SOCRadar®
Your Eyes Beyond

BRAZIL

Threat Landscape Report 2024

SOCRadar®
Your Eyes Beyond

Table of Contents

Executive Summary

As Latin America's largest economy and one of the most influential global players, Brazil occupies a central role in regional economic and geopolitical dynamics. Its diverse economy, which spans agriculture, mining, technology, and finance, rapidly embraces digital transformation. However, this growth comes with heightened vulnerability to an expanding array of cyber threats.

Amidst intensifying geopolitical challenges and a fast-evolving cyber landscape, Brazil has increasingly become a target for criminal and state-backed cyber actors. Threat actors frequently seek to exploit weaknesses in Brazil's expanding digital infrastructure, with particular emphasis on sectors such as finance, energy, and government, where the potential for disruption and financial gain is substantial.

Our findings point to a surge in ransomware attacks, data breaches, and sophisticated phishing operations aimed at Brazilian organizations. Notably, there has been a rise in activity linked to Advanced Persistent Threat (APT) groups, often tied to nation-states, targeting Brazil's critical infrastructure to extract sensitive information or disrupt essential services.

The growing prominence of the Dark Web has also given cybercriminals a platform to exchange tools, trade in stolen data, and coordinate attacks with greater anonymity. This has contributed to the increasing complexity of the threat environment, especially as ransomware-as-a-service (RaaS) offerings enable even inexperienced attackers to inflict significant damage on Brazilian enterprises.

This report delivers an in-depth analysis of Brazil's cyber threat landscape, drawing on open-source intelligence and proprietary research to assess the most pressing risks. It is intended to guide decision-makers in both the public and private sectors, helping them to refine their defensive strategies, reduce exposure to cyber risks, and bolster the country's resilience against increasingly sophisticated cyber threats.

To access SOCRadar's 2023 Brazil report, **click here.**

Top Takeaways

Dark Web Dynamics: In 2024, a diverse group of 91 threat actors actively targeted Brazilian enterprises, posting 629 times on the Dark Web. These activities predominantly revolved around the sale of databases, emphasizing the critical need for robust data security measures.

Dark Eyes on Public Administration: The public administration sector accounted for 10.65% of the Dark Web activities, making it the industry most targeted by global threat actors. This underscores the sector's strategic significance and its susceptibility to digital threats.

Ransomware Resurgence: Brazil faced 248 distinct ransomware incidents throughout the year, with 166 attacks targeting the country. This demonstrates a concentrated effort by cybercriminals to exploit Brazilian entities.

Notorious Ransomware Syndicates: High-profile ransomware groups like LockBit 3.0, Conti, and ALPHV BlackCat aggressively targeted Brazil, reflecting the heightened sophistication and severity of the country's cyber threat landscape.

Stealer Logs: The widespread use of Stealer Logs in 2024 resulted in substantial data breaches, compromising sensitive information for thousands of individuals across Brazil.

Phishing in the Digital Economy: 1,449 phishing attacks were recorded during the year, primarily impacting the emerging Information Services industry. This underscores the increasing cyber risks facing this rapidly growing sector in Brazil.

Unprecedented DDoS Attacks: Brazil endured a record-breaking Distributed Denial of Service (DDoS) attack involving 23 different vectors, reaching a peak bandwidth of 4 Tbps. This occurred within a broader context of 372,825 DDoS incidents, illustrating the intensity and escalation of cyber assaults targeting the country.

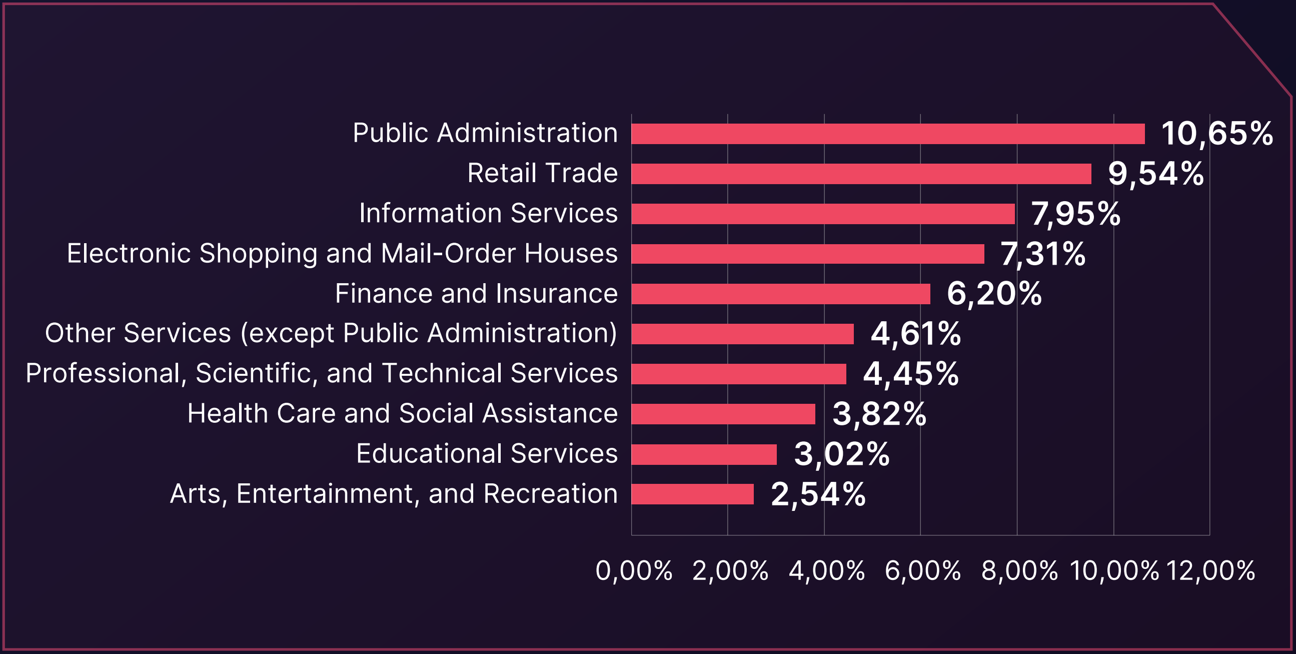
Technical Details

Dark Web Threats Targeting Brazilian Entities

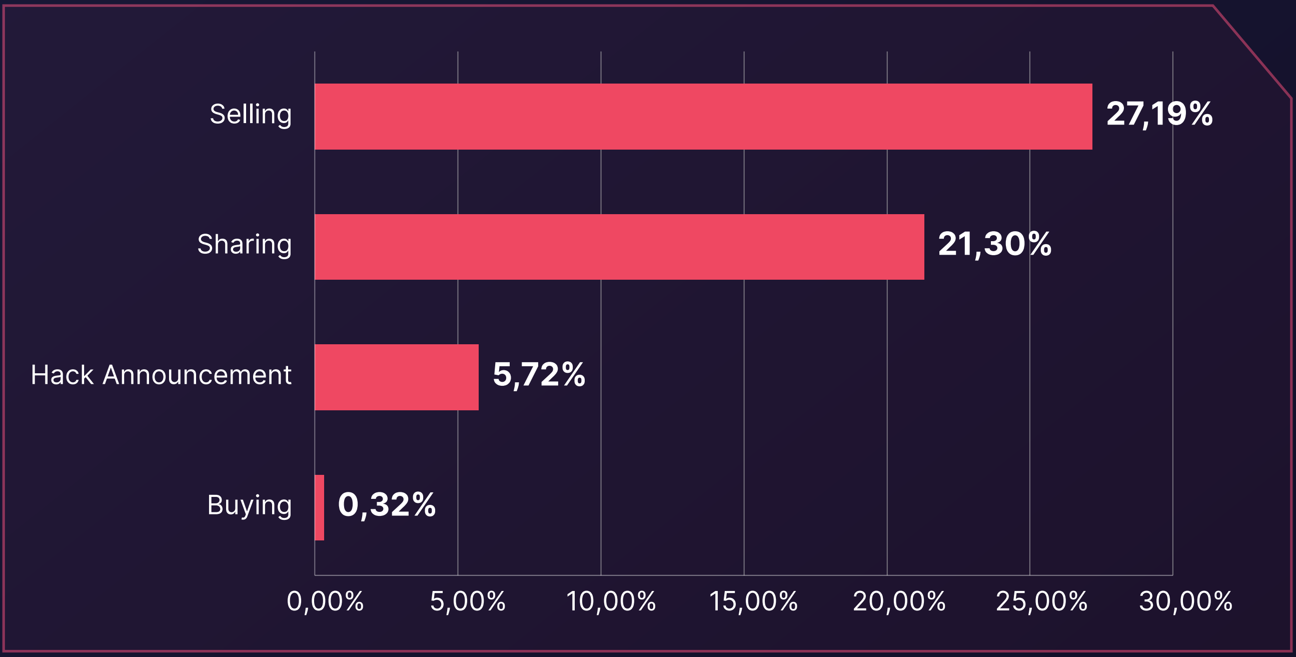
Over the preceding year, SOCRadar's Dark Web Analysts diligently monitored activities within the Dark Web, identifying notable trends and establishing connections between Brazilian enterprises and covert threat actors. Throughout 2024, Brazilian entities encountered a continuous barrage of cyber threats, with various actors attempting to exploit successful intrusions by trading or leveraging their gains in Dark Web forums.

SOCRadar observed 629 Dark Web forum posts linked to 91 distinct threat actors during this period. Public Administration emerged as the most prominently affected industry among the targeted industries, representing 10.65% of the identified cyber threats during this period. Following closely behind, the Retail Trade and Information Services industries accounted for 9.45% and 7.95% respectively.

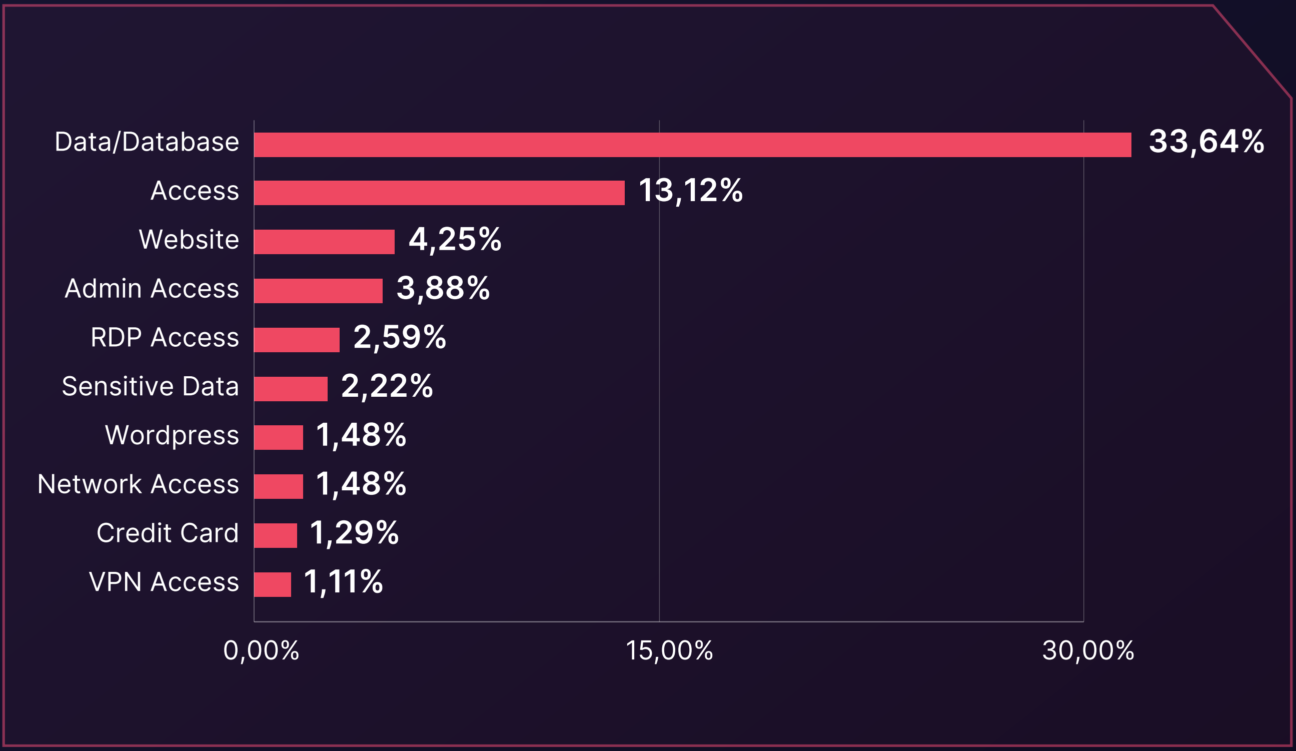
Industry Distribution of Dark Web Threats



Distribution of Dark Web Threats by Post Type

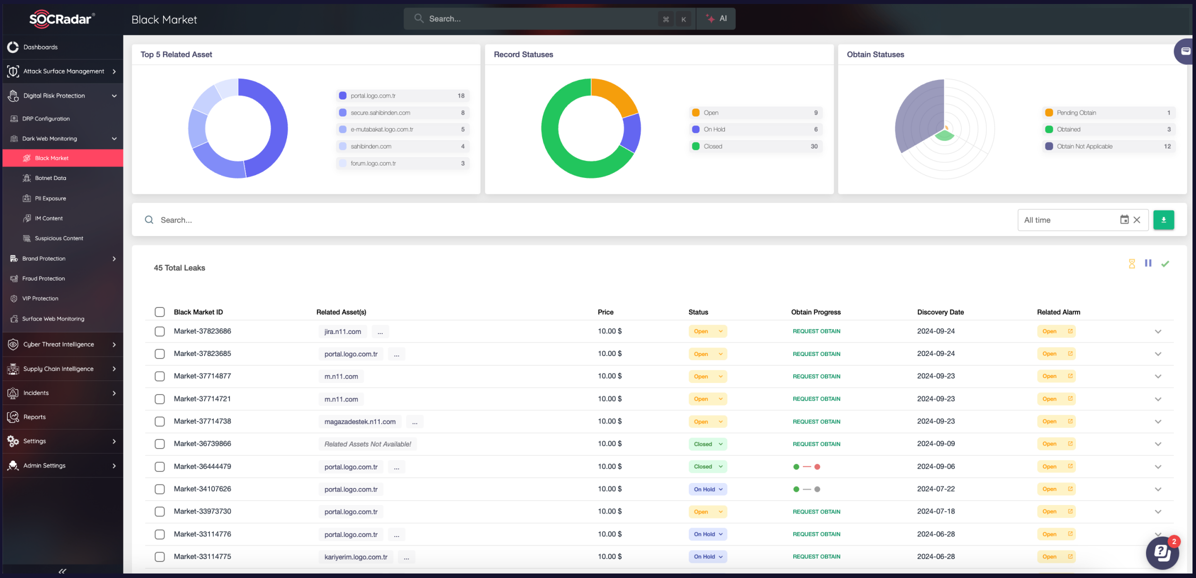


Distribution of Dark Web Threats by Threat Type



SOCRadar's Advanced Dark Web Monitoring provides Brazilian organizations with critical insights into hidden threats targeting their sectors, including Public Administration and Retail Trade, which have faced significant risks over the past year. With real-time tracking of underground chatter and sensitive data exposure, SOCRadar enables proactive defense against dark web threats.

Activate your free demo today to safeguard your organization’s most valuable assets.



45 Total Leaks

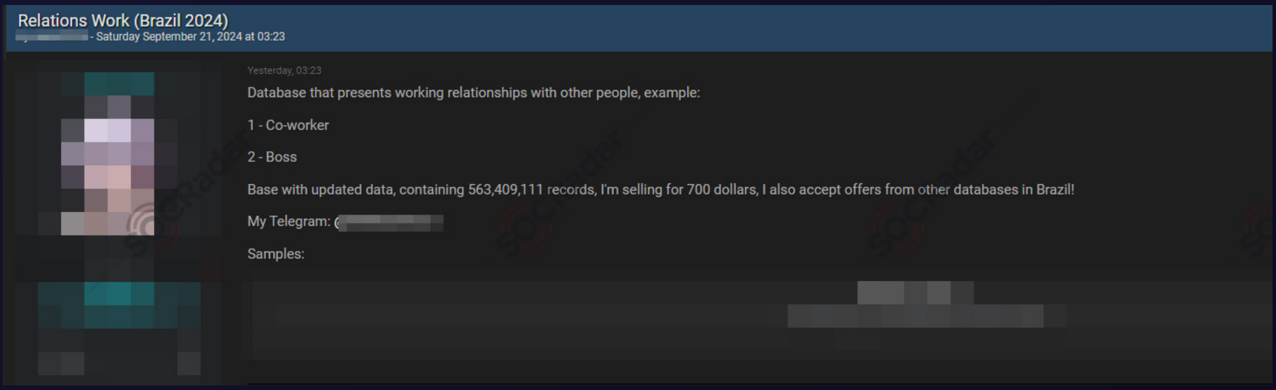
Black Market ID	Related Asset(s)	Price	Status	Obtain Progress	Discovery Date	Related Alarm
Market-37823686	jira.n11.com ...	10.00 $	Open	REQUEST OBTAIN	2024-09-24	Open
Market-37823685	portal.logo.com.tr ...	10.00 $	Open	REQUEST OBTAIN	2024-09-24	Open
Market-37714877	m.n11.com	10.00 $	Open	REQUEST OBTAIN	2024-09-23	Open
Market-37714721	m.n11.com	10.00 $	Open	REQUEST OBTAIN	2024-09-23	Open
Market-37714738	magazadestek.n11.com ...	10.00 $	Open	REQUEST OBTAIN	2024-09-23	Open
Market-36739866	*Related Assets Not Available!*	10.00 $	Closed	REQUEST OBTAIN	2024-09-09	Open
Market-36444479	portal.logo.com.tr ...	10.00 $	Closed	● — ●	2024-09-06	Open
Market-34107626	portal.logo.com.tr	10.00 $	On Hold	● — ●	2024-07-22	Open
Market-33973730	portal.logo.com.tr	10.00 $	Open	REQUEST OBTAIN	2024-07-18	Open
Market-33114776	portal.logo.com.tr ...	10.00 $	On Hold	REQUEST OBTAIN	2024-06-28	Open
Market-33114775	kariyerim.logo.com.tr ...	10.00 $	On Hold	REQUEST OBTAIN	2024-06-28	Open

Recent Dark Web Activities Targeting Brazilian Entities

21 Sep
2024

The Alleged Relations Work Data of Brazil is on Sale

A hacker forum monitored by SOCRadar detected a new alleged sale of relations work data for Brazil. The database reportedly includes 563,409,111 records and is being offered for sale on the forum.



Relations Work (Brazil 2024)
[redacted] - Saturday September 21, 2024 at 03:23

Yesterday, 03:23

Database that presents working relationships with other people, example:

1 - Co-worker

2 - Boss

Base with updated data, containing 563,409,111 records, I'm selling for 700 dollars, I also accept offers from other databases in Brazil!

My Telegram: [redacted]

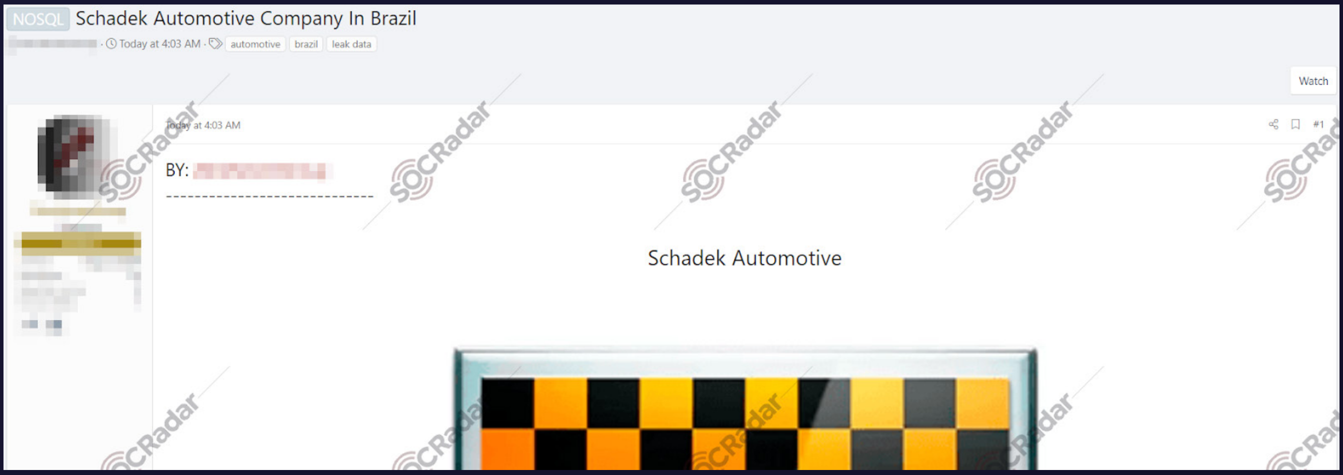
Samples:

Screenshot of the forum post - Relations Work (Brazil 2024)

22 Sep
2024

The Alleged Data of Schadek Automotive is Leaked

A new alleged data leak for Schadek Automotive was detected in a hacker forum monitored by SOCRadar. The leaked data includes sensitive information such as projects, employee details, customer data, financial information, and manufacturing designs.



NOSQL Schadek Automotive Company In Brazil

[redacted] · Today at 4:03 AM · automotive brazil leak data

Watch

Today at 4:03 AM

#1

BY: [redacted]

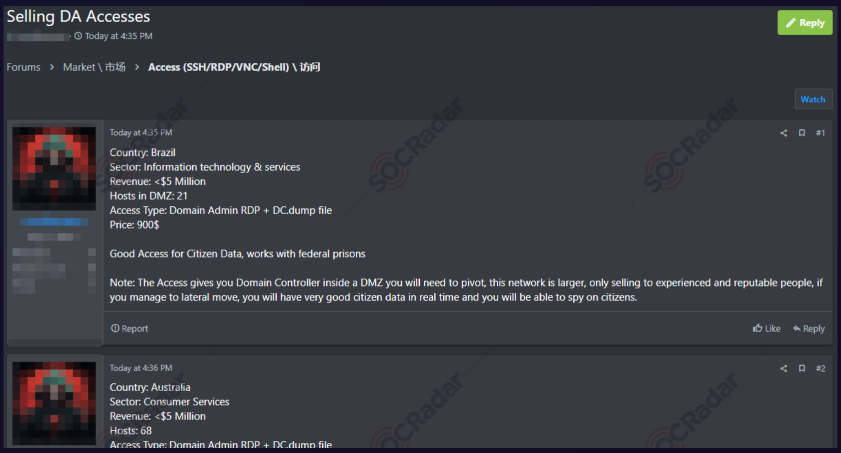
Schadek Automotive

Screenshot of the forum post - Schadek Automotive Company In Brazil

11 Sep
2024

The Alleged Unauthorized Domain Admin Access Sales are Detected for Many Companies

In a hacker forum monitored by SOCRadar, an unauthorized sale of domain admin access was detected. The access allegedly belongs to many companies operating in Brazil and Australia. It includes Domain Admin RDP and DC.dump files, providing potential attackers with privileged access to sensitive data and systems.



Selling DA Accesses

[redacted] · Today at 4:35 PM

Reply

Forums › Market \ 市场 › **Access (SSH/RDP/VNC/Shell) \ 访问**

Watch

Today at 4:35 PM

#1

Country: Brazil
Sector: Information technology & services
Revenue: <$5 Million
Hosts in DMZ: 21
Access Type: Domain Admin RDP + DC.dump file
Price: 900$

Good Access for Citizen Data, works with federal prisons

Note: The Access gives you Domain Controller inside a DMZ you will need to pivot, this network is larger, only selling to experienced and reputable people, if you manage to lateral move, you will have very good citizen data in real time and you will be able to spy on citizens.

Report

Like Reply

Today at 4:36 PM

#2

Country: Australia
Sector: Consumer Services
Revenue: <$5 Million
Hosts: 68
Access Type: Domain Admin RDP + DC.dump file

Screenshot of the forum post - Selling DA Accesses

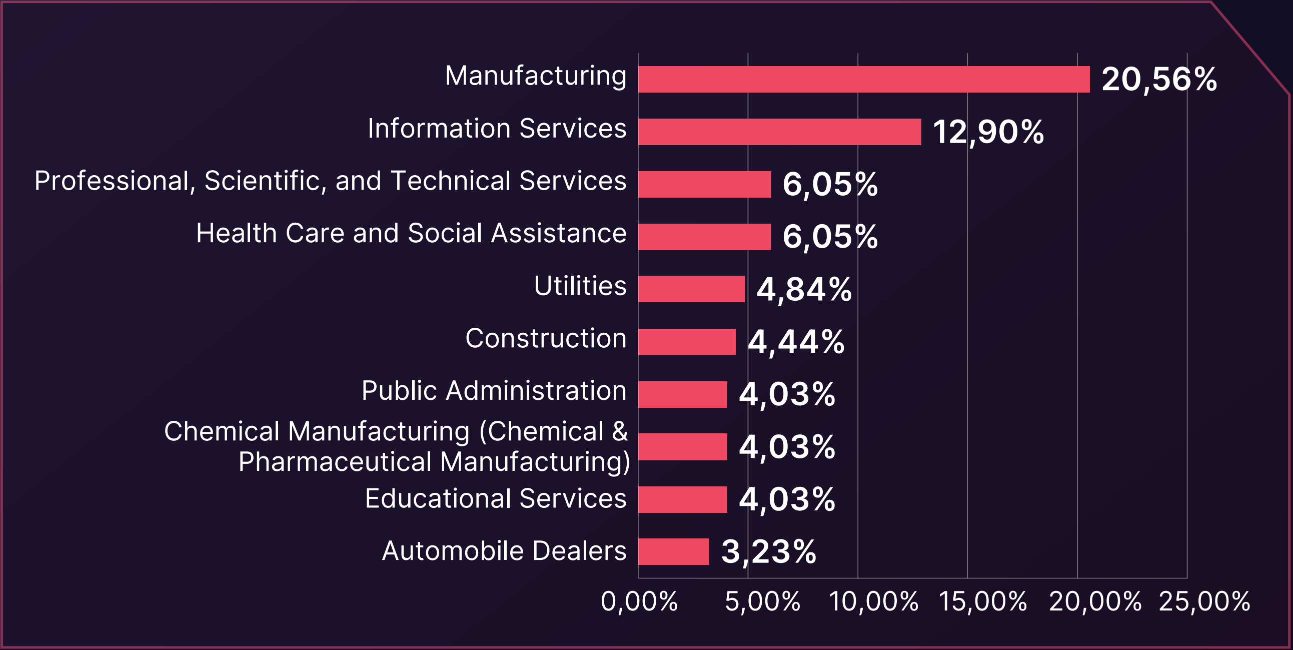
Ransomware Attacks Targeting Brazilian Entities

Ransomware attacks represent significant threats to organizations, often resulting in dire consequences such as extensive data loss and the exposure of sensitive information. SOCRadar's surveillance has identified 248 instances of ransomware victim notifications attributable to various ransomware threat actors and/or groups.

Of the 248 ransomware attacks referenced, Brazil emerges as the primary target in 166 cases, with the nation also featuring among the most affected countries in the remaining 82 global incidents.

Manufacturing emerges as the most prominently affected sector among the targeted industries, representing 20.56% of the identified ransomware attacks during this period. Following this, the Information Services industry accounted for 12.90% of the attacks, while the Professional, Scientific, and Technical Services industry experienced 6.05% of the ransomware incidents.

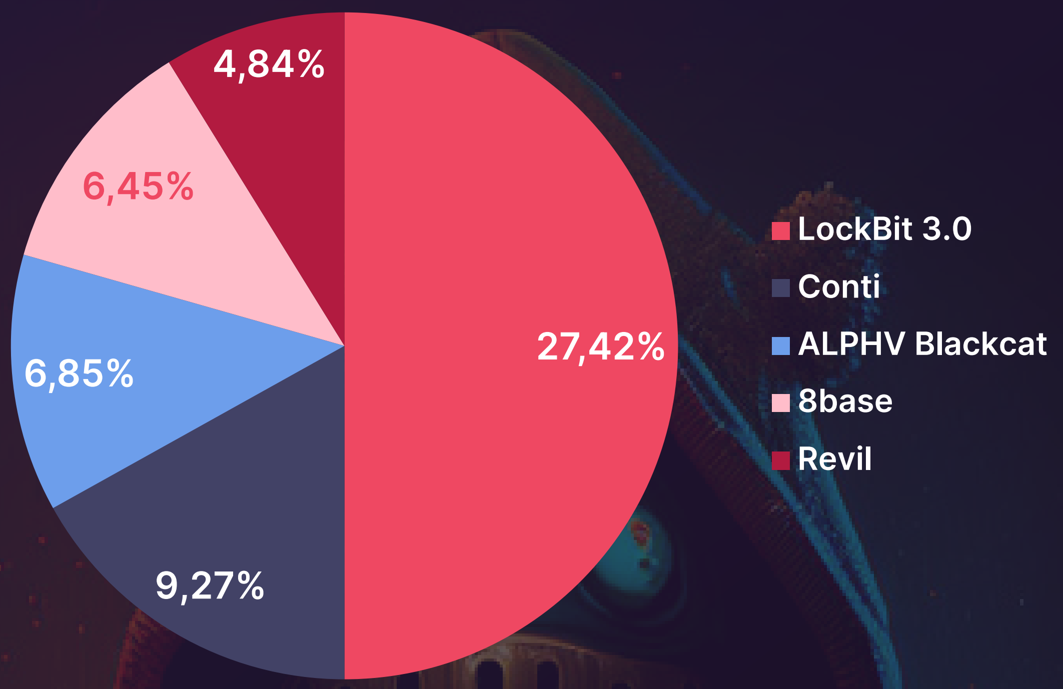
Distribution of Ransomware Attacks by Industry



Top Ransomware Groups Targeting Brazil

When examining the top ransomware groups targeting Brazil, **LockBit 3.0** emerges as the most prolific threat, accounting for **27.42%** of the attacks. Following this, **Conti** represents **9.27%** of the ransomware incidents. **ALPHV Blackcat** accounts for **6.85%**, while **8base** accounts for **6.45%**. Lastly, **Revil** contributes to **4.84%** of the ransomware activity in Brazil.
This analysis highlights the dominant presence of LockBit 3.0, followed by a diverse range of other ransomware groups.

Top Ransomware Groups Targeting Brazil

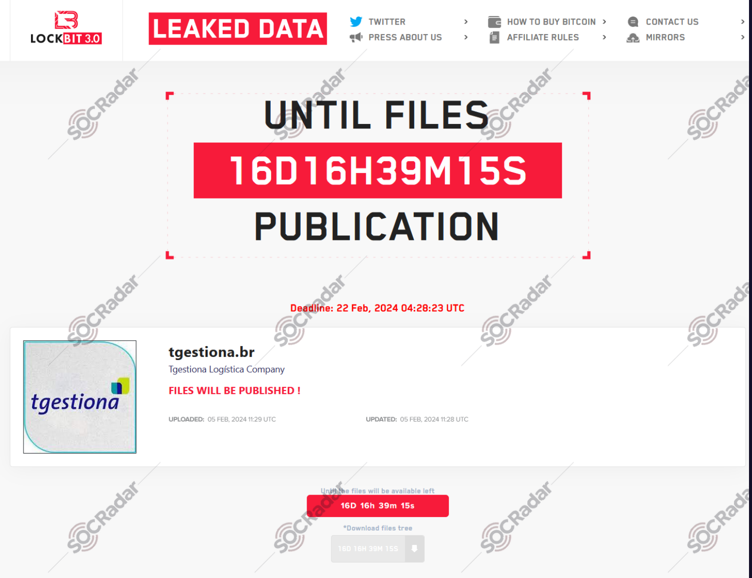


Recent Ransomware Attacks Targeting Brazilian Entities

05 Feb
2024

The New Ransomware Victim of LockBit 3.0: Tgestiona Logística

On the **LockBit 3.0 ransomware group** website monitored by SOCRadar, a new victim was allegedly announced as Tgestiona Logística. The group has already uploaded some of the company's files to its website and is threatening to publish the rest if the ransom is not paid by February 22, 2024, as the payment deadline draws near.



UNTIL FILES
16D16H39M15S
PUBLICATION

Deadline: 22 Feb, 2024 04:28:23 UTC

tgestiona.br
Tgestiona Logística Company
FILES WILL BE PUBLISHED !
UPLOADED: 05 FEB, 2024 11:29 UTC
UPDATED: 05 FEB, 2024 11:28 UTC

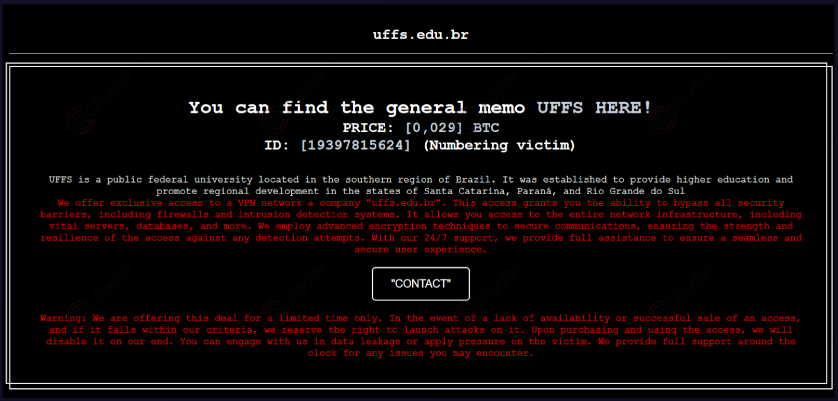
Until the files will be available left
16D 16h 39m 15s
*Download files tree
16D 16H 39M 15S

Screenshot from Lockbit 3.0 ransomware group's website

18 Jan
2024

The New Ransomware Victim of Stormous: UFFS

On the Stormous ransomware group website monitored by SOCRadar, a new ransomware victim was allegedly announced as UFFS / Federal University of Fronteira Sul. The group offers exclusive access to a VPN network that bypasses security barriers, providing access to the entire network infrastructure, including critical servers and databases. It employs advanced encryption techniques to secure communications and ensure access remains undetected.



uffs.edu.br

You can find the general memo UFFS HERE!
PRICE: [0,029] BTC
ID: [19397815624] (Numbering victim)

UFFS is a public federal university located in the southern region of Brazil. It was established to provide higher education and promote regional development in the states of Santa Catarina, Paraná, and Rio Grande do Sul
We offer exclusive access to a VPN network a company "uffs.edu.br". This access grants you the ability to bypass all security barriers, including firewalls and intrusion detection systems. It allows you access to the entire network infrastructure, including vital servers, databases, and more. We employ advanced encryption techniques to secure communications, ensuring the strength and resilience of the access against any detection attempts. With our 24/7 support, we provide full assistance to ensure a seamless and secure user experience.

"CONTACT"

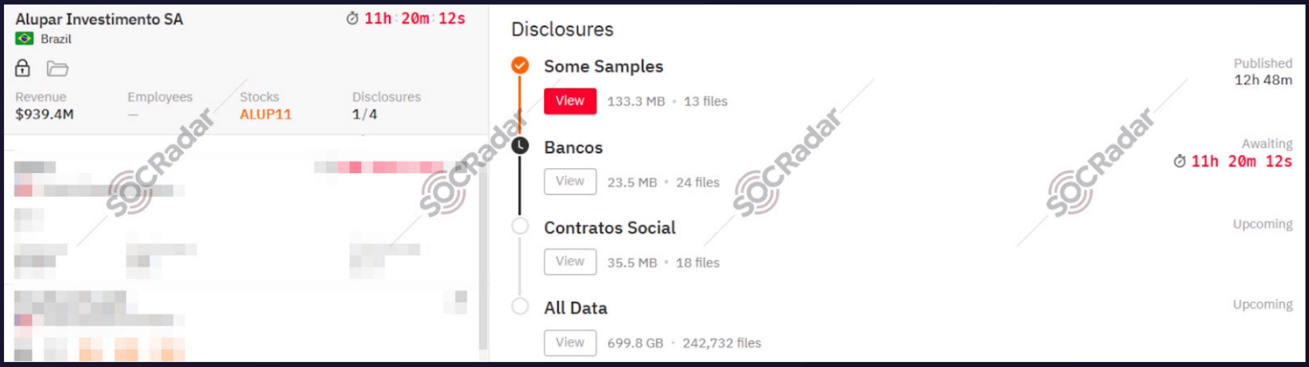
Warning: We are offering this deal for a limited time only. In the event of a lack of availability or successful sale of an access, and if it falls within our criteria, we reserve the right to launch attacks on it. Upon purchasing and using the access, we will disable it on our end. You can engage with us in data leakage or apply pressure on the victim. We provide full support around the clock for any issues you may encounter.

Screenshot from Stormous ransomware group's website

22 Jan
2024

Hunters International Ransomware Group Leaked The Data of Alupar Investimento

In the Hunters International ransomware group website monitored by SOCRadar, new data leaks detected allegedly belong to Alupar Investimento. The leaked data includes various files, such as bank details, contracts, and social information, totaling 699.8 GB.



Alupar Investimento SA
Brazil
11h 20m 12s

Revenue	Employees	Stocks	Disclosures
$939.4M	—	ALUP11	1/4

Disclosures

Some Samples
View 133.3 MB · 13 files
Published 12h 48m

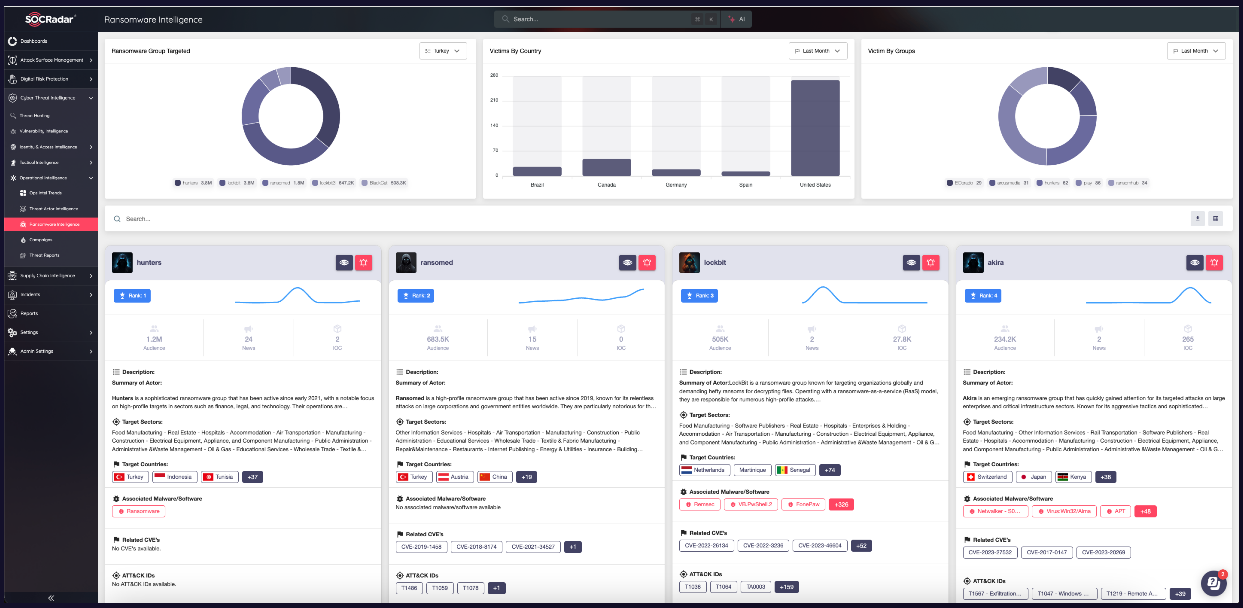
Bancos
View 23.5 MB · 24 files
Awaiting 11h 20m 12s

Contratos Social
View 35.5 MB · 18 files
Upcoming

All Data
View 699.8 GB · 242,732 files
Upcoming

Screenshot from Hunters International ransomware group's website

Explore **SOCRadar's Ransomware Intelligence** module and gain comprehensive insights with detailed group profiles, MITRE Visualizer, and actionable IOCs. These insights will empower you to stay ahead of evolving threats and enhance your cybersecurity strategy.



hunters
Rank: 1
1.2M Audience · 24 News · 2 IOC

Description:
Summary of Actor:
Hunters is a sophisticated ransomware group that has been active since early 2021, with a notable focus on high-profile targets in sectors such as finance, legal, and technology. Their operations are...

Target Sectors:
Food Manufacturing - Real Estate - Hospitals - Accommodation - Air Transportation - Manufacturing - Construction - Electrical Equipment, Appliance, and Component Manufacturing - Public Administration - Administrative &Waste Management - Oil & Gas - Educational Services - Wholesale Trade - Textile &...

Target Countries:
Turkey · Indonesia · Tunisia · +37

Associated Malware/Software
Ransomware

Related CVE's
No CVE's available.

ATT&CK IDs
No ATT&CK IDs available.

ransomed
Rank: 2
683.5K Audience · 15 News · 0 IOC

Description:
Summary of Actor:
Ransomed is a high-profile ransomware group that has been active since 2019, known for its relentless attacks on large corporations and government entities worldwide. They are particularly notorious for th...

Target Sectors:
Other Information Services - Hospitals - Air Transportation - Manufacturing - Construction - Public Administration - Educational Services - Wholesale Trade - Textile & Fabric Manufacturing - Repair&Maintenance - Restaurants - Internet Publishing - Energy & Utilities - Insurance - Building...

Target Countries:
Turkey · Austria · China · +19

Associated Malware/Software
No associated malware/software available

Related CVE's
CVE-2019-1458 · CVE-2018-8174 · CVE-2021-34527 · +1

ATT&CK IDs
T1486 · T1059 · T1078 · +1

lockbit
Rank: 3
505K Audience · 2 News · 27.8K IOC

Description:
Summary of Actor: LockBit is a ransomware group known for targeting organizations globally and demanding hefty ransoms for decrypting files. Operating with a ransomware-as-a-service (RaaS) model, they are responsible for numerous high-profile attacks....

Target Sectors:
Food Manufacturing - Software Publishers - Real Estate - Hospitals - Enterprises & Holding - Accommodation - Air Transportation - Manufacturing - Construction - Electrical Equipment, Appliance, and Component Manufacturing - Public Administration - Administrative &Waste Management - Oil & G...

Target Countries:
Netherlands · Martinique · Senegal · +74

Associated Malware/Software
Remsec · VB.PwShell.2 · FonePaw · +326

Related CVE's
CVE-2022-26134 · CVE-2022-3236 · CVE-2023-46604 · +52

ATT&CK IDs
T1038 · T1064 · TA0003 · +159

akira
Rank: 4
234.2K Audience · 2 News · 265 IOC

Description:
Summary of Actor:
Akira is an emerging ransomware group that has quickly gained attention for its targeted attacks on large enterprises and critical infrastructure sectors. Known for its aggressive tactics and sophisticated...

Target Sectors:
Food Manufacturing - Other Information Services - Rail Transportation - Software Publishers - Real Estate - Hospitals - Accommodation - Manufacturing - Construction - Electrical Equipment, Appliance, and Component Manufacturing - Public Administration - Administrative &Waste Management - Oil & G...

Target Countries:
Switzerland · Japan · Kenya · +38

Associated Malware/Software
Netwalker - S0... · Virus:Win32/Alma · APT · +48

Related CVE's
CVE-2023-27532 · CVE-2017-0147 · CVE-2023-20269

ATT&CK IDs
T1567 - Exfiltration... · T1047 - Windows ... · T1219 - Remote A... · +39

Top Threat Actors Targeting Brazilian Organizations

Lockbit 3.0 Ransomware Group

Country of Origin: Russia

The most successful RaaS group operating since 2019. The group is continuously evolving and is highly active in deploying models such as double-extortion and initial access broker affiliates.

-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, 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.

You can visit our blog post for more detailed Lockbit 3.0 Ransomware Group information.

Conti Ransomware Group

Conti is one of the most notorious ransomware groups responsible for hundreds of attacks globally. The group operates as a Ransomware-as-a-Service (RaaS), which allows affiliates to use Conti's ransomware in exchange for a share of the profits. Conti is known for its highly sophisticated attacks, which leverage double extortion techniques—encrypting data and threatening to leak sensitive information if the ransom is not paid.

The Conti group was also linked to several high-profile attacks, including incidents targeting critical infrastructure and healthcare organizations. Their aggressive tactics and willingness to target essential services have made them one of the most disruptive ransomware groups in recent years.

You can visit our blog post for more detailed information about the Conti Ransomware Group.

ALPHV Blackcat Ransomware Group

BlackCat Ransomware

Country of Origin: Russia

BlackCat, or ALPHV, is a ransomware group known for being the pioneer to use Rust and the group first announced its RaaS affiliate program in a dark web forum in December 2021.

-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

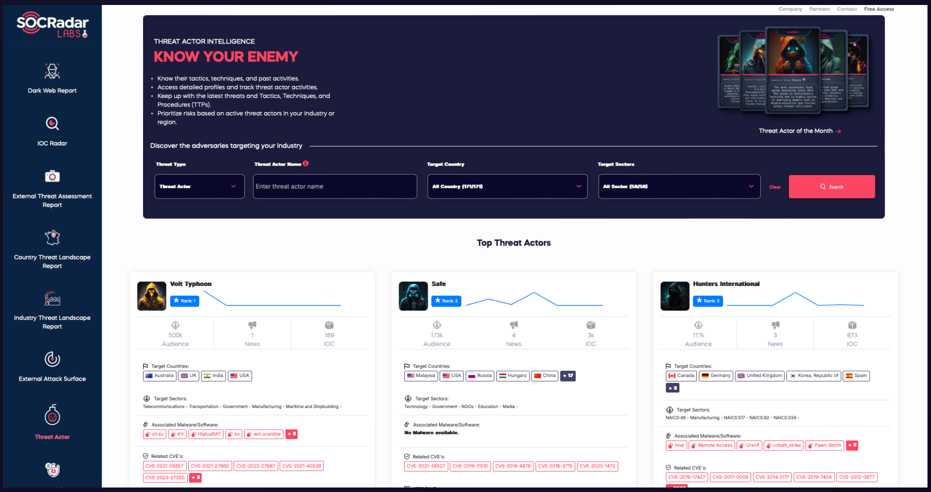
-TTPs-

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 successfully use Rust—a cross-platform programming language that allows for easy malware customization for different operating systems, such as Windows and Linux. 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 not designed to analyze malware written in Rust.

You can visit our blog post for more detailed information about the ALPHV BlackCat Ransomware Group.

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.



THREAT ACTOR INTELLIGENCE

KNOW YOUR ENEMY

- Know their tactics, techniques, and past activities.
- Access detailed profiles and track threat actor activities.
- Keep up with the latest threats and Tactics, Techniques, and Procedures (TTPs).
- Prioritize risks based on active threat actors in your industry or region.

Discover the adversaries targeting your industry

Top Threat Actors

Volt Typhoon
Rank: 1
500k Audience | 1 News | 189 IOC
Target Countries: Australia, UK, India, USA
Target Sectors: Telecommunications - Transportation - Government - Manufacturing - Maritime and Shipbuilding -
Associated Malware/Software: sh.kv, KV, HiatusRAT, kv, win.scanline, +3
Related CVE's: CVE-2021-26857, CVE-2021-27860, CVE-2022-27997, CVE-2021-40539, CVE-2023-27350, +3

Safe
Rank: 2
173k Audience | 4 News | 3k IOC
Target Countries: Malaysia, USA, Russia, Hungary, China, + 17
Target Sectors: Technology - Government - NGOs - Education - Media -
Associated Malware/Software: No Malware available.
Related CVE's: CVE-2021-34527, CVE-2019-11510, CVE-2018-4878, CVE-2016-3715, CVE-2020-1472

Hunters International
Rank: 3
117k Audience | 3 News | 673 IOC
Target Countries: Canada, Germany, United Kingdom, Korea, Republic of, Spain, + 3
Target Sectors: NAICS:48 - Manufacturing - NAICS:517 - NAICS:92 - NAICS:334 -
Associated Malware/Software: hive, Remote Access, Ursnif, cobalt_strike, Pawn Storm, + 2
Related CVE's: CVE-2019-17427, CVE-2017-0009, CVE-2014-2117, CVE-2019-7404, CVE-2012-0877

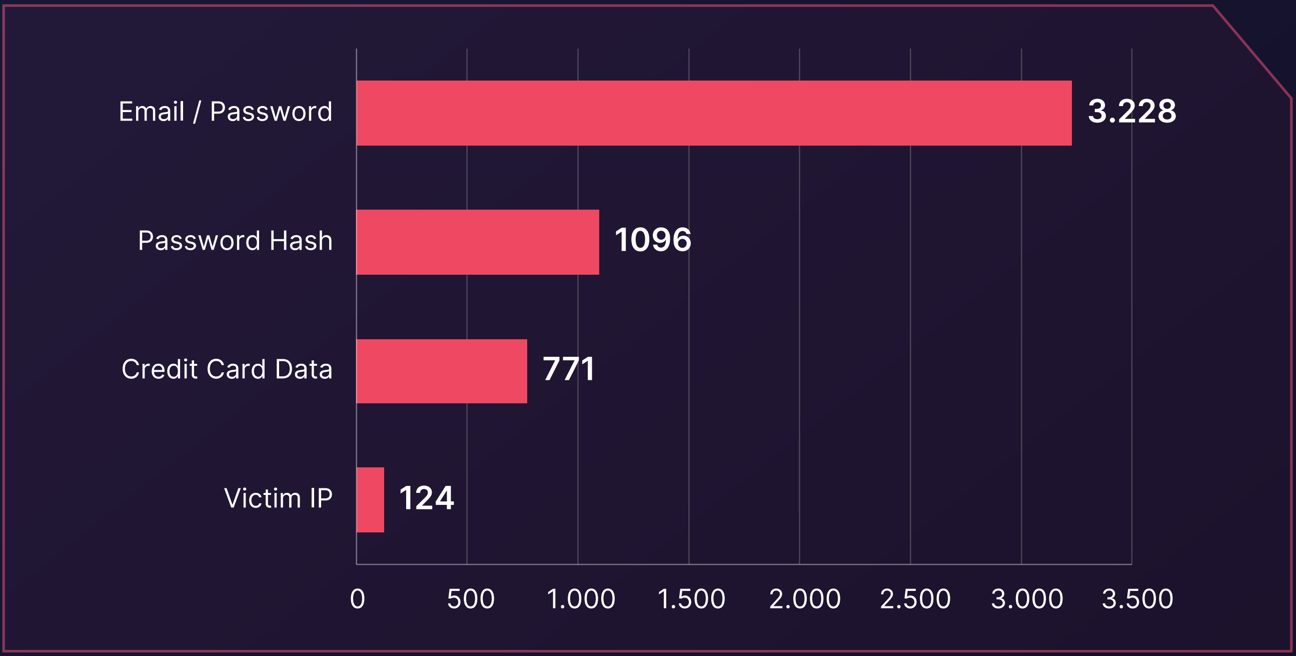
Stealer Log Statistics: Top Domains in Brazil

Throughout 2024, thousands of users' user IDs/email addresses, passwords, credit card data, password hashes, and victim IP address information were compromised via Stealer Logs from the computers of users with accounts or access to some of the highest traffic domains in Brazil.

The table below lists the domains that receive the highest traffic from Brazil.

uol.com.br
globo.com
tudocelular.com
gov.br
mercadolivre.com.br
terra.com.br
caixa.gov.br
metropoles.com
acesso.gov.br
cnnbrasil.com.br

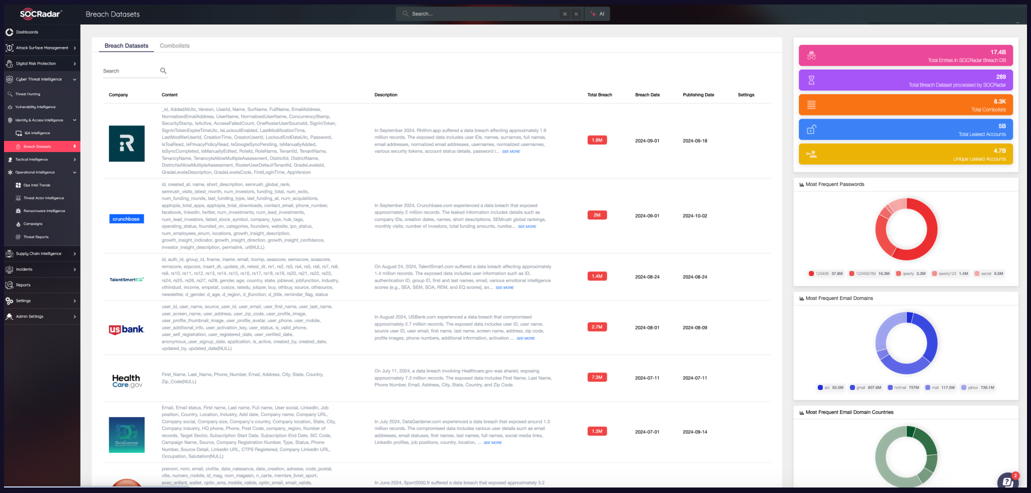
Stealer Logs- Compromise Data



The data reveals significant dissemination of compromised information, including **3,228** email/password combinations, **1,096** password hashes, **771** credit card data entries, and **124** compromised victim IPs, each representing significant instances of compromise.

These discoveries emphasize the gravity of data compromises that impact users, highlighting the urgent need for robust cybersecurity protocols to mitigate such risks efficiently.

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.



Company	Content	Description	Total Breach	Breach Date	Publishing Date	Settings
R	_id, AddedAtUtc, Version, UserId, Name, SurName, FullName, EmailAddress, NormalizedEmailAddress, UserName, NormalizedUserName, ConcurrencyStamp, SecurityStamp, IsActive, AccessFailedCount, OneRosterUserSourceId, SignInToken, SignInTokenExpireTimeUtc, IsLockoutEnabled, LastModificationTime, LastModifierUserId, CreationTime, CreatorUserId, LockoutEndDateUtc, Password, IsToaRead, IsPrivacyPolicyRead, IsGoogleSyncPending, IsManuallyAdded, IsSyncCompleted, IsManuallyEdited, RoleId, RoleName, TenantId, TenantName, TenancyName, TenancyIsAllowMultipleAssessment, DistrictId, DistrictName, DistrictIsAllowMultipleAssessment, RosterUserDefaultTenantId, GradeLevelsId, GradeLevelsDescription, GradeLevelsCode, FirstLoginTime, AppVersion	In September 2024, Rhithm.app suffered a data breach affecting approximately 1.9 million records. The exposed data includes user IDs, names, surnames, full names, email addresses, normalized email addresses, usernames, normalized usernames, various security tokens, account status details, password i... SEE MORE	1.9M	2024-09-01	2024-09-18	
crunchbase	id, created_at, name, short_description, semrush_global_rank, semrush_visits_latest_month, num_investors, funding_total, num_exits, num_funding_rounds, last_funding_type, last_funding_at, num_acquisitions, apptopia_total_apps, apptopia_total_downloads, contact_email, phone_number, facebook, linkedin, twitter, num_investments, num_lead_investments, num_lead_investors, listed_stock_symbol, company_type, hub_tags, operating_status, founded_on, categories, founders, website, ipo_status, num_employees_enum, locations, growth_insight_description, growth_insight_indicator, growth_insight_direction, growth_insight_confidence, investor_insight_description, permalink, url(NULL)	In September 2024, Crunchbase.com experienced a data breach that exposed approximately 2 million records. The leaked information includes details such as company IDs, creation dates, names, short descriptions, SEMrush global rankings, monthly visits, number of investors, total funding amounts, numbe... SEE MORE	2M	2024-09-01	2024-10-02	
TalentSmartEQ	id, auth_id, group_id, fname, lname, email, tcomp, seascore, semscore, soascore, remscore, eqscore, insert_dt, update_dt, retest_dt, rs1, rs2, rs3, rs4, rs5, rs6, rs7, rs8, rs9, rs10, rs11, rs12, rs13, rs14, rs15, rs16, rs17, rs18, rs19, rs20, rs21, rs22, rs23, rs24, rs25, rs26, rs27, rs28, gender, age, country, state, joblevel, jobfunction, industry, othindust, income, empstat, cosize, ratedu, jobper, buy, othbuy, source, othsource, newsletter, d_gender, d_age, d_region, d_jfunction, d_jtitle, reminder_flag, status	On August 24, 2024, TalentSmart.com suffered a data breach affecting approximately 1.4 million records. The exposed data includes user information such as ID, authentication ID, group ID, first and last names, email, various emotional intelligence scores (e.g., SEA, SEM, SOA, REM, and EQ scores), an... SEE MORE	1.4M	2024-08-24	2024-08-24	
usbank	user_id, user_name, source_user_id, user_email, user_first_name, user_last_name, user_screen_name, user_address, user_zip_code, user_profile_image, user_profile_thumbnail_image, user_profile_avatar, user_phone, user_mobile, user_additional_info, user_activation_key, user_status, is_valid_phone, user_self_registration, user_registered_date, user_verified_date, anonymous_user_signup_date, application, is_active, created_by, created_date, updated_by, updated_date(NULL)	In August 2024, USBank.com experienced a data breach that compromised approximately 2.7 million records. The exposed data includes user ID, user name, source user ID, user email, first name, last name, screen name, address, zip code, profile images, phone numbers, additional information, activation ... SEE MORE	2.7M	2024-08-01	2024-08-09	
Health Care.gov	First_Name, Last_Name, Phone_Number, Email, Address, City, State, Country, Zip_Code(NULL)	On July 11, 2024, a data breach involving Healthcare.gov was shared, exposing approximately 7.3 million records. The exposed data includes First Name, Last Name, Phone Number, Email, Address, City, State, Country, and Zip Code.	7.3M	2024-07-11	2024-07-11	
DataGardener	Email, Email status, First name, Last name, Full name, User social, LinkedIn, Job position, Country, Location, Industry, Add date, Company name, Company URL, Company social, Company size, Company's country, Company location, State, City, Company industry, HQ phone, Phone, Post Code, company_region, Number of records, Target Sector, Subscription Start Date, Subscription End Date, SIC Code, Campaign Name, Source, Company Registration Number, Type, Status, Phone Number, Source Detail, LinkedIn URL, CTPS Registered, Company LinkedIn URL, Occupation, Salutation(NULL)	In July 2024, DataGardener.com experienced a data breach that exposed around 1.3 million records. The compromised data includes various user details such as email addresses, email statuses, first names, last names, full names, social media links, LinkedIn profiles, job positions, country, location, ... SEE MORE	1.3M	2024-07-01	2024-09-14	
	prenom, nom, email, civilite, date_naissance, date_creation, adresse, code_postal, ville, numero_mobile, id_mag, nom_magasin, n_carte, membre_livret_sport, avec_enfant, wallet, optin_sms, mobile_valide, optin_email, email_valide,	In June 2024, Sport2000.fr suffered a data breach that exposed approximately 3.2				

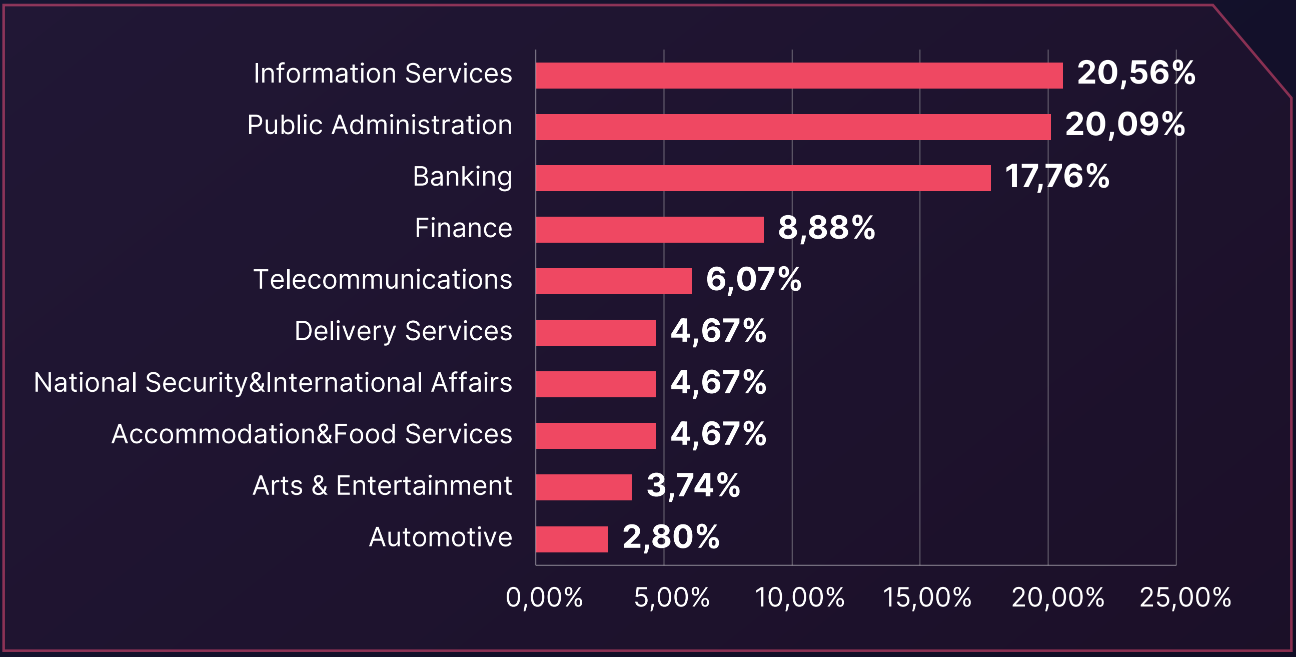
17.4B	Total Entries In SOCRadar Breach DB
289	Total Breach Dataset processed by SOCRadar
8.3K	Total Combolists
5B	Total Leaked Accounts
4.7B	Unique Leaked Accounts

Phishing Threats Targeting Brazil

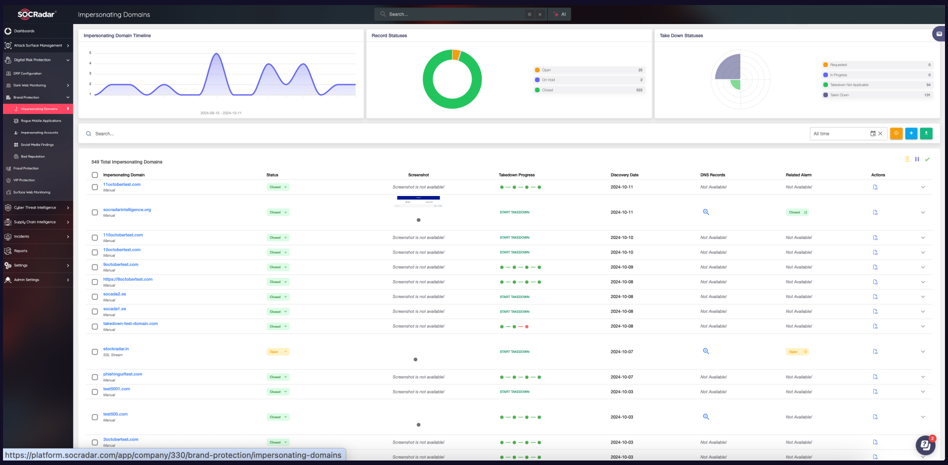
Phishing is an effective method to initially breach an organization's infrastructure by deceiving individuals into divulging sensitive credentials on fraudulent websites.

Typically, phishing attacks are coupled with social engineering tactics to acquire such credentials. Over the past year, Brazilian enterprises have encountered ***1,449 distinct instances of phishing attacks***, primarily targeting the ***Information Services*** industry.

Phishing Attacks - Distribution by Industry



With SOCRadar's AI-powered Phishing Domain Detection module, you can swiftly identify malicious domains and protect your brand from phishing threats. **Start safeguarding your digital presence today with SOCRadar— request a free demo and see the platform in action.**



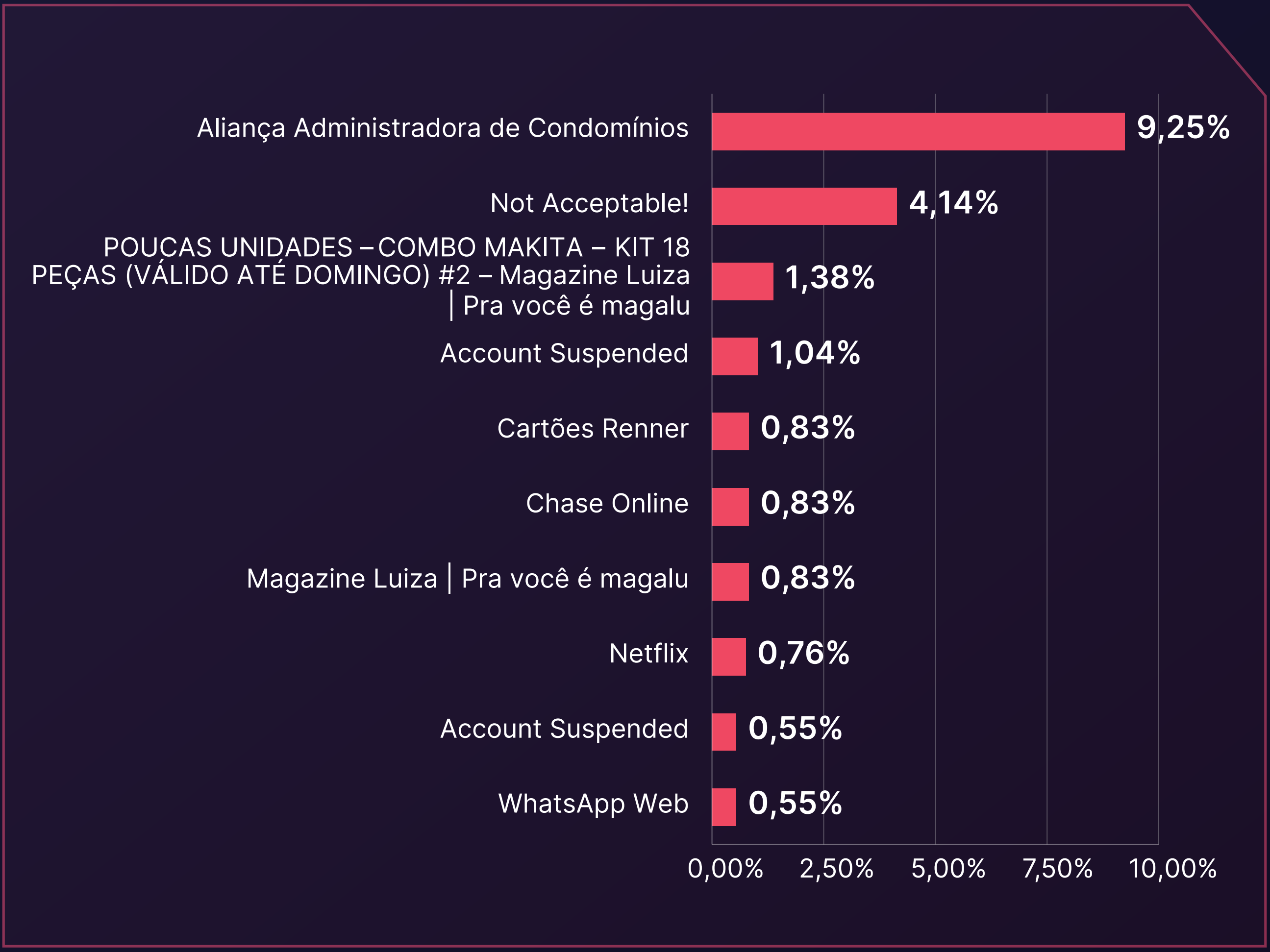
549 Total Impersonating Domains

□	Impersonating Domain	Status	Screenshot	Takedown Progress	Discovery Date	DNS Records	Related Alarm	Actions
□	11octobertest.com Manual	Closed	Screenshot is not available!	●—●—●—●	2024-10-11	Not Available!	Not Available!	
□	socradarintelligence.org Manual	Closed		START TAKEDOWN	2024-10-11	🔍	Closed	
□	110octobertest.com Manual	Closed	Screenshot is not available!	START TAKEDOWN	2024-10-10	Not Available!	Not Available!	
□	10octobertest.com Manual	Closed	Screenshot is not available!	START TAKEDOWN	2024-10-10	Not Available!	Not Available!	
□	9octobertest.com Manual	Closed	Screenshot is not available!	●—●—●—●	2024-10-09	Not Available!	Not Available!	
□	https://8octobertest.com Manual	Closed	Screenshot is not available!	●—●—●—●	2024-10-08	Not Available!	Not Available!	
□	socada2.es Manual	Closed	Screenshot is not available!	START TAKEDOWN	2024-10-08	Not Available!	Not Available!	
□	socada1.es Manual	Closed	Screenshot is not available!	START TAKEDOWN	2024-10-08	Not Available!	Not Available!	
□	takedown-test-domain.com Manual	Closed	Screenshot is not available!	●—●—●	2024-10-08	Not Available!	Not Available!	
□	stockradar.in SSL Stream	Open		START TAKEDOWN	2024-10-07	🔍	Open	
□	phishingurltest.com Manual	Closed	Screenshot is not available!	●—●—●—●	2024-10-07	Not Available!	Not Available!	
□	test5001.com Manual	Closed	Screenshot is not available!	START TAKEDOWN	2024-10-03	Not Available!	Not Available!	
□	test500.com Manual	Closed		●—●—●—●	2024-10-03	🔍	Not Available!	
□	3octobertest.com Manual	Closed	Screenshot is not available!	●—●—●—●	2024-10-03	Not Available!	Not Available!	
			Screenshot is not available!	●—●—●—●	2024-10-03	Not Available!	Not Available!	

https://platform.socradar.com/app/company/330/brand-protection/impersonating-domains

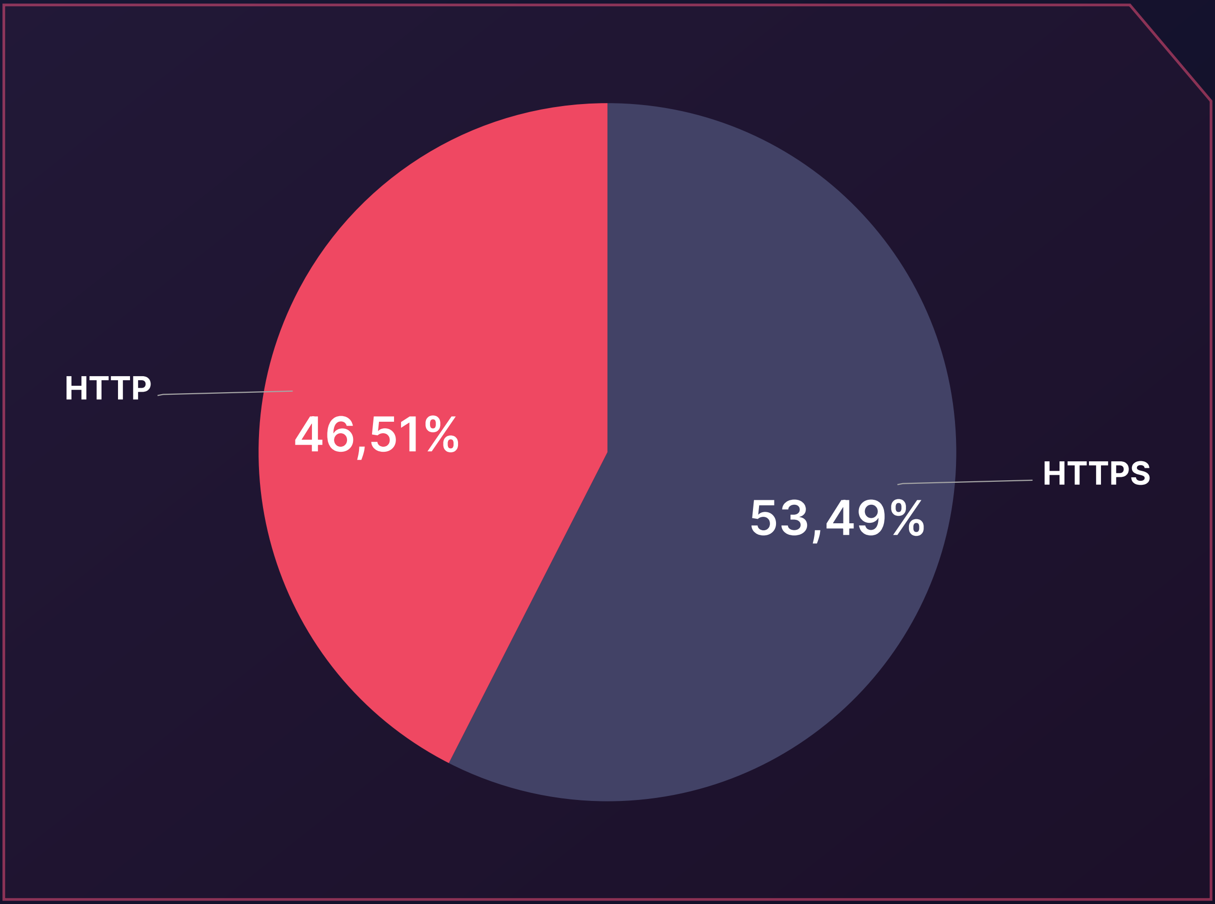
The graph below illustrates the distribution of Page Titles used by threat actors for phishing attacks. Notably, the data reveals a predominant usage of the ***Aliança Administradora de Condomínios*** page title.

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



DDoS Attack Statistics

Brazil experienced a dynamic DDoS threat landscape marked by considerable cyber activity in 2024.

- The most extensive multivector DDoS attack recorded encompassed **23 vectors**, featuring prevalent techniques such as **DNS Amplification and ICMP attacks**.
- The maximum bandwidth observed during a DDoS attack reached **4 Tbps** (peak aggregate bandwidth in one minute), indicating the severe capacity of these cyber threats.
- The highest recorded throughput during these incidents was **350.00 Mpps** (peak aggregate throughput in one minute), underscoring the intense rate at which data packets were sent.
- On average, each DDoS attack lasted for **51.85 minutes**, indicating a strategy aimed at prolonged and effective service disruption.
- **372,825 DDoS attacks** were recorded throughout the year, illustrating a high frequency of cyber-attacks aimed at targets in Brazil.

Attack Vector	Number of Attacks in 2023
TCP ACK	134,878
DNS Amplification	96,660
TCP SYN/ACK	83,769
TCP Reset	74,236
ICMP	65,442

The ongoing evolution of DDoS tactics underscores the importance of implementing stringent monitoring and resilient defense mechanisms to safeguard essential infrastructures and ensure uninterrupted service delivery.

Enhance your DDoS defense with SOCRadar's DoS Resilience Free Tool, a sophisticated tool designed to assess and fortify your infrastructure's resilience to DoS attacks.

Lessons Learned: Key Insights and Strategic Recommendations

Upon examining the cybersecurity threats facing organizations in Brazil, several critical lessons and recommendations have emerged. These insights, enhanced by SOCRadar's capabilities, provide a strategic roadmap to bolster cyber resilience and safeguard operational integrity. Here are the key takeaways from our analysis:

Vigilance in an Evolving Cyber Threat Landscape

The dynamic nature of the cyber threat landscape, marked by an increase in Dark Web activities and ransomware incidents related to Brazil, demands constant vigilance.

Organizations must keep pace with these changes by adapting their security strategies. By adopting a proactive approach like **SOCRadar’s Extended Threat Intelligence solution**, organizations can gain real-time insights into emerging threats, positioning them to counteract cyber adversaries proactively.

Implementation of Multi-layered Security Measures

Given the broad spectrum of industries targeted by cyber threats, it is essential to implement multi-layered security defenses. SOCRadar supports these efforts with its proactive **Threat Intelligence** and **Advanced Dark Web Monitoring** services, ensuring comprehensive protection.

Consistent Guard Against Ransomware

The persistent ransomware threat underscores the need for defensive, solid, and responsive strategies. **SOCRadar’s Attack Surface Management** capabilities are crucial for businesses to identify potential ransomware threats and to formulate effective countermeasures.

Continuous Employee Education and Training

The ongoing risk of phishing attacks makes continuous employee education and training imperative. Enhancing their ability to recognize phishing tactics and detection methods is vital.

SOCRadar's Digital Risk Protection suite provides comprehensive **VIP Protection** and **Brand Protection** services, effectively addressing the challenges posed by identity-based attacks.

Robust Defenses Against Stealer Malware

Brazil is frequently targeted by Stealer malware, so strengthening defenses against this malicious software is crucial.

SOCRadar’s Identity & Access Intelligence module is vital in detecting and mitigating data breach threats, enhancing an organization’s security framework.

Strategies Against DDoS Attacks

As DDoS attacks become more complex and voluminous, organizations must prioritize implementing robust DDoS mitigation strategies. This involves deploying advanced DDoS protection technologies that absorb high-volume traffic and effectively mitigate multi-vector attack strategies.

Enhance your DDoS defense with SOCRadar's DoS Resilience Free Tool, a sophisticated tool designed to assess and fortify your infrastructure's resilience to DoS attacks. Leveraging state-of-the-art AI and cloud technologies, this module provides a crucial layer of protection for global organizations.

SOCRadar’s Recommendations: Proactive Strategies for Threat Detection, Dark Web Monitoring, and Brand Protection

- Adopting a proactive and comprehensive cybersecurity approach is crucial for Brazil's organizations.
- Partnering with advanced solutions like SOCRadar enhances defenses and helps navigate the evolving cyber threat landscape.
- Building a culture of risk awareness and implementing proactive mitigation strategies fortifies defenses against dynamic threats.
- Utilizing Cyber Threat Intelligence (CTI) empowers teams to respond to immediate threats and confidently prepare for future challenges.
- Collaboration among cybersecurity professionals, supported by robust CTI frameworks, is essential for safeguarding digital assets and maintaining organizational resilience against cyber 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.

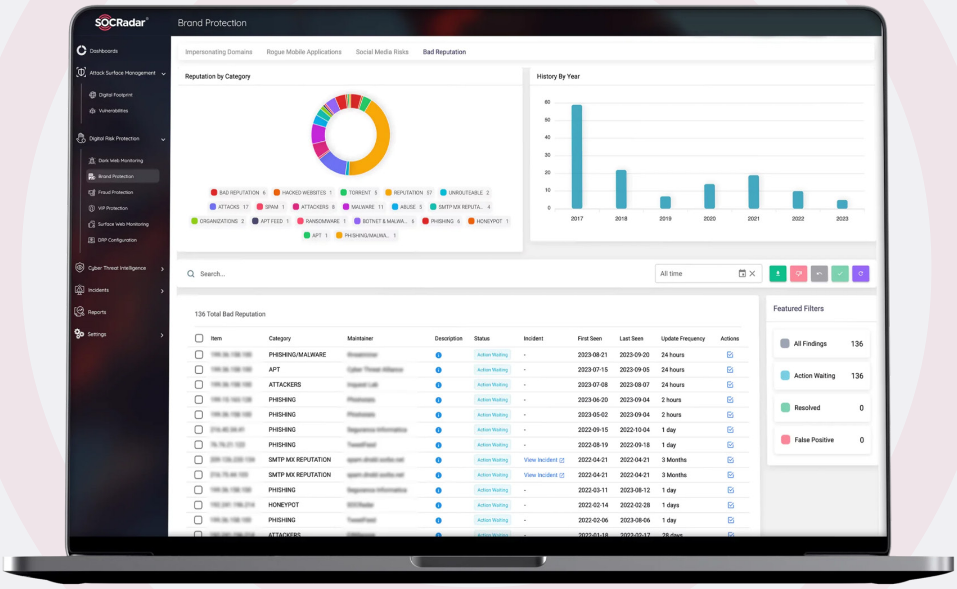
Credit Card Monitoring: Enhance your fraud detection mechanisms with automation speed by identifying stolen credit card data on popular global black markets, carding forums, social channels, and chatters.

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 PERSONALIZED DEMO

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.



136 Total Bad Reputation

☐	Item	Category	Maintainer	Description	Status	Incident	First Seen	Last Seen	Update Frequency	Actions
☐	[redacted]	PHISHING/MALWARE	[redacted]	ℹ	Action Waiting	-	2023-08-21	2023-09-20	24 hours	☑
☐	[redacted]	APT	[redacted]	ℹ	Action Waiting	-	2023-07-15	2023-09-05	24 hours	☑
☐	[redacted]	ATTACKERS	[redacted]	ℹ	Action Waiting	-	2023-07-08	2023-08-07	24 hours	☑
☐	[redacted]	PHISHING	[redacted]	ℹ	Action Waiting	-	2023-06-20	2023-09-04	2 hours	☑
☐	[redacted]	PHISHING	[redacted]	ℹ	Action Waiting	-	2023-05-02	2023-09-04	2 hours	☑
☐	[redacted]	PHISHING	[redacted]	ℹ	Action Waiting	-	2022-09-15	2022-10-04	1 day	☑
☐	[redacted]	PHISHING	[redacted]	ℹ	Action Waiting	-	2022-08-19	2022-09-18	1 day	☑
☐	[redacted]	SMTP MX REPUTATION	[redacted]	ℹ	Action Waiting	View Incident	2022-04-21	2022-04-21	3 Months	☑
☐	[redacted]	SMTP MX REPUTATION	[redacted]	ℹ	Action Waiting	View Incident	2022-04-21	2022-04-21	3 Months	☑
☐	[redacted]	PHISHING	[redacted]	ℹ	Action Waiting	-	2022-03-11	2023-08-12	1 day	☑
☐	[redacted]	HONEYPOT	[redacted]	ℹ	Action Waiting	-	2022-02-14	2022-02-28	1 days	☑
☐	[redacted]	PHISHING	[redacted]	ℹ	Action Waiting	-	2022-02-06	2023-08-06	1 day	☑
☐	[redacted]	ATTACKERS	[redacted]	ℹ	Action Waiting	-	2022-01-18	2022-02-17	28 days	☑

Featured Filters	
All Findings	136
Action Waiting	136
Resolved	0
False Positive	0