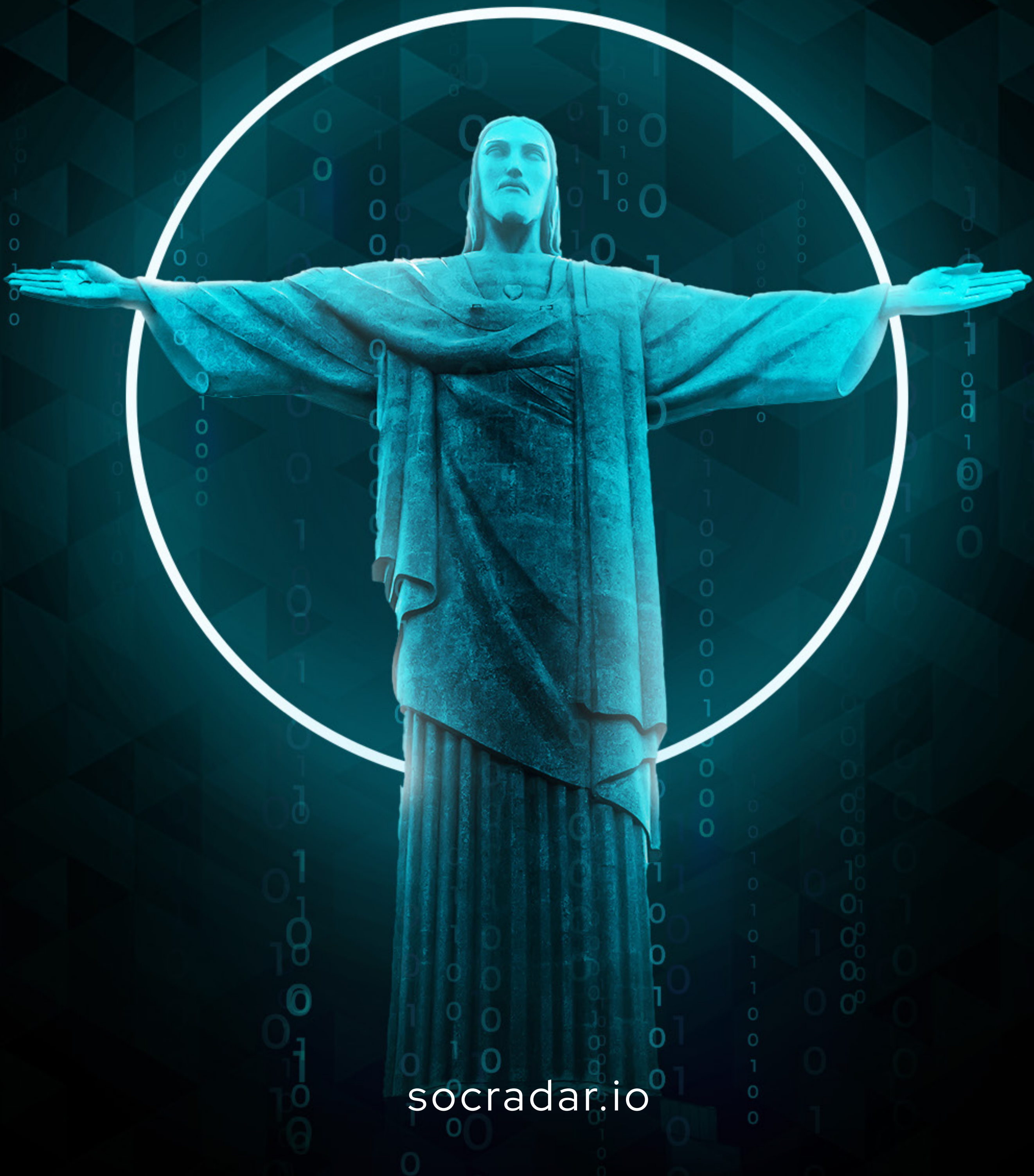
SOCRadar®
Your Eyes Beyond

BRAZIL THREAT LANDSCAPE REPORT

“Unmasking Stealer Malware Dominance in Brazil”



socradar.io

SOCRadar®
Your Eyes Beyond

Table of Contents

www.socradar.io

Executive Summary

This comprehensive report provides an in-depth analysis of the cyber threat landscape facing Brazil, including dark web activities, ransomware attacks, phishing threats, and the prevalence of Stealer malware. The following key findings have emerged from our research:

1. **Dark Web Activities:** The number of dark web posts mentioning Brazil has seen a significant increase over the last two years. The most targeted industries include Public Administration, E-commerce, Finance and Insurance, Information Technologies, and Telecommunications. The majority of these posts are related to data sharing and selling.

2. **Ransomware Attacks:** We've observed a decrease in ransomware attacks on Brazilian organizations in the past year. However, the Information Technologies industry remains the most targeted sector. A substantial number of these attacks are announced via shares in ransomware groups` own blog and leak sites, underscoring the importance of monitoring such platforms for early threat detection.

3. **Phishing Threats:** The registration of potential phishing domains impersonating Brazilian organizations remains a significant concern, despite a slight decrease in the past year. Most of these domains are secured by HTTPS, highlighting threat actors' efforts to appear legitimate and exploit the trust associated with SSL/TLS protocols. Industries related to cryptocurrency, international affairs, and banking are particularly targeted.

4. **Stealer Malware:** Brazil currently leads the world in infections by Stealer malware. Several factors contribute to this alarming trend, including **rampant usage of unlicensed software,** low cybersecurity awareness, a high population, and a substantial number of phishing attempts. The gaming market and the usage of free, untested VPNs also present a unique challenge in this context.

These findings underline the urgent need for enhanced cybersecurity measures and increased awareness to navigate the complex threat environment in Brazil. It is our hope that this report will equip organizations and individuals with the necessary information to better understand these threats and proactively protect themselves.

Introduction

In today's interconnected digital era, cybersecurity threats have become a universal concern. However, the risk landscape varies significantly from one country to another, influenced by a variety of factors such as local cyber practices, infrastructure, and threat awareness. This report focuses on one such nation with a unique threat landscape - Brazil.

Brazil, with its vast digital footprint and a growing economy, offers a fertile ground for cybercriminals. This report explores the different facets of the cyber threat environment in Brazil, providing a comprehensive insight into the prominent types of cyber threats faced by Brazilian organizations and the reasons why Brazil holds the unfortunate distinction of leading the world in certain malware infections.

We delve into several crucial aspects, including Dark Web activities, ransomware attacks, phishing threats, and the peculiar issue of Stealer malware that plagues the nation. Each section uses the latest available data and expert analysis to shed light on the current trends and potential countermeasures.

Understanding these threats is the first step towards a more secure digital future. By raising awareness about the specific cyber challenges facing Brazil, this report aims to contribute to the global discourse on cybersecurity and help Brazilian organizations better protect themselves against these evolving threats.

Timeline of Significant Cybersecurity Incidents in Brazil

Navigating through Brazil's cyber threat landscape, one must delve into the historical context defining its present cybersecurity challenges. Over time, Brazil has witnessed a significant volume of cyber threats - from high-profile government attacks to long-running campaigns targeting financial institutions - emphasizing the need for robust cybersecurity measures.

In 2022, Latin America and the Caribbean, including Brazil, fell victim to over **360 billion** attempted cyber attacks, according to data from FortiGuard Labs. In the region, Mexico bore the brunt of these attempts, suffering **187 billion** attacks, followed by Brazil with **103 billion,** indicating the relentless and massive scale of cyber threats confronting Brazil.

On May 30, 2021, JBS S.A., the world's largest meat supplier based in Brazil, fell victim to a devastating ransomware attack. The assault disrupted its computer networks across the US, Canada, and Australia, leading to a significant shutdown of its operations, including all US beef plants, accounting for nearly a quarter of American beef supply.

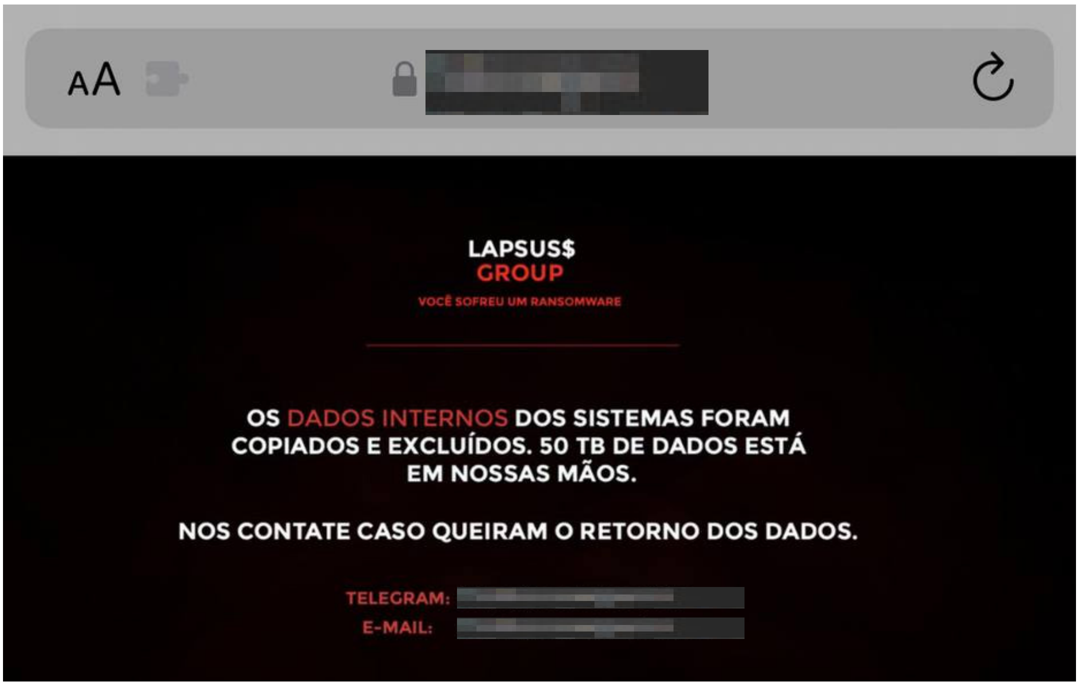
Creator: David Zalubowski | Credit: AP

Copyright: Copyright 2020 The Associated Press. All rights reserved.

Timeline of Significant Cybersecurity Incidents in Brazil

A major persistent and active campaign known as Operation Magalenha, initiated in 2021 and led by a Brazilian threat group, has further accentuated the threat landscape. Targeting users of over **30** Portuguese financial institutions, this ongoing operation employs a diverse arsenal of malware, including backdoors, credential stealers, and data exfiltration tools. The threat group has been quite successful in their endeavors, stealing credentials and personal information from numerous victims, potentially exploiting this information for financial gain or other malicious intentions.

One of the most significant and high-profile attacks occurred on December 10, 2021, when Brazil's Ministry of Health was subjected to a disruptive ransomware attack. The Lapsus$ Group claimed responsibility for the attack, alleging to have copied and then deleted a substantial **50TB of data** from the Ministry's systems. The data comprised sensitive information regarding the COVID-19 vaccination status of millions of Brazilian citizens.



[redacted]

LAPSUS$
GROUP
VOCÊ SOFREU UM RANSOMWARE

OS DADOS INTERNOS DOS SISTEMAS FORAM COPIADOS E EXCLUÍDOS. 50 TB DE DADOS ESTÁ EM NOSSAS MÃOS.

NOS CONTATE CASO QUEIRAM O RETORNO DOS DADOS.

TELEGRAM: [redacted]
E-MAIL: [redacted]

Not only did the attack render the Ministry's websites inaccessible, but it also disrupted the issuance of Brazil's COVID-19 digital vaccination certificate, a mandatory document for international travelers entering Brazil. This issue had potential ramifications for international travel during a global pandemic.

Other Important Attacks:

The Banco de Brasília Suffers a Ransomware Attack

On October 3, 2022, the government-controlled Banco de Brasília suffered a ransomware attack, with hackers demanding a ransom of 50 BTC to refrain from leaking sensitive user data. An individual using the pseudonym "Crydat" informed local media Tecmundo about the ransom demand, which equated to 5.2 million Brazilian Reals (BRL) at the time. The ransomware used was LockBit, popular among cybercriminals for its efficiency in encrypting system files and demanding cryptocurrency ransoms for their release.

PixPirate Targets Brazil's PIX Payments Platform

Between the end of 2022 and early 2023, a new Android banking Trojan, PixPirate, emerged, targeting Brazilian financial institutions via the PIX payments platform. Cybersecurity company Cleafy discovered the malware and is closely monitoring it. PIX, introduced by Banco Central do Brasil in November 2020, quickly became a cornerstone of Brazil's financial system, with over 107.5 million registered accounts and transactions worth more than half a trillion BRL in a year. PixPirate's focus on PIX payments suggests a calculated strategy to exploit this widely-used system, showcasing the inherent risks of digital financial platforms.

Aker Solutions' Brazil M&M Operation Targeted by Cyber Attack

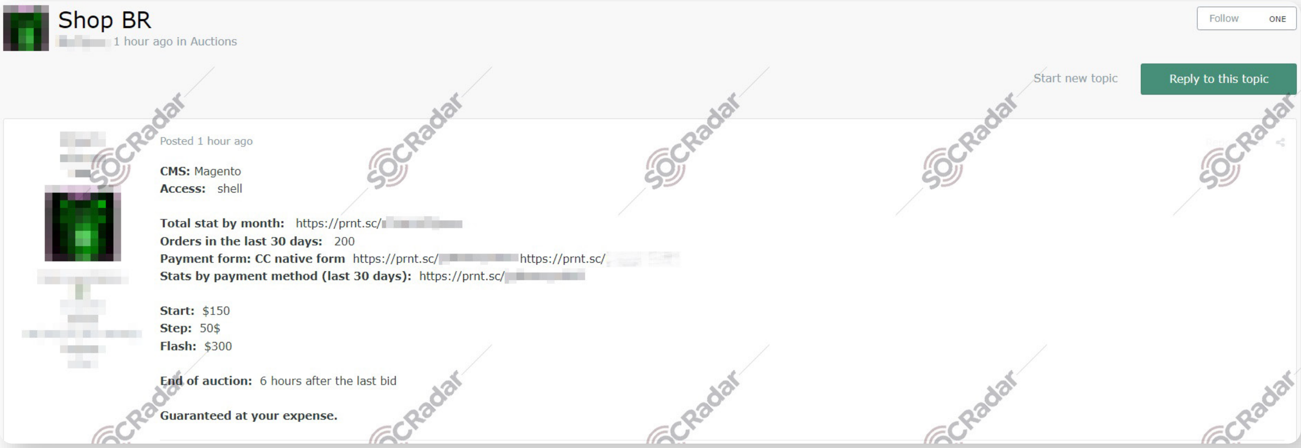
On February 15, 2023, Aker Solutions' subsidiary in Brazil, CSE, fell victim to a cyberattack. The assailants claimed to have infiltrated the IT systems, encrypted digital files, and locked access to data. CSE provides maintenance and modifications to Brazil's offshore oil and gas installations, servicing key clients like state-run Petrobras and various international energy companies. The implications of this attack underscore the pervasive cybersecurity threats facing critical energy infrastructure.

Recent Events:

May 28
2023

Unauthorized Shell Access Sale is Detected for a Brazilian E-Commerce Company

In a hacker forum monitored by SOCRadar, an unauthorized shell access sale is detected, allegedly belonging to an e-commerce company that operates in Brazil.



[redacted] 1 hour ago in Auctions

Posted 1 hour ago

CMS: Magento
Access: shell

Total stat by month: https://prnt.sc/[redacted]
Orders in the last 30 days: 200
Payment form: CC native form https://prnt.sc/[redacted] https://prnt.sc/[redacted]
Stats by payment method (last 30 days): https://prnt.sc/[redacted]

Start: $150
Step: 50$
Flash: $300

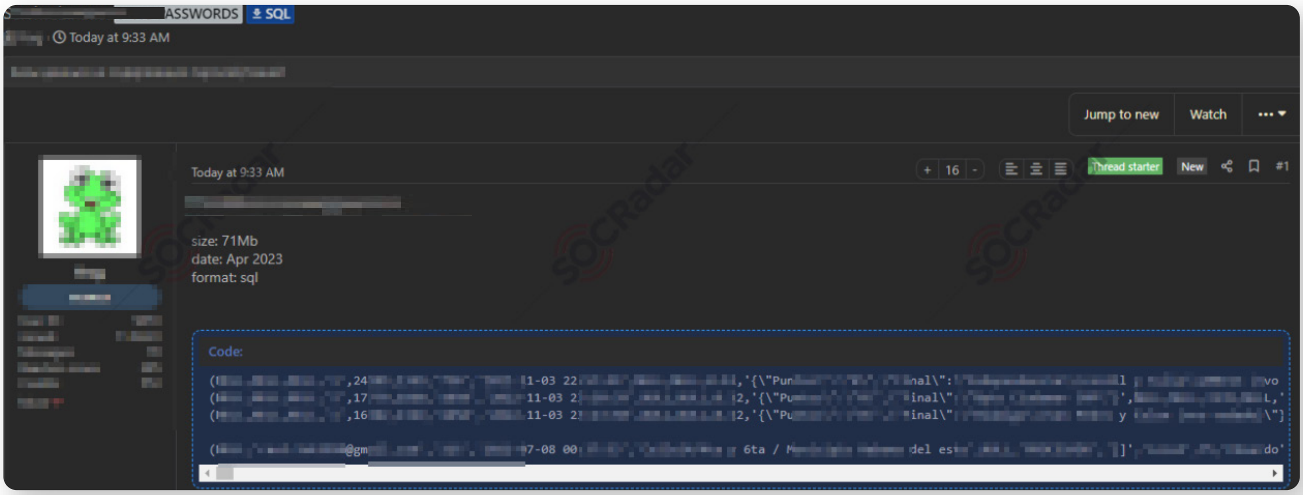
End of auction: 6 hours after the last bid

Guaranteed at your expense.

May 23
2023

Unauthorized Network Access Sale is Detected for a Brazilian Cloud Company

In a hacker forum monitored by SOCRadar, an unauthorized network access sale is detected allegedly belongs to a cloud company that operates in Brazil.



[redacted] Today at 9:33 AM

[redacted]

Today at 9:33 AM

[redacted]

size: 71Mb
date: Apr 2023
format: sql

Code:

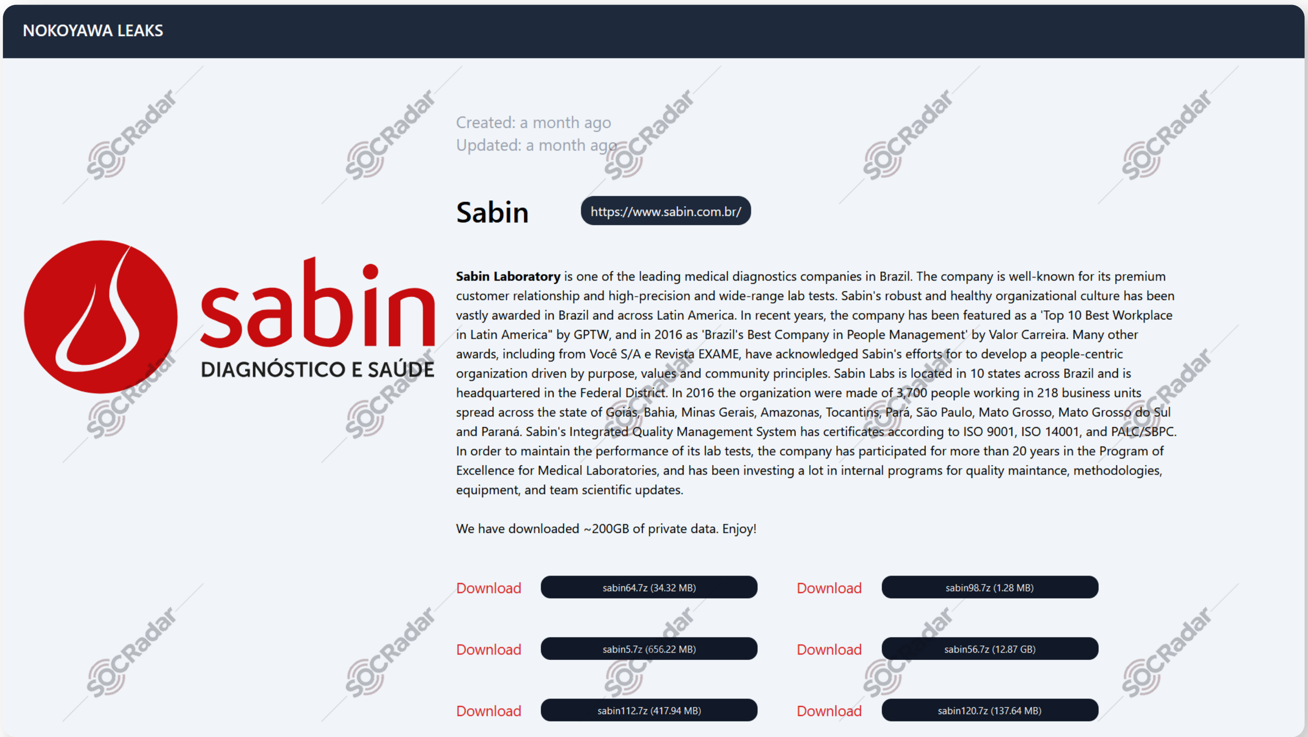
```
([redacted],24[redacted]11-03 22[redacted],'{\"Pu[redacted]nal\":[redacted]l [redacted]vo
([redacted],17[redacted]11-03 2[redacted]2,'{\"Pu[redacted]inal\"[redacted]',[redacted]L,'
([redacted],16[redacted]11-03 2[redacted]2,'{\"Pu[redacted]inal\"[redacted] y [redacted]\"}

([redacted]@gm[redacted]7-08 00[redacted] 6ta / M[redacted]del es[redacted]]'[redacted]do'
```

Recent Events:

May 22
2023

Nokoyawa Ransomware Group Leaked The Data of Grupo Sabin

In the Nokoyawa ransomware group website monitored by SOCRadar, new data leaks detected allegedly belong to Grupo Sabin.



Created: a month ago
Updated: a month ago

Sabin https://www.sabin.com.br/

Sabin Laboratory is one of the leading medical diagnostics companies in Brazil. The company is well-known for its premium customer relationship and high-precision and wide-range lab tests. Sabin's robust and healthy organizational culture has been vastly awarded in Brazil and across Latin America. In recent years, the company has been featured as a 'Top 10 Best Workplace in Latin America" by GPTW, and in 2016 as 'Brazil's Best Company in People Management' by Valor Carreira. Many other awards, including from Você S/A e Revista EXAME, have acknowledged Sabin's efforts for to develop a people-centric organization driven by purpose, values and community principles. Sabin Labs is located in 10 states across Brazil and is headquartered in the Federal District. In 2016 the organization were made of 3,700 people working in 218 business units spread across the state of Goiás, Bahia, Minas Gerais, Amazonas, Tocantins, Pará, São Paulo, Mato Grosso, Mato Grosso do Sul and Paraná. Sabin's Integrated Quality Management System has certificates according to ISO 9001, ISO 14001, and PALC/SBPC. In order to maintain the performance of its lab tests, the company has participated for more than 20 years in the Program of Excellence for Medical Laboratories, and has been investing a lot in internal programs for quality maintance, methodologies, equipment, and team scientific updates.

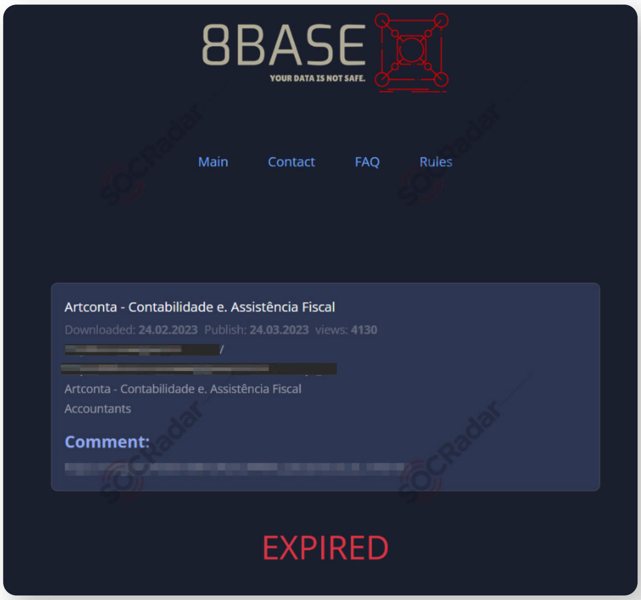
We have downloaded ~200GB of private data. Enjoy!

Download	sabin64.7z (34.32 MB)	Download	sabin98.7z (1.28 MB)
Download	sabin5.7z (656.22 MB)	Download	sabin56.7z (12.87 GB)
Download	sabin112.7z (417.94 MB)	Download	sabin120.7z (137.64 MB)

May 21
2023

8Base Ransomware Group Leaked The Data of Artconta

In the 8Base ransomware group website monitored by SOCRadar, new data leaks detected allegedly belong to Artconta.



Artconta - Contabilidade e. Assistência Fiscal
Downloaded: **24.02.2023** Publish: **24.03.2023** views: **4130**
[redacted]/
Artconta - Contabilidade e. Assistência Fiscal
Accountants

Comment:
[redacted]

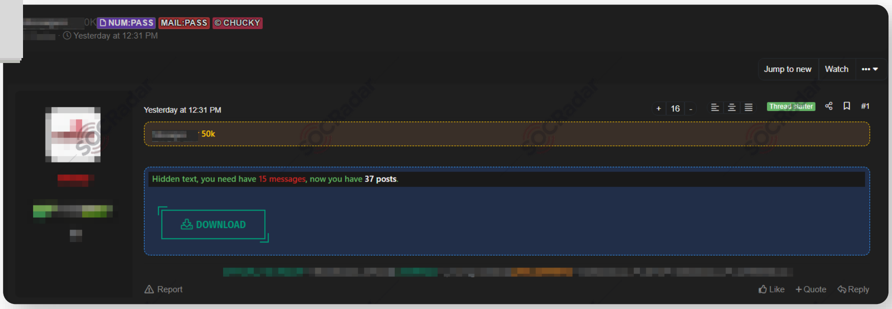
EXPIRED

Recent Events:

May 20
2023

A Database of Claro customers is Leaked

In a hacker forum monitored by SOCRadar, a new alleged database leak is detected for Claro.



[redacted] 0K NUM:PASS MAIL:PASS ©CHUCKY
[redacted] · Yesterday at 12:31 PM

Yesterday at 12:31 PM

[redacted] 50k

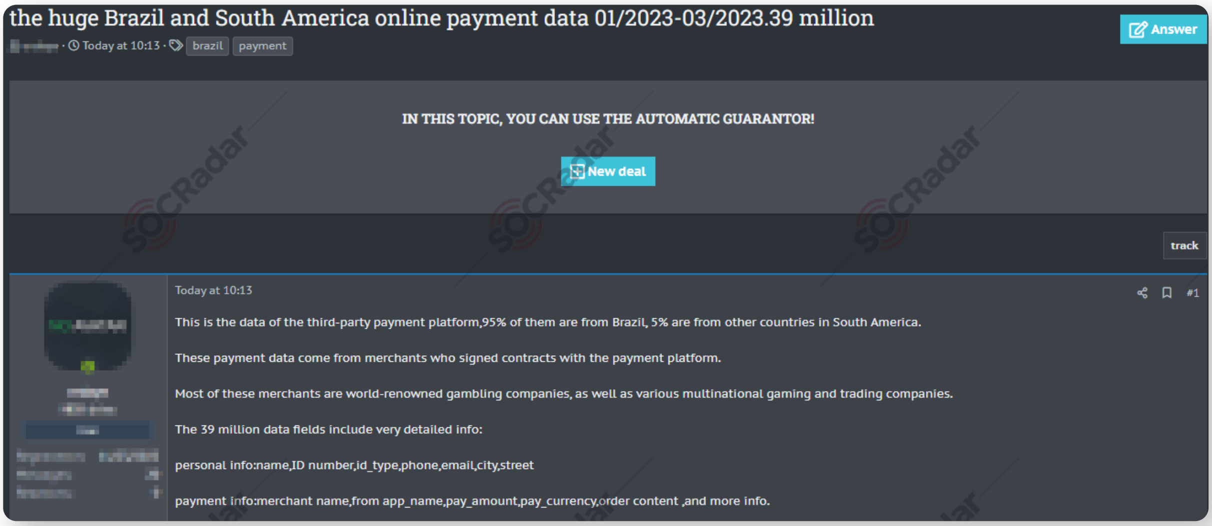
Hidden text, you need have 15 messages, now you have 37 posts.

May 9
2023

Database of Online Payments with 39M Entries Reportedly for Sale

SOCRadar's monitoring of a hacker forum has led to the detection of a potential database sale, associated with an online payment service that operates primarily in Brazil and other parts of South America. It's alleged that this database originates from a third-party payment platform, with an overwhelming 95% of the data pertaining to Brazil and the rest spread across other South American countries. The threat actor claims that the purported payment information originates from merchants contracted to this third-party payment platform. The database in question comprises 39 million records, with each entry offering extensive details.

The stored information allegedly covers a wide range, including personal data such as names, ID numbers, ID types, phone numbers, emails, cities, and street addresses. Furthermore, it encompasses payment specifics like the name of the merchant, the app from which the payment was made, payment amount, payment currency, and order content. Remarkably, it also appears to include numerous merchant passwords and tokens.



the huge Brazil and South America online payment data 01/2023-03/2023.39 million

[redacted] · Today at 10:13 · brazil payment

IN THIS TOPIC, YOU CAN USE THE AUTOMATIC GUARANTOR!

Today at 10:13

This is the data of the third-party payment platform,95% of them are from Brazil, 5% are from other countries in South America.

These payment data come from merchants who signed contracts with the payment platform.

Most of these merchants are world-renowned gambling companies, as well as various multinational gaming and trading companies.

The 39 million data fields include very detailed info:

personal info:name,ID number,id_type,phone,email,city,street

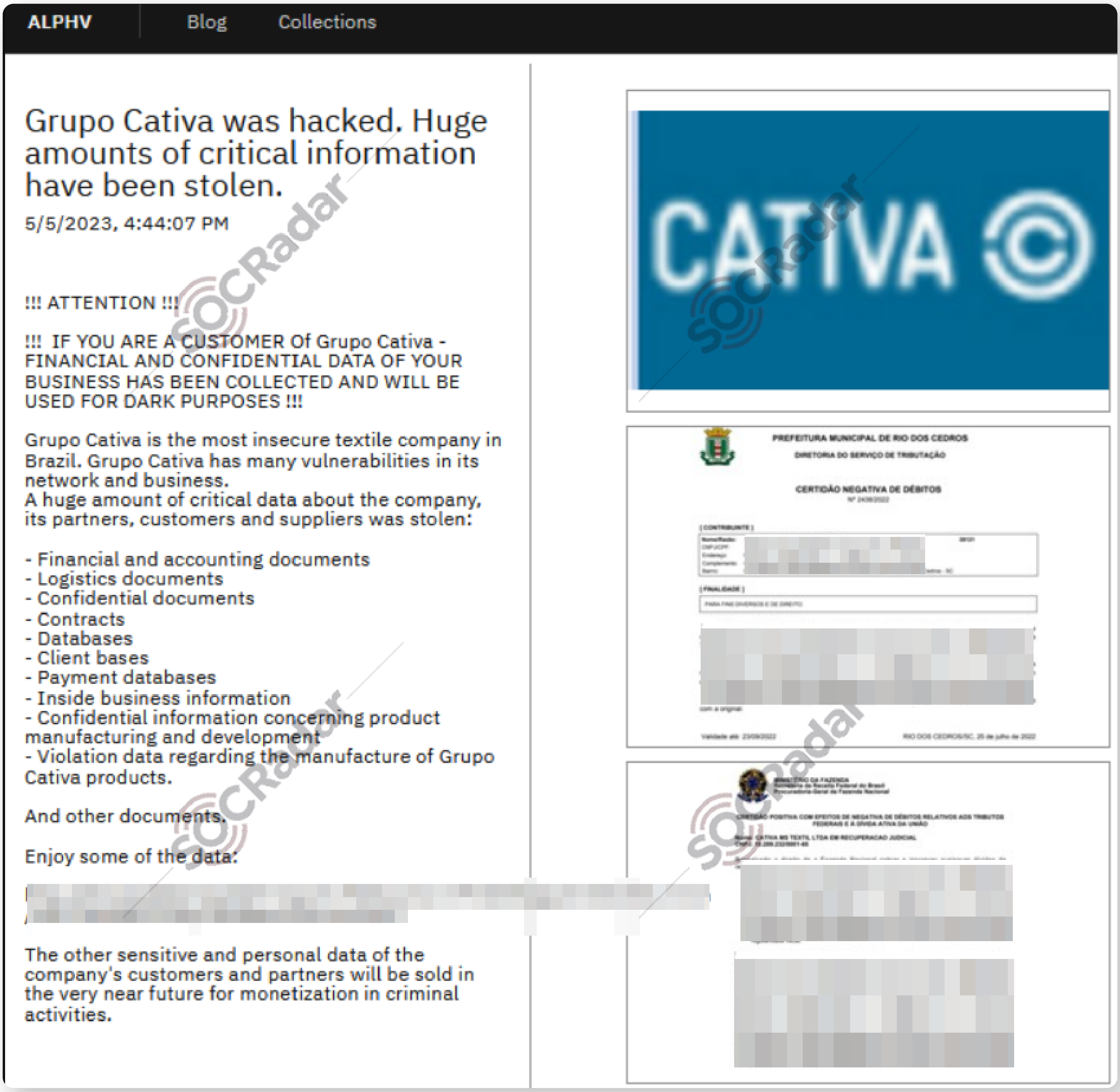
payment info:merchant name,from app_name,pay_amount,pay_currency,order content ,and more info.

Recent Events:

May 4
2023

AlphVM Blackcat Ransomware Group Leaked of Grupo Cativa

In the AlphVM / Blackcat ransomware group website monitored by SOCRadar, new data leaks detected allegedly belong to Grupo Cativa.



Grupo Cativa was hacked. Huge amounts of critical information have been stolen.

5/5/2023, 4:44:07 PM

!!! ATTENTION !!!

!!! IF YOU ARE A CUSTOMER Of Grupo Cativa - FINANCIAL AND CONFIDENTIAL DATA OF YOUR BUSINESS HAS BEEN COLLECTED AND WILL BE USED FOR DARK PURPOSES !!!

Grupo Cativa is the most insecure textile company in Brazil. Grupo Cativa has many vulnerabilities in its network and business.
A huge amount of critical data about the company, its partners, customers and suppliers was stolen:

- Financial and accounting documents
- Logistics documents
- Confidential documents
- Contracts
- Databases
- Client bases
- Payment databases
- Inside business information
- Confidential information concerning product manufacturing and development
- Violation data regarding the manufacture of Grupo Cativa products.

And other documents.

Enjoy some of the data:

[redacted]

The other sensitive and personal data of the company's customers and partners will be sold in the very near future for monetization in criminal activities.

PREFEITURA MUNICIPAL DE RIO DOS CEDROS
DIRETORIA DO SERVIÇO DE TRIBUTAÇÃO

CERTIDÃO NEGATIVA DE DÉBITOS

[CONTRIBUINTE]

[redacted]

[FINALIDADE]

PARA FINS DIVERSOS E DE DIREITO

[redacted]

com o original.

Validade até: 23/09/2022 RIO DOS CEDROS/SC, 25 de julho de 2022

MINISTÉRIO DA FAZENDA
Secretaria da Receita Federal do Brasil
Procuradoria-Geral da Fazenda Nacional

CERTIDÃO POSITIVA COM EFEITOS DE NEGATIVA DE DÉBITOS RELATIVOS AOS TRIBUTOS FEDERAIS E À DÍVIDA ATIVA DA UNIÃO

Nome: CATIVA MS TEXTIL LTDA EM RECUPERACAO JUDICIAL
CNPJ: [illegible]

[redacted]

[redacted]

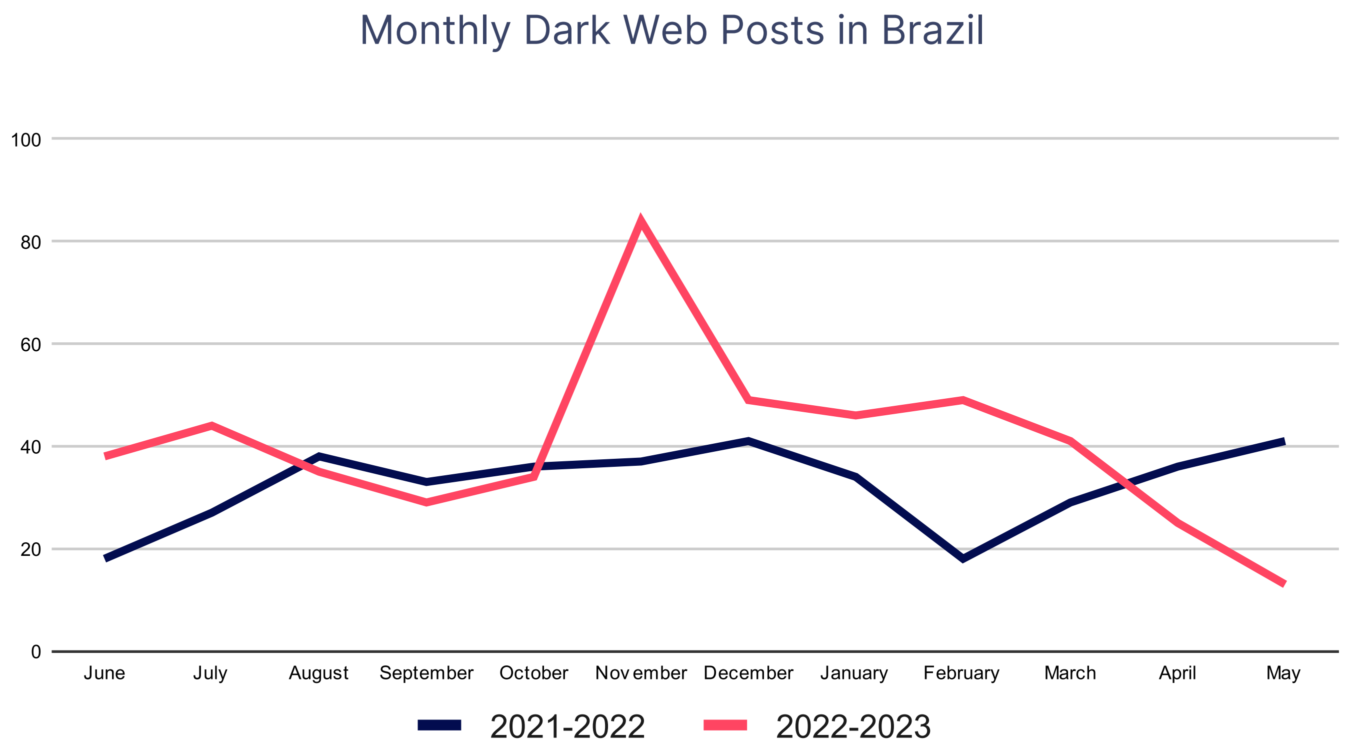
This timeline elucidates the ongoing and escalating cybersecurity challenges in Brazil, underscoring the critical need for enhanced threat intelligence, effective preventive strategies, and improved incident response capabilities.

Dark Web Radar: A Deep Dive into Brazil-Related Activities

This section offers an analysis of Brazil-related activities on the dark web, focusing on specific periods from 2021 to 2023.

Monthly Posts

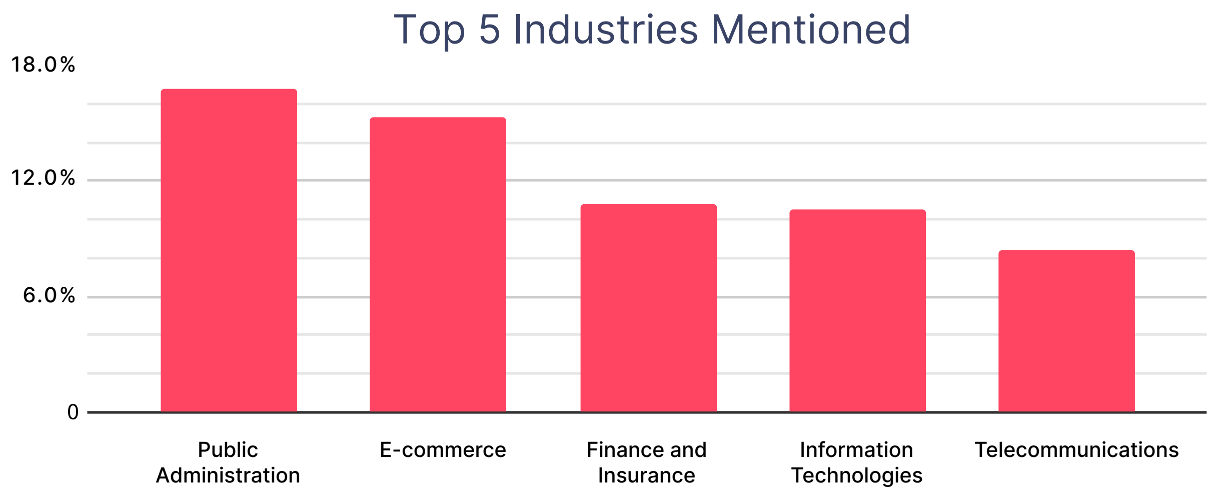
The first part of our analysis involves a comparison of the total number of monthly dark web posts referencing Brazil over a span of two years, from June 2021 to May 2023. During the 2021-2022 period, the number of posts averaged around 32 per month. This number saw a marked increase during the 2022-2023 period, with an average of 41 posts per month, indicating a growing interest in Brazil on the dark web. November 2022 was the peak of this activity, seeing a total of 84 posts related to Brazil.



Dark Web Radar: A Deep Dive into Brazil-Related Activities

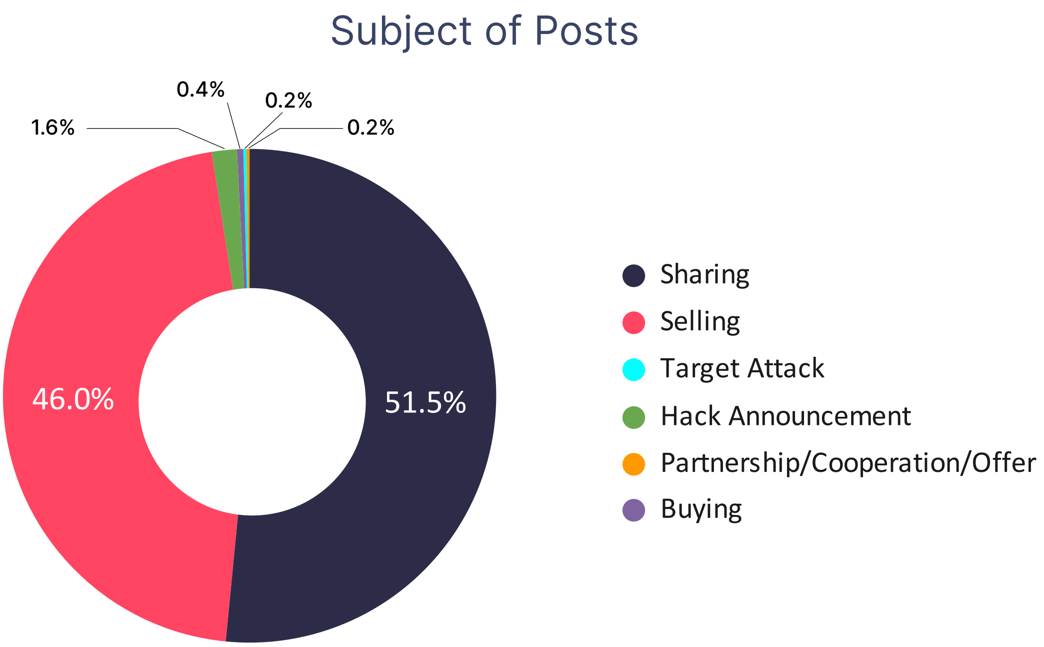
Top Targeted Industries on Dark Web

In a closer look at the last year, from June 2022 to May 2023, we analyzed the industries most often targeted in these posts. Public Administration emerged as the most frequently mentioned, accounting for 11.5% of all posts. E-commerce was a close second at 10.5%. Finance and Insurance represented 7.4% of the posts, while Information Technologies and Telecommunications were mentioned in 7.2% and 5.7% of posts respectively. These figures highlight the most discussed and potentially vulnerable sectors on the dark web.



Subjects of Posts

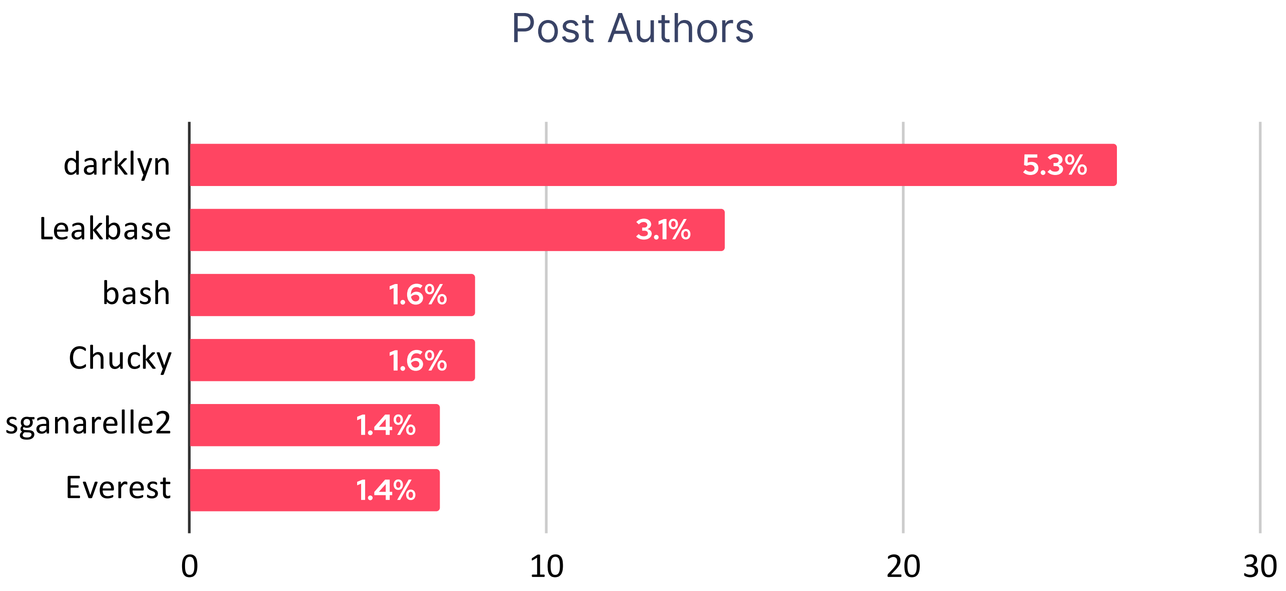
Further examining the last year's data, we categorized posts by their subject matter. Most posts, at 51.5%, revolved around Sharing, with Selling following closely at 46.0%. Other topics like Hack Announcements, Buying, Target Attacks, and Partnership/Cooperation/Offer were significantly less common, showing that the bulk of these posts focused on information exchange or transactional purposes.



Dark Web Radar: A Deep Dive into Brazil-Related Activities

Post Authors

Finally, we identified the most active authors of posts concerning Brazil in the past year. **"Darklyn"** took the lead, contributing 5.3% of the posts, followed by **"Leakbase"** at 3.1%. Other contributors like **"bash"**, **"Chucky"**, **"sganarelle2",** and **"Everest"** added to the dialogue, but at a lower frequency. However, it's important to clarify that we currently make no assertions about any connections between the authors of the posts and the threat actors, due to the absence of sufficient supporting evidence at this time.



Overall, this analysis reveals a rising trend of Brazil-centric activities on the dark web over the past two years, with a more detailed snapshot of the last year showing the most targeted industries, common subjects, and active authors. Understanding these trends is critical for anticipating potential threats and developing robust cyber defenses.

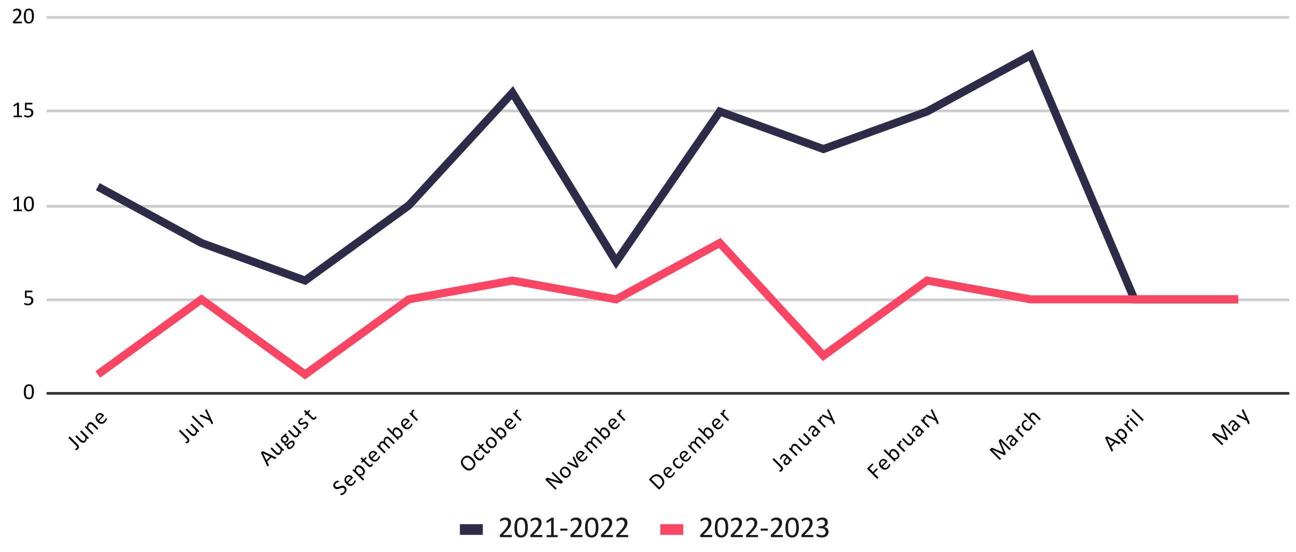
Analyzing Ransomware Threat Landscape of Brazilian Organizations

This section delves into a detailed assessment of ransomware activities that have targeted Brazilian organizations over specific periods from 2021 to 2023.

Trends in Ransomware Attacks

We begin by exploring the total number of ransomware-related posts following attacks on Brazilian organizations over the last two years, from June 2021 to May 2023. The period of 2021-2022 saw a higher frequency of posts, with a monthly average of 10.75, which significantly decreased in the subsequent year, averaging at 4.5 posts monthly.

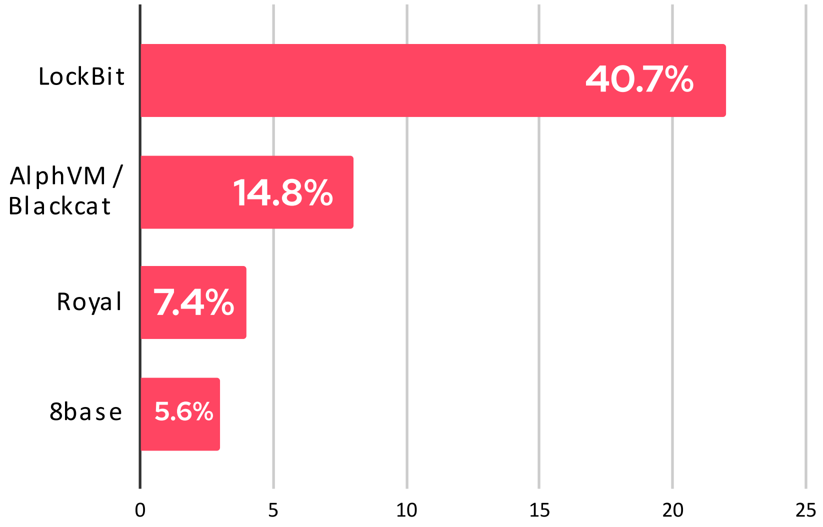
Top Ransomware Groups Targeting Brazilian Organizations



Prominent Ransomware Groups

Next, we examine the ransomware groups that were most active in targeting Brazilian organizations during the last year. The group known as "LockBit" stood out, responsible for 40.7% of the attacks. Other active groups included "AlphVM / Blackcat", contributing 14.8%, "Royal" at 7.4%, and "8base" with 5.6%.

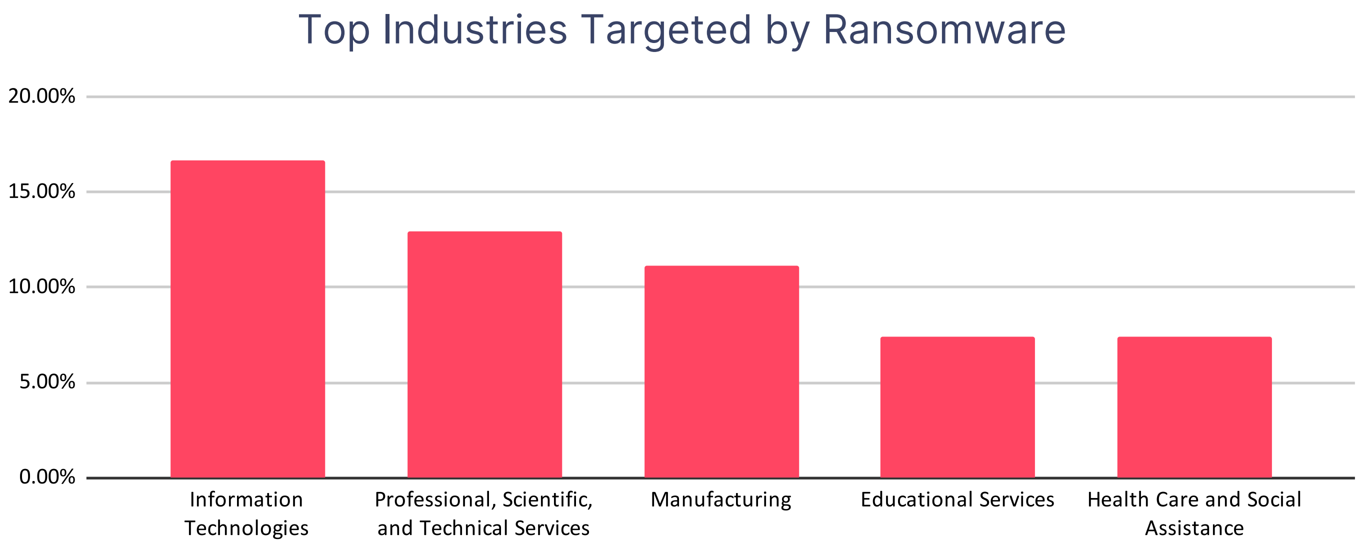
Top Ransomware Groups Targeting Brazilian Organizations



Analyzing Ransomware Threat Landscape of Brazilian Organizations

Industries Under Siege

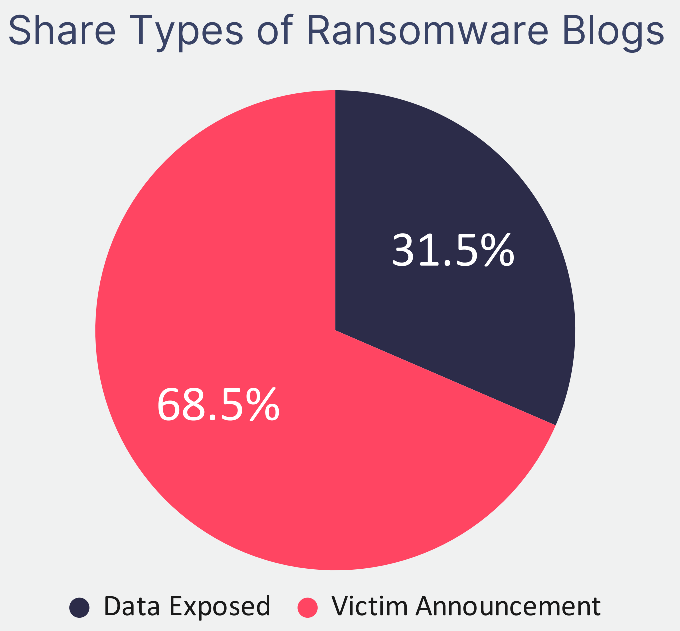
Turning our attention to the most recent year from June 2022 to May 2023, we highlight the industries most often mentioned in these ransomware posts. Information Technologies was most frequently targeted, making up 16.7% of all posts. The Professional, Scientific, and Technical Services followed closely at 13.0%, with Manufacturing at 11.1%. Educational Services and Health Care and Social Assistance were not spared either, each constituting 7.4% of the posts.



Categorizing Ransomware Posts

Last, we categorize the ransomware posts from the past year by their type. The majority of the posts, 68.5%, were Victim Announcements, while Data Exposed posts constituted 31.5%. This suggests a focus on broadcasting attacks and identifying victims over sharing sensitive compromised data.

This analysis gives a thorough understanding of the ransomware threat landscape in Brazilian organizations, helping them design robust defense strategies against such attacks.

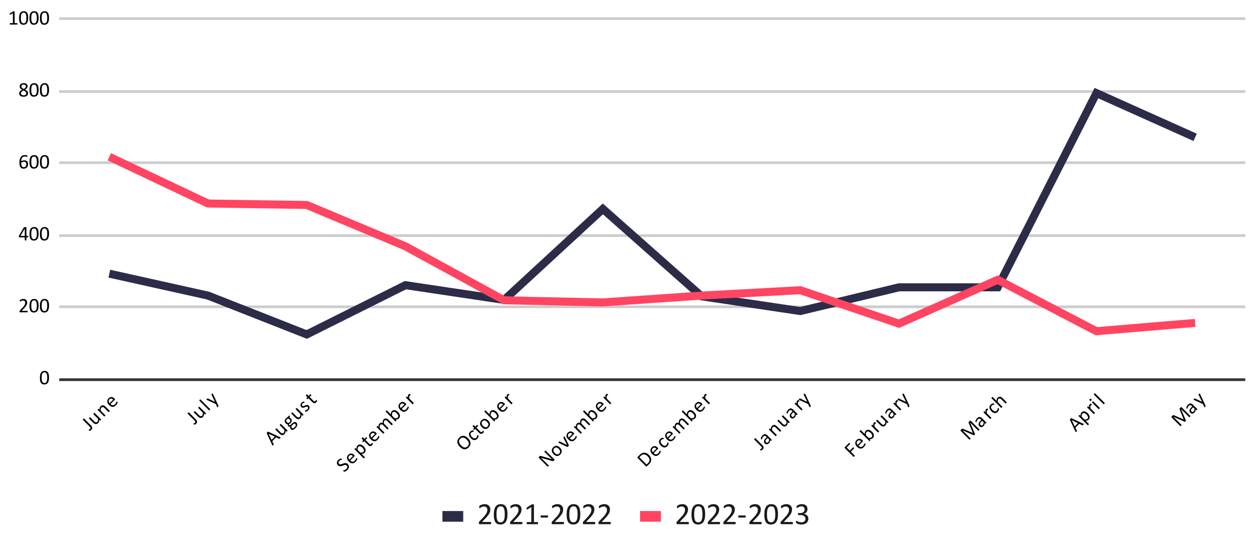


Deceptive Domains: Unpacking the Phishing Threats against Brazilian Organizations

Escalation in Phishing Domain Registrations

Over the past two years, from June 2021 to May 2023, there has been a significant number of potential phishing domains registered with the intent to impersonate Brazilian organizations. During the 2021-2022 period, a total of 3.999 domains were registered, averaging around 333 per month. In the subsequent year, 2022-2023, a total of 3.589 domains were identified, translating to a monthly average of approximately 299. While these numbers show a slight decrease in the recent year, the threat remains substantial, as evident in the still high number of potential phishing domains. These domains can dupe users into sharing sensitive information under the guise of interacting with a legitimate entity.

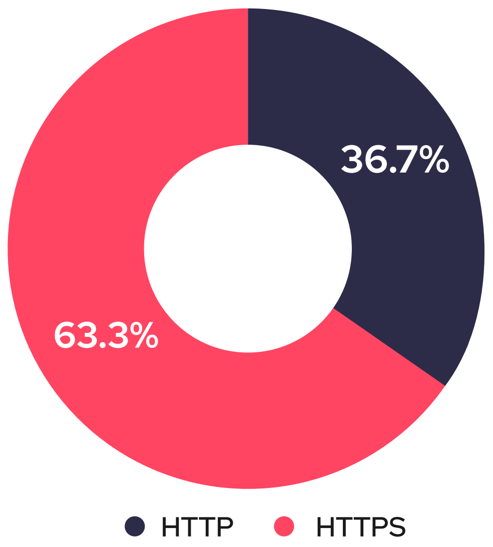
Number of Potential Phishing Domains



Misuse of SSL/TLS Protocols by Phishing Domains

When analyzing the usage of SSL/TLS protocols by these potential phishing domains, a concerning trend emerges. A significant 63.3% of these domains used HTTPS, while the remaining 36.7% opted for HTTP. It's important to note that threat actors often misuse HTTPS to lend a false sense of security to their potential victims. The presence of the padlock icon next to the HTTPS protocol can deceive users into believing that the website is secure and authentic, making them more likely to share sensitive data.

HTTP/S Protocol Usage



Deceptive Domains: Unpacking the Phishing Threats against Brazilian Organizations

Target Industries and Commonly Used Website Titles

In the context of targeted industries for potential impersonating domains, the top five are: CryptoCurrency & NFT, National Security & International Affairs, Information Services, Public Administration, and Banking, indicating their high-risk status for phishing threats.

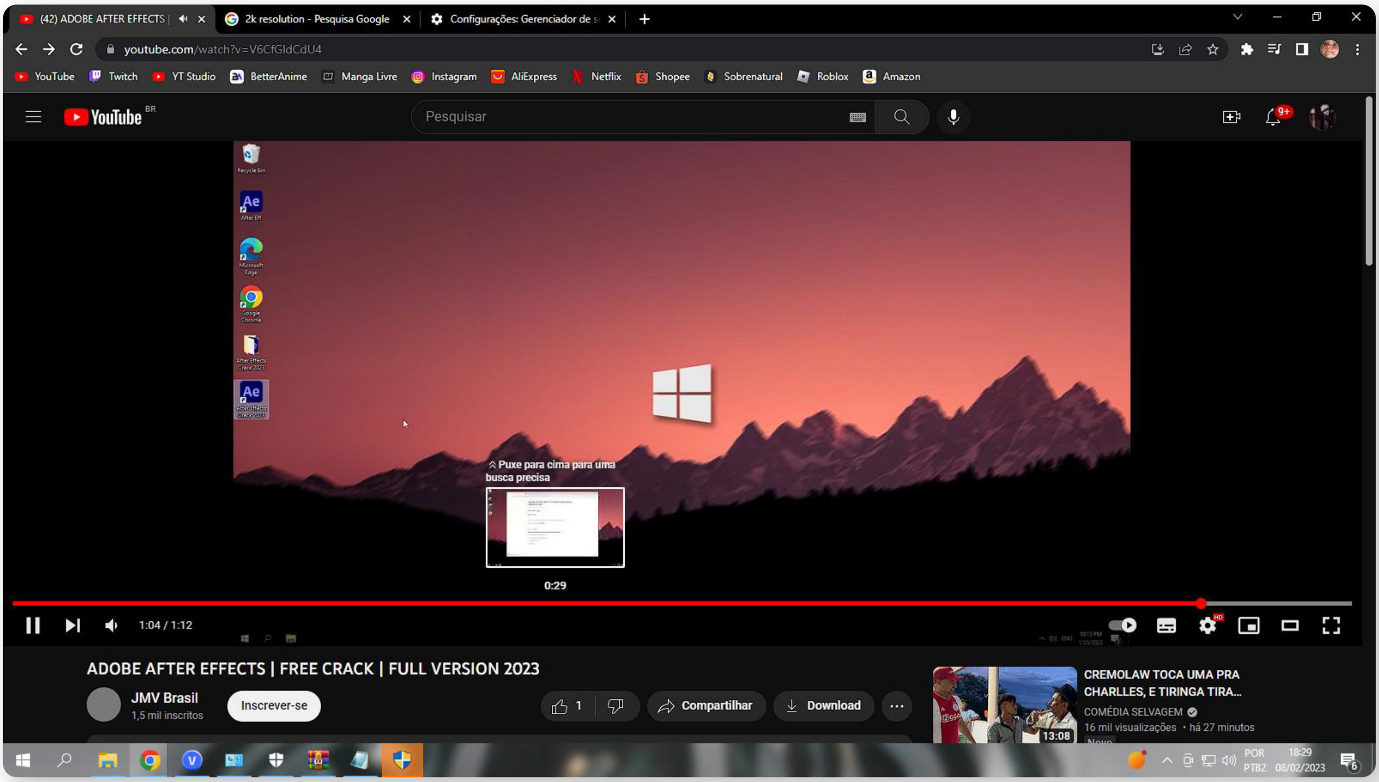
Meanwhile, the titles used in these potential phishing domains often impersonate reputable and globally recognized platforms. Some of the top titles found include: "Join the HypeSquad | Discord," "Sign in to Kraken - Kraken," "Microsoft account," and "Sign in to Outlook". These well-known names help to increase the credibility of the phishing domains, thereby enhancing their chance of successfully deceiving users.

These trends underline the persistent and evolving nature of phishing threats that Brazilian organizations face, emphasizing the need for continuous vigilance, regular updates to security protocols, and user education to mitigate these risks.

A Deep Dive into Stealer Malware: Why Brazil Leads the Infection Charts

Stealer malware, as the name suggests, is malicious software designed to steal sensitive data from the user's device. It's a part of the growing cyber threat landscape that has been gaining prominence due to its effectiveness and affordability. Especially pertinent to our focus is the alarmingly high infection rate of this specific type of malware in Brazil.

To provide context, a recent whitepaper published by SOCRadar, titled 'Snapshot of 70 Million Stealer Logs,' reveals the extent of the global Stealer problem. The study analyzed a sample of 400 gigabytes of stealer log data from the first week of March 2023, derived from a variety of sources such as illegal forums, chat platforms, and social media groups. The data, cleaned to remove any artificially inflated records, suggests that in just a week, over 100,000 individuals from 200 different countries had been infected by stealer malware.

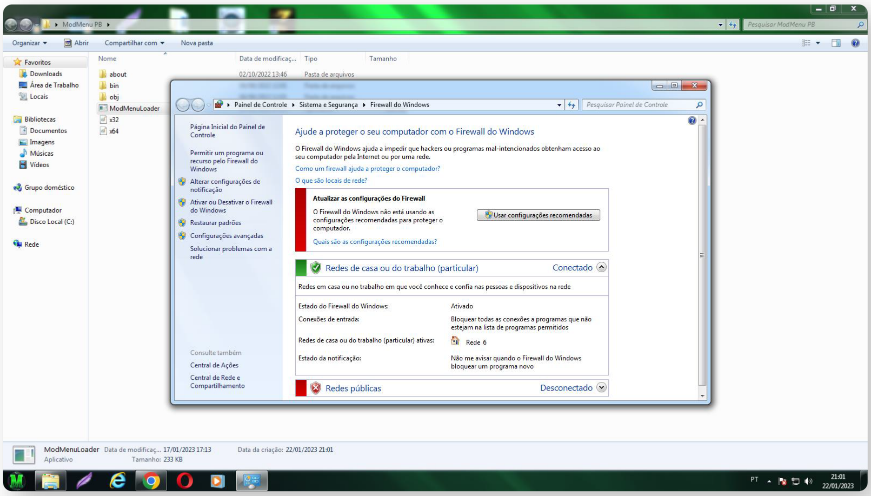

(42) ADOBE AFTER EFFECTS |
2k resolution - Pesquisa Google
Configurações: Gerenciador de s
youtube.com/watch?v=V6CfGldCdU4
YouTube
Twitch
YT Studio
BetterAnime
Manga Livre
Instagram
AliExpress
Netflix
Shopee
Sobrenatural
Roblox
Amazon
Pesquisar
Puxe para cima para uma busca precisa
0:29
1:04 / 1:12
ADOBE AFTER EFFECTS | FREE CRACK | FULL VERSION 2023
JMV Brasil
1,5 mil inscritos
Inscrever-se
1
Compartilhar
Download
CREMOLAW TOCA UMA PRA CHARLLES, E TIRINGA TIRA...
COMÉDIA SELVAGEM
16 mil visualizações · há 27 minutos
13:08
POR PTB2
18:29
08/02/2023

A screenshot captured by a malicious stealer malware shows a Brazilian victim attempting to install the software through a video tutorial.

The rise of 'Stealer-as-a-Service,' a model where info-stealer tools are sold or leased over the internet, only exacerbates the problem. As reported by SOCRadar, this model is increasingly being utilized by cybercriminals ranging from nation-state groups to amateurs with low technical skills.

A Deep Dive into Stealer Malware: Why Brazil Leads the Infection Charts

Of the countries analyzed, Brazil stood out, along with Egypt and India, in the top three countries most infected by stealer malware. These findings are corroborated by additional studies, such as one conducted by Accenture's Cyber Threat Intelligence team, which indicated a significant increase in infostealer victims in Brazil between July and October 2022.



02/10/2022 13:46 Pasta de arquivos

Ajude a proteger o seu computador com o Firewall do Windows

O Firewall do Windows ajuda a impedir que hackers ou programas mal-intencionados obtenham acesso ao seu computador pela Internet ou por uma rede.

Como um firewall ajuda a proteger o computador?

O que são locais de rede?

Atualizar as configurações do Firewall

O Firewall do Windows não está usando as configurações recomendadas para proteger o computador.

Quais são as configurações recomendadas?

Redes de casa ou do trabalho (particular) Conectado

Redes em casa ou no trabalho em que você conhece e confia nas pessoas e dispositivos na rede

Estado do Firewall do Windows:	Ativado
Conexões de entrada:	Bloquear todas as conexões a programas que não estejam na lista de programas permitidos
Redes de casa ou do trabalho (particular) ativas:	Rede 6
Estado da notificação:	Não me avisar quando o Firewall do Windows bloquear um programa novo

Redes públicas Desconectado

ModMenuLoader Data de modificaç... 17/01/2023 17:13 Data da criação: 22/01/2023 21:01
Aplicativo Tamanho: 233 KB

A separate screenshot, taken by the stealer malware, reveals another Brazilian victim disabling the Windows firewall in order to download cheat modes for a game.

But what makes Brazil such a hotbed for stealer malware infections? Various factors might be contributing to this heightened risk:

Widespread Use of Unlicensed Software: Brazil ranks high for visits to software piracy sites, which often contain hidden malware.

Low Cybersecurity Awareness: Lack of knowledge and understanding about cybersecurity best practices among the population increases vulnerability to such threats.

Unique Video Gaming Market: Brazil's mixed gaming market, featuring both licensed and cracked games, provides ample opportunities for malware distribution.

High Population: Brazil ranks 6th in the world in terms of population, meaning a larger pool of potential victims.

High Number of Phishing Attempts: As we've previously discussed in this report, Brazil faces a high number of phishing attempts, which is a common delivery method for stealer malware.

VPN Usage: The current ban on Telegram in Brazil has led to an increase in free and untested VPN software usage, presenting another avenue for malware attacks.

The data provides a clear warning. Cybersecurity threats are increasingly sophisticated, and no region is immune. A proactive, informed approach to cyber threats is more necessary than ever, especially in nations like Brazil, where the risk is significantly heightened.

Lessons Learned: Key Takeaways and Strategic Recommendations

As we reflect on the cyber threat landscape encompassing Brazilian organizations, several crucial lessons and recommendations become evident. These insights, combined with the capabilities of SOCRadar, can provide a roadmap for enhancing cyber resilience and maintaining operational integrity. Here are five key takeaways from our analysis:

1. **Maintain awareness of the evolving cyber threat landscape:** It's clear that the cyber threat landscape is rapidly changing, as indicated by the increase in dark web posts related to Brazil and the proliferation of ransomware attacks. Organizations must keep abreast of these changes and adjust their security strategies accordingly. With SOCRadar's Cyber Threat Intelligence, businesses can access real-time insights on emerging threats, allowing them to remain one step ahead of cyber criminals.

2. **Focus on multi-layered security measures:** The diverse industries targeted by cyber threats emphasize the need for multi-layered security measures. As we've seen, attackers don't discriminate based on industry. Thus, all sectors, from Public Administration to Information Technologies, should adopt a comprehensive security approach. SOCRadar can aid in this effort with its proactive threat intelligence and monitoring services.

3. **Educate and train employees:** As phishing remains a prevalent issue, there's a strong need for continuous education and training for employees. Understanding the nature of phishing attempts and how to detect them is crucial. SOCRadar's solutions can help here too by identifying potential phishing domains and raising awareness of the latest phishing tactics.

4. **Stay vigilant against ransomware:** Ransomware continues to be a significant threat, and it's essential to not only have robust defenses in place but also to have a strong response plan for if your organization falls victim. SOCRadar's threat intelligence can help businesses identify potential ransomware threats and develop an effective response plan.

5. **Ensure security against Stealers:** With Brazil being the leading country for infected Stealer malware, companies need to bolster their defense mechanisms against these malicious software. SOCRadar's advanced threat intelligence can assist in detecting and combating Stealer threats, contributing to the overall security posture of the organization.

In conclusion, it's essential to have a proactive, informed, and comprehensive approach to cyber security. By partnering with solutions like SOCRadar, Brazilian organizations can strengthen their defenses and be better prepared to respond to the rapidly changing cyber threat landscape.

Who is SOCRadar®?

Your Eyes Beyond

As an Extended Threat Intelligence (XTI) platform and inventor of the concept, SOCRadar's approach effectively integrates Threat Intelligence, Digital Risk Protection, and External Attack Surface Management (EASM). Adapting proactive security with a hacker mindset, we aim to help security teams to detect blindspots before attackers.

The shortage of cybersecurity experts is a growing problem worldwide. All companies around the world must use resources efficiently to provide adequate cyber security with their limited resources. Automated security solutions offer precisely the opportunity that corporations are looking for. With its AI-powered automation technology. **With providing protection against threats for more than 6.000+ companies from 157 countries, SOCRadar has become an extension of SOC teams from every industry.**

SOCRadar provides extended cyber threat intelligence (XTI) that combines: **"Cyber Threat Intelligence, Digital Risk Protection, and External Attack Surface Management Services."** SOCRadar provides the actionable and timely intelligence context you need to manage the risks in the transformation era.

8.400
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 12 MONTHS FOR FREE

Gartner Peer Insights Customer First

Gartner. Peer Insights™ 5/5 ★★★★★

Contact Us

✉ info@socradar.io

☎ +1 (571) 249-4598

651 N Broad St, Suite 205,
Middletown, DE 19709