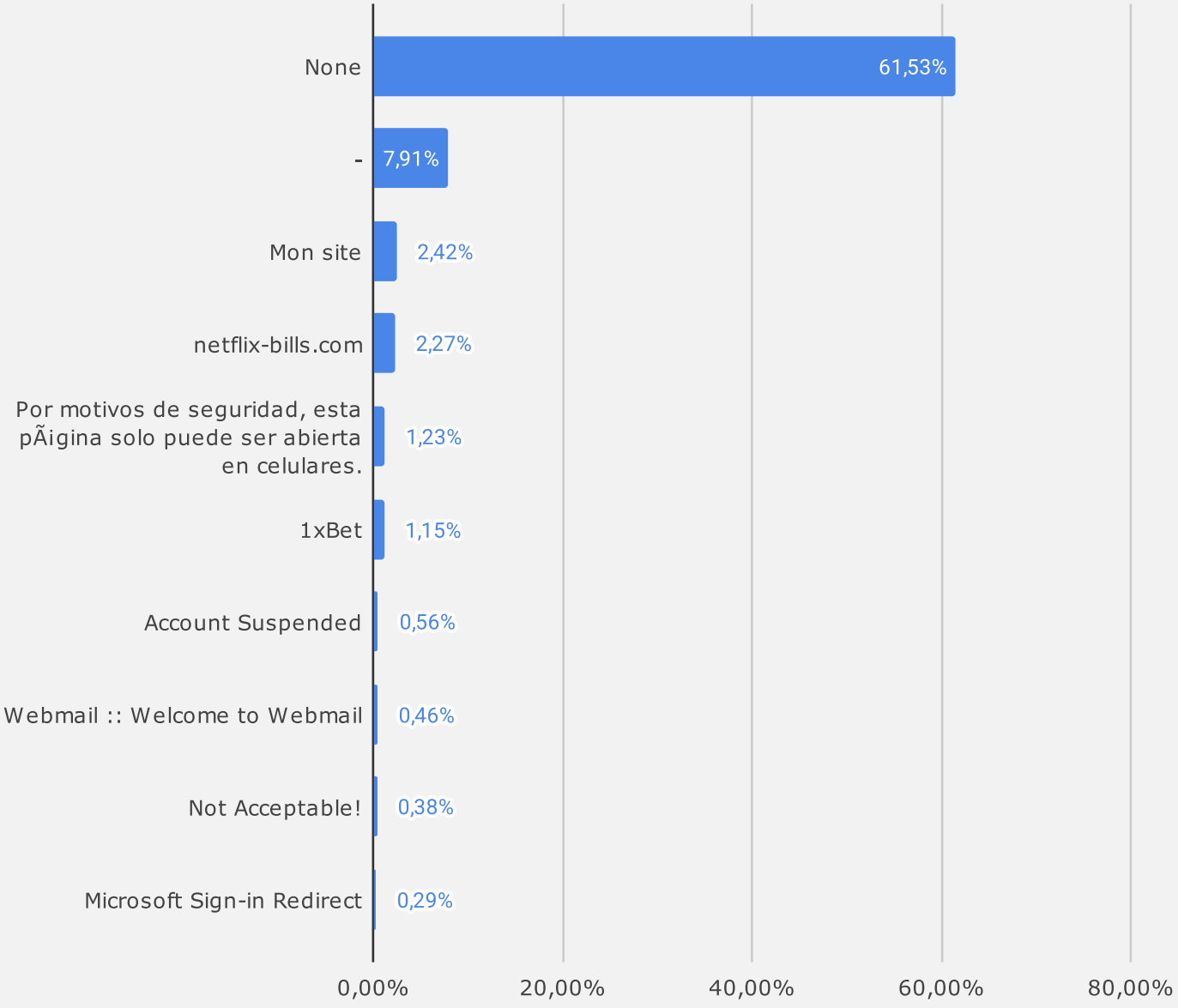
Overall, phishing campaigns show a broad distribution, affecting both public and private sectors with high data or financial stakes.

Phishing Attacks - Distribution by Country



Brazil accounts for over half of all phishing attacks in the dataset (51.25%), making it the primary hotspot in the region. This dominance may reflect Brazil's large digital user base and economic size. Panama (10.64%) and Argentina (9.85%) follow, showing that phishing activity is also significant in smaller but economically active countries. The rest of the region, including Mexico, Peru, and Chile, shows moderate levels of activity.

Phishing Attacks - Distribution by Phishing Page Title



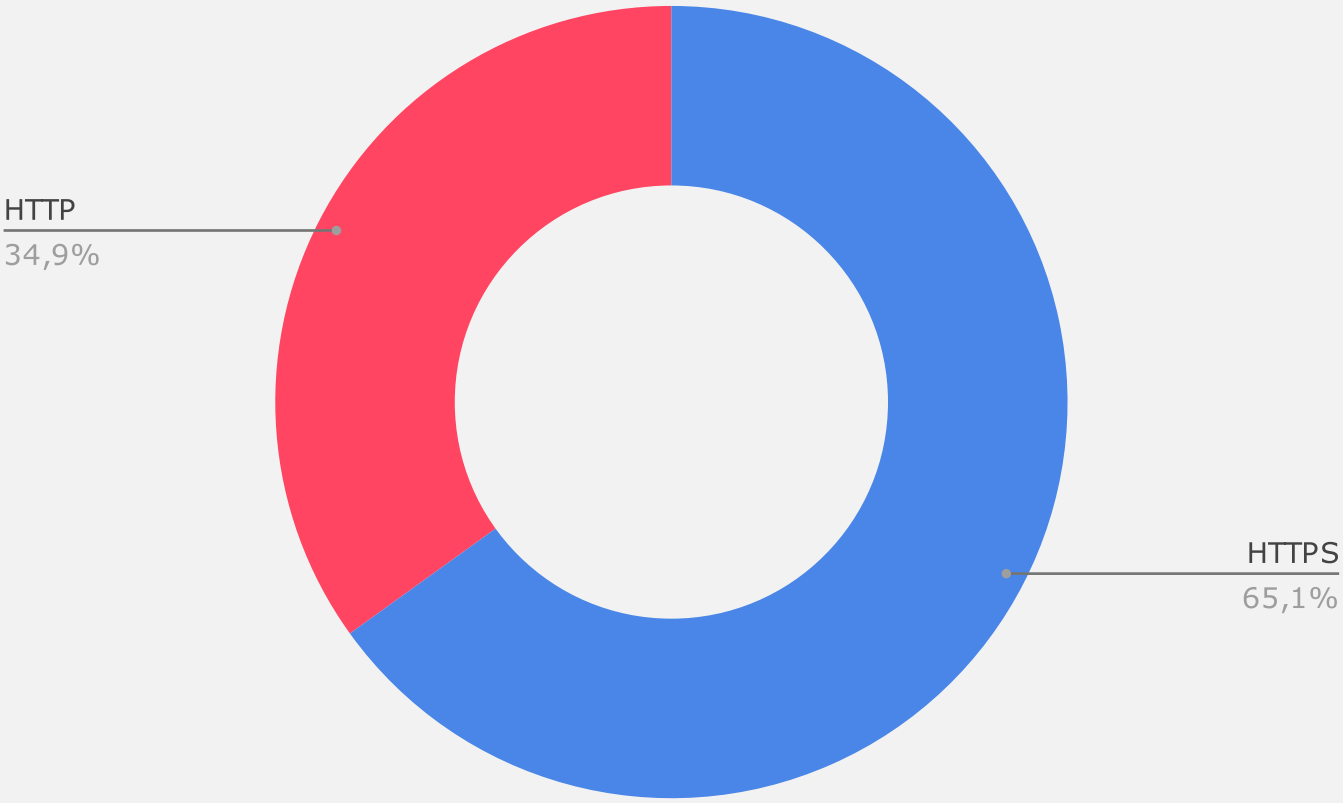
The majority of phishing pages (61.53%) lack a defined title, suggesting either automated deployments or intentional obfuscation to evade detection. Generic or placeholder titles like “-” (7.91%) and “Mon site” (2.42%) further indicate low-effort or mass phishing campaigns.

Some pages mimic recognizable services such as Netflix (2.27%), 1xBet (1.15%), and Microsoft login portals (0.29%), aiming to trick users into credential disclosure.

Other entries like “Account Suspended” and “Webmail :: Welcome to Webmail” show attempts to create urgency or impersonate common platforms.

Overall, the data reflects a mix of unsophisticated and brand-specific phishing strategies.

Phishing Attacks - Distribution by SSL/TLS Protocol



A majority of phishing attacks (65.07%) use HTTPS, indicating that threat actors are increasingly adopting SSL/TLS encryption to make their malicious sites appear legitimate and bypass basic security checks. Meanwhile, 34.93% of phishing pages still operate over unsecured HTTP, which may reflect lower sophistication or older infrastructure. The widespread use of HTTPS underscores that the presence of a secure connection alone is no longer a reliable indicator of site safety.

Lessons Learned: Key Insights and Strategic Recommendations

Strategic Recommendations

- **Invest in Comprehensive Threat Intelligence:** Staying informed about evolving threats and actors enables more proactive defenses.
- **Harden Authentication Mechanisms:** Deploy MFA and encourage password hygiene to protect against credential theft.
- **Enhance Incident Response Capabilities:** Develop and regularly test robust response and recovery plans, particularly for ransomware attacks.
- **Strengthen Employee Awareness:** Security awareness training is essential to combat phishing and social engineering attacks.
- **Collaborate for Greater Resilience:** Share intelligence with industry peers and cybersecurity alliances to stay ahead of emerging threats.

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.

Trusted by
21.000+ companies
in **150+ countries**

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

START YOUR FREE TRIAL

Discover SOCRadar's powerful tools and easy-to-use interface to enhance cyber threat intelligence efforts. Schedule a demo with our experts to see it in action, and we'll show you what SOCRadar can do.