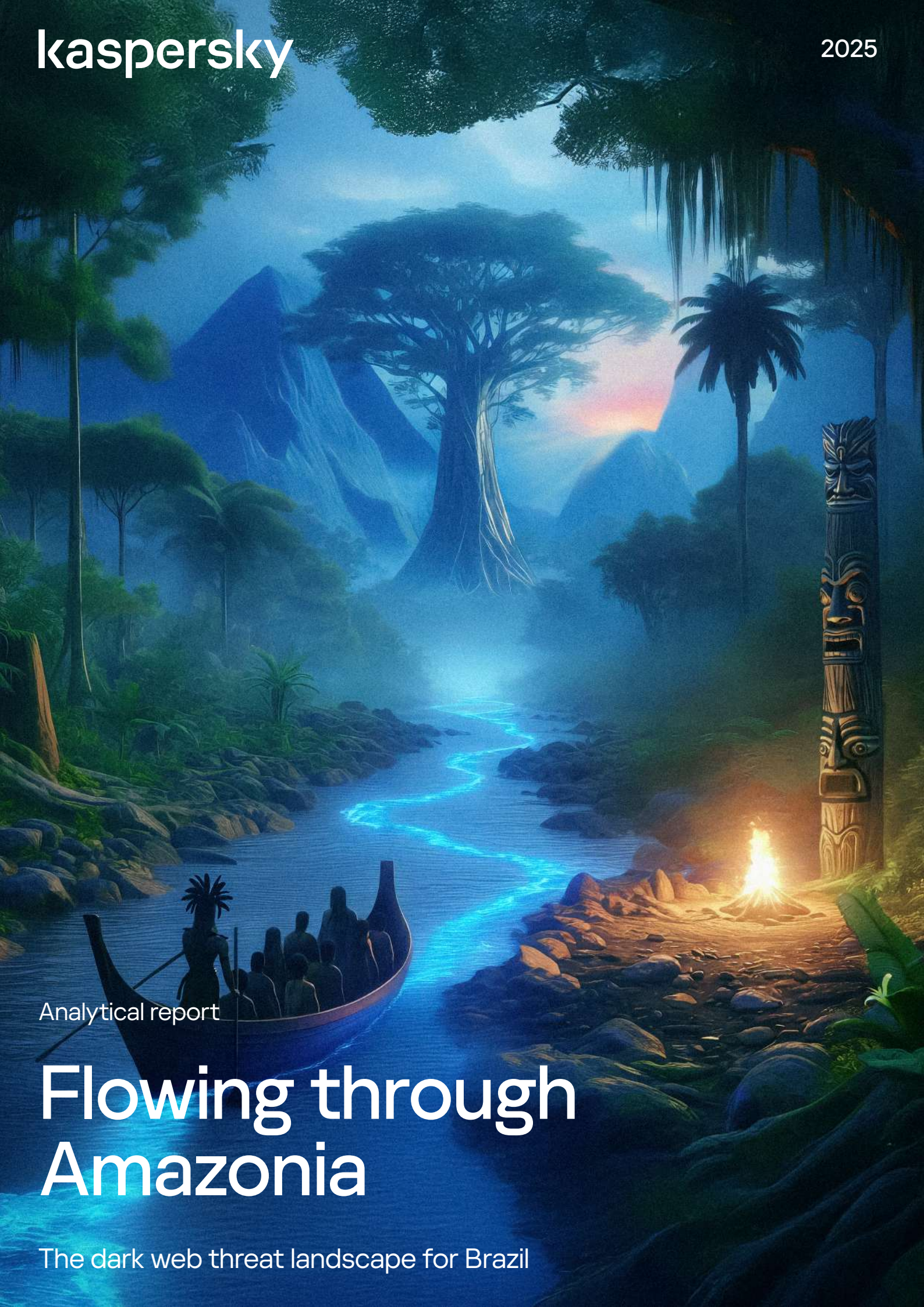
kaspersky

2025



Analytical report

Flowing through Amazonia

The dark web threat landscape for Brazil

Contents

Before the journey

Before the journey

The Kaspersky Digital Footprint Intelligence team has prepared a report that highlights the most severe and prominent dark web threats commonly faced by organizations in Brazil. Brazil was not chosen by chance — with the largest and developing economy in Latin America, vast of resources and variety of businesses, it has been a tasty target for cybercriminals for years. Our research goes beyond simply providing an overview of the dark web threat landscape — it identifies potential risks, assesses their consequences, and offers a clear protection strategy.

Today, managing the security of any IT infrastructure — whether for governments, businesses or personal devices — requires a clear understanding of current cybersecurity threats and trends. It's no secret that malicious actors, from individuals to organized groups operating in shadow markets, are constantly refining their tactics, tools and procedures. They continuously develop new attack methods for every attack phase, from initial planning and reconnaissance to gaining access and maintaining long-term persistence. These intrusions can last for years, with impacts ranging from data breaches to the complete or partial destruction of an infrastructure.

This is why it's necessary to stay informed about active actors, evolving approaches and methods, and the threat landscape in general to detect, stop or even prevent attacks and fraud at the earliest stages. With this knowledge, we believe that that this report will benefit organizations across various industries, including but not limited to:

- Government
- Professional services
- Retail
- Manufacturing
- Healthcare
- Transportation and logistics
- Telecommunications
- Consumer services and goods
- IT and software
- Finance and insurance
- Education
- Electricity, gas and oil, mining, and all other industrials
- Construction and real estate
- Agriculture
- and so on

What we explored

In total, we analyzed publications, posts and messages on all layers of the dark web, including:

- Archives of web intrusions and defaced web resources
- Public and private Telegram chats and channels
- Cybercriminal forums, both public and restricted-access
- Ransomware actors' blogs
- Shadow marketplaces for various cybercriminal activities
- Other onion resources used by cybercriminals

Diving into the treacherous river

A few words about the structure of the dark web

The dark web[1], usually refers to a hidden part of the Internet that is not indexed by search engines (such as Google). More descriptively, the dark web can be compared with a whirlpool — as you go deeper, you traverse different layers that differ mainly in how accessible they are.

The real dark web — in the depths

Fully private, unindexed resources which, as a rule, require additional checks and verification by the administrators before access is granted

Surface web — outside the whirlpool

Sites, forums, and Telegram channels accessible in the 'visible' or open web — any Internet user can access and sign up to these resources

Deep web — halfway down

Private chats and channels in messengers and resources with limited access that are not indexed and cannot be accessed from regular search engines, only by using additional tools (such as Tor)

1

What is the Deep and Dark Web?

Key dangers on the way

Our investigation uncovered the most prevalent threats facing Brazilian state institutions and businesses:

There were **30 ransomware groups** operating in Brazil. Analysis of posts published in their blogs last year shows that they executed at least 114 attacks against 105 companies, with nine organizations falling victim twice in the year. The most active gangs were RansomHub, Arcus Media, Lockbit 3.0, Quilong and Eraleign. Together, they were behind the attacks on 53% of organizations affected. As for the industries targeted, our research revealed that the top 3 were healthcare (including hospitals), financial services and professional services. Public entities also appeared in the top 10.

The market for initial access to Brazilian companies and state entities — including entry points into corporate networks and access to separate corporate devices, hosts, services or systems — is highly diverse and developed. For 2024 alone, we discovered and analyzed more than 100 ads offering access to companies in healthcare, government, construction, agriculture, and other industries. Threat actors, from individual cybercriminals to ransomware gangs and APT groups, regularly need these access points to develop their attacks.

A vast number of leaked databases (both corporate-related ones and those containing information on Brazilian individuals or companies) were discovered on the dark web. In total for the past year, cybercriminals shared or traded 309 corporate databases allegedly leaked from 185 organizations across various industries, with government agencies (16% of all breaches), telecoms and professional services firms the most affected[2].

Info stealer activity continues to rise, with data-stealing malware infections skyrocketing year on year. Our analysis of logs published by info stealer operators on the dark web in 2024 revealed 37 million records of compromised user accounts linked to Brazilian resources, 38% of which were compromised in 2024 alone. The most prevalent malware families — RedLine, Lumma and RisePro — accounted for 70% of total activity.

When it comes to specific industries, our research revealed that government, healthcare, finance and insurance were the most targeted. Previously, cybercriminals tended to avoid attacking certain 'shielded' targets, such as hospitals and other healthcare organizations due to their connection with human life. However, these unwritten rules appear to no longer apply.

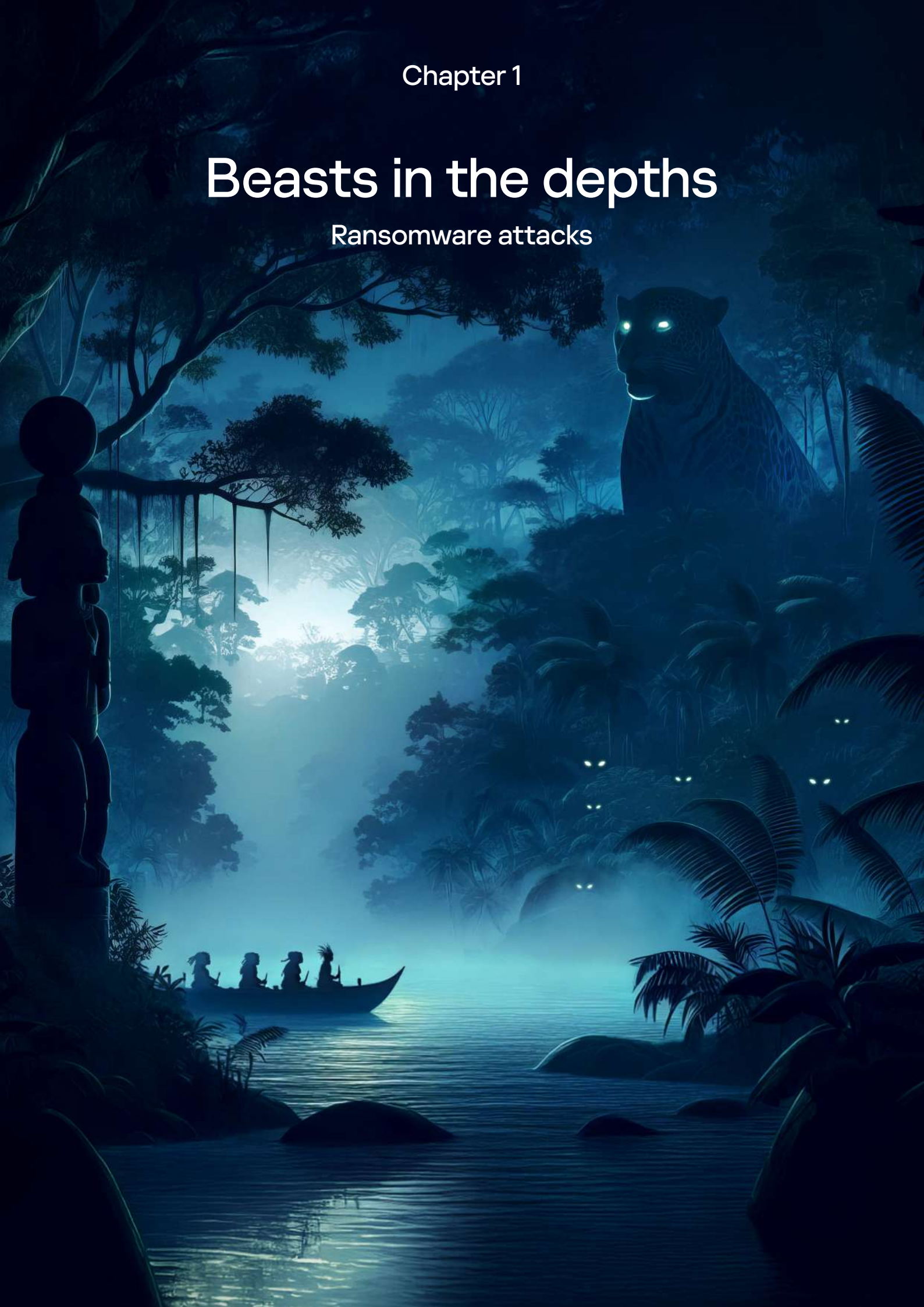
These may only be a part of the variety of threats that dark web cybercriminals pose to Brazilian organizations, but they are significant and evolving. Being aware of them is essential to strengthen defenses and proactively protect the IT environment.

2 The statistics are based on information from posts made by threat actors on the dark web. To prevent unauthorized access to the affected companies' data during the research, the compromised information was not verified in any way.

Chapter 1

Beasts in the depths

Ransomware attacks



Beasts in the depths

Ransomware attacks

Ransomware groups are expanding their activity year-to-year worldwide. Any organization in any industry can become a victim — government institutions, banks, industrials, critical infrastructure, businesses of all sizes, and even hospitals and other healthcare organizations (while healthcare was once somewhat shielded from attacks due to its life-or-death operations, the sector is now increasingly targeted in Brazil).

These days, ransomware attacks are among the most critical threats to the operational integrity and security of any company. They always lead to the most devastating consequences, including stealing of all sensitive data, which could be useful for further attacks or valuable among other cybercriminals, and full encryption of filesystems on all hosts in the victim infrastructure. So, it is essential to monitor all information security events, alerts, and incidents to detect potential attacks and defend against them before it's too late, or at least to minimize the potential damage.

We analyzed ransomware gang blogs for posts about attacks on Brazilian companies. These blogs publish information about the latest successful hacks and, if a ransom isn't paid, publish the stolen data.

Our analysis also confirms that the number of ransomware attacks in Brazil has increased year on year: In 2024, 105 Brazilian organizations suffered ransomware attacks, with nine of them falling victim twice — attacked either in different months or by different ransomware groups. In comparison, in 2023, the number of victims was 62, and in 2022, 39 (when again some were targeted several times). This shows that the number of ransomware victim organizations in Brazil has almost doubled each year.

However, it's worth mentioning that the actual number of attacks may be even higher, as some incidents might not be publicly reported in ransomware blogs.

Figure 1 | Ransomware attacks targeting Brazil in 2022 – 2024

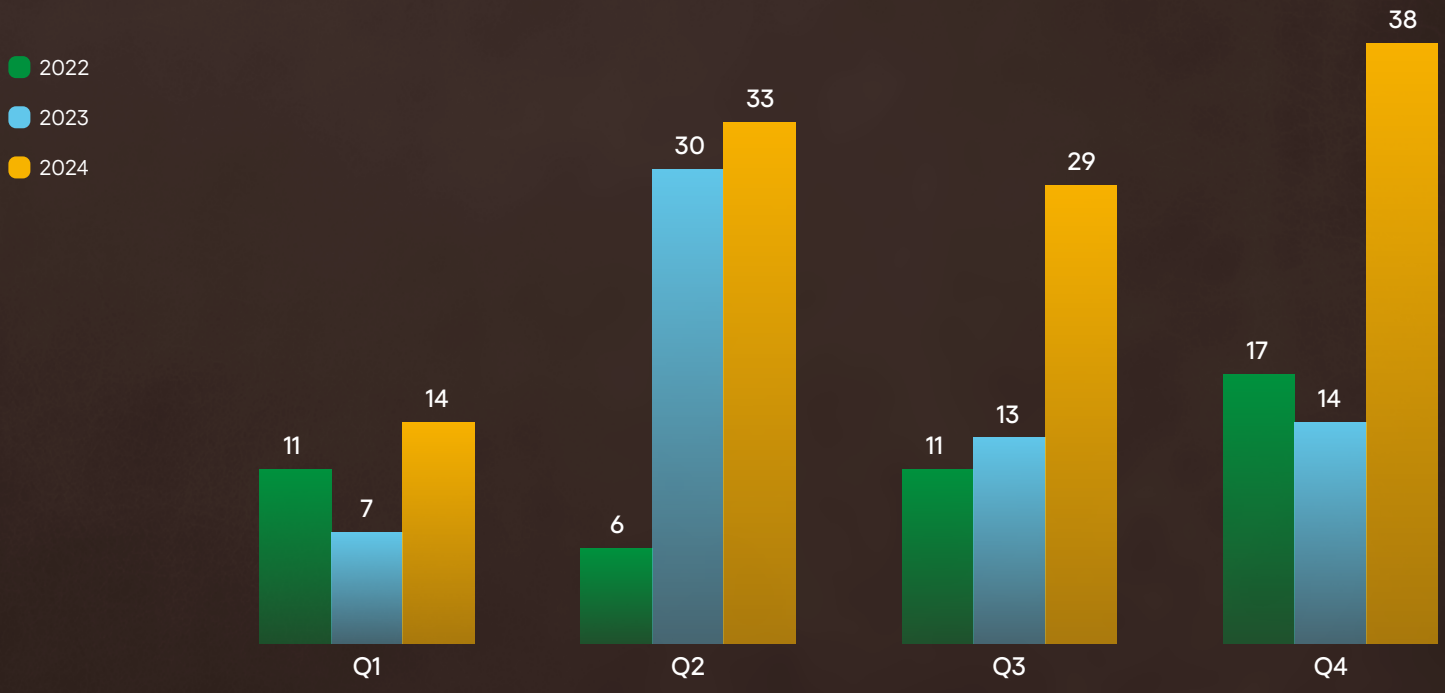
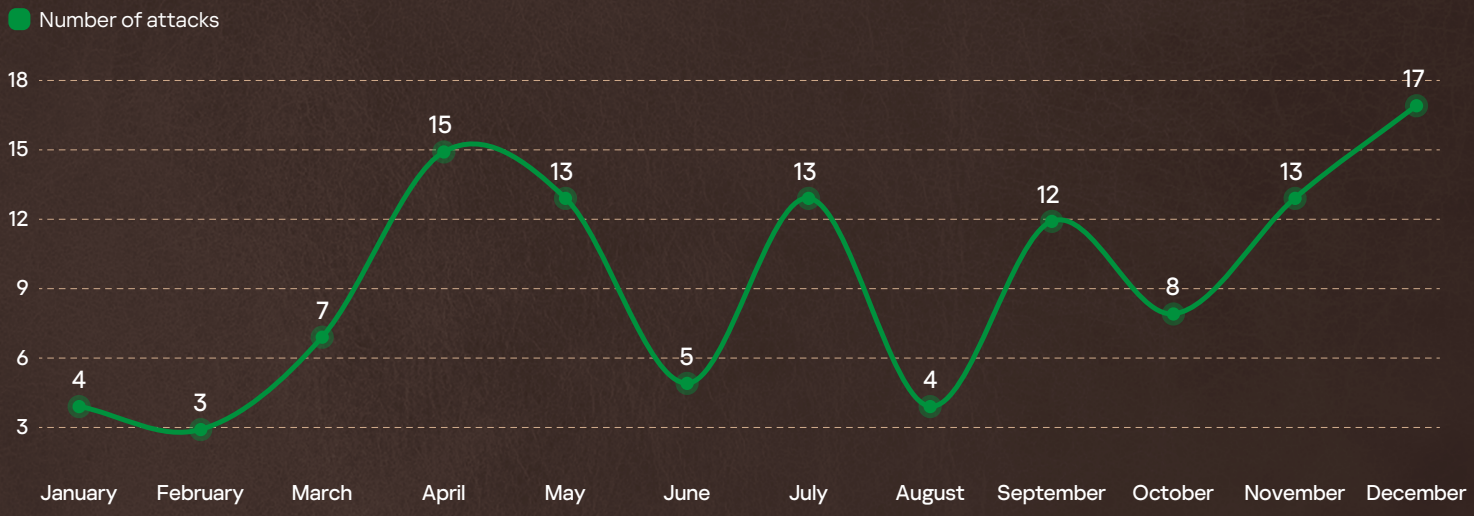
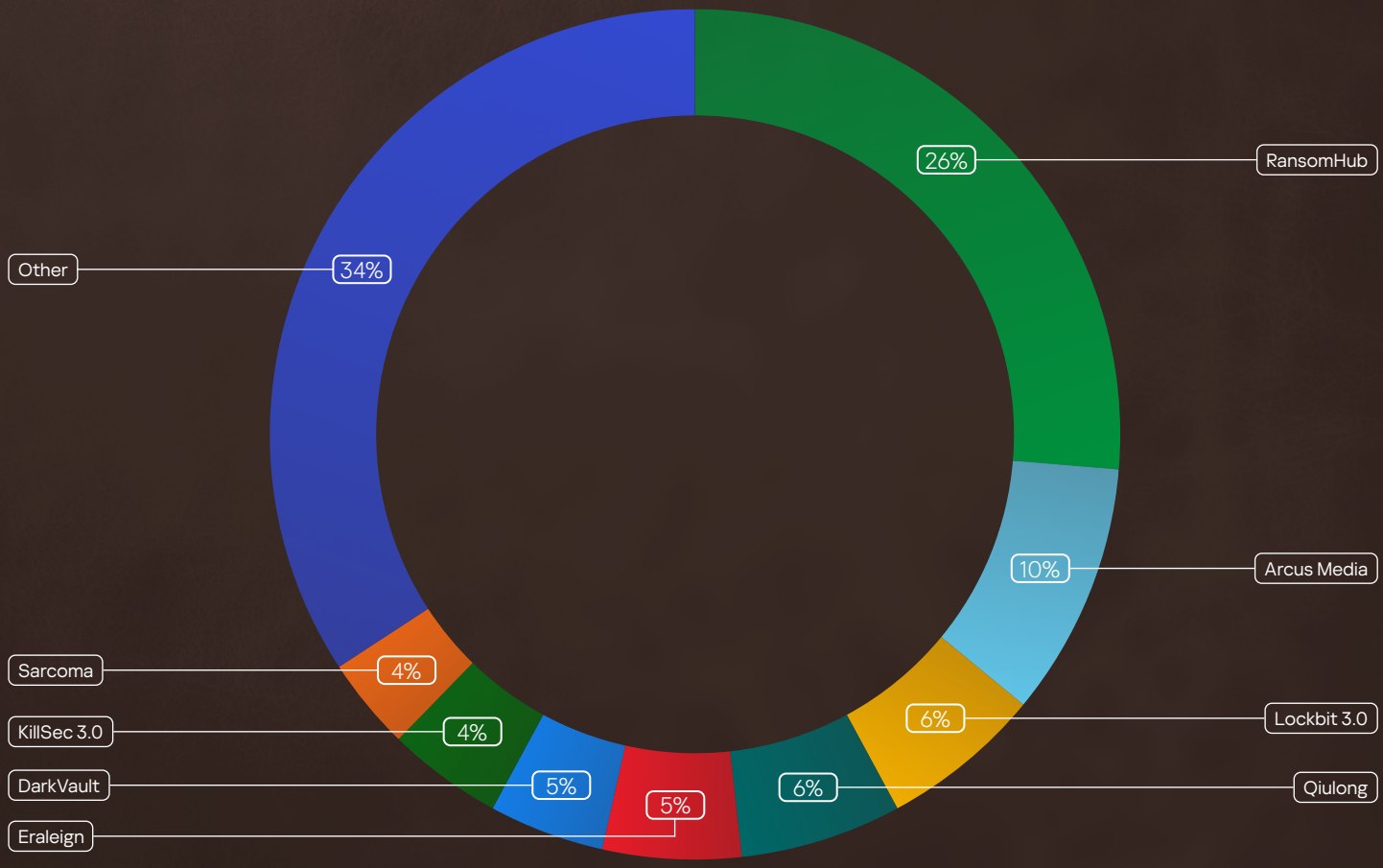


Figure 2 | Ransomware attacks targeting Brazilian organizations in 2024



A total of around 30 ransomware actors attacked Brazilian companies in 2024. The most active were RansomHub, Arcus Media, Lockbit 3.0, Quilong and Eraleign. Together, they carried out 53% of all the attacks that year.

Figure 3 | Ransomware actors targeting Brazil in 2024



A total of around 30 ransomware actors attacked Brazilian companies in 2024. The most active were RansomHub, Arcus Media, Lockbit 3.0, Quilong and Eraleign. Together, they carried out 53% of all the attacks that year.

Financial gain is the main motivation for ransomware actors, whether through ransom payments or the sale of stolen data. Attackers choose targets based on an estimation of potential earnings taking into consideration factors like a company's revenue, industry, and so on.

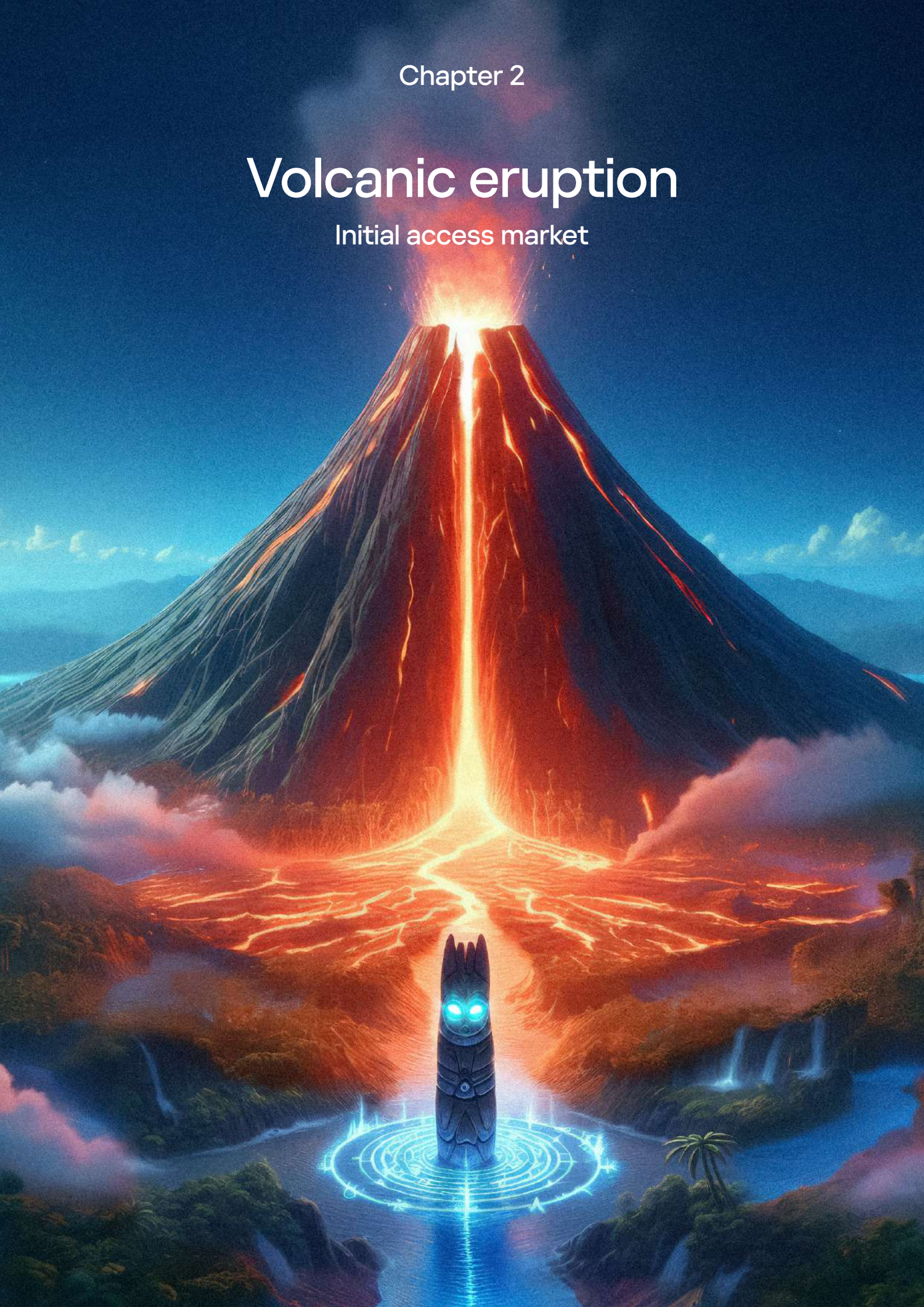
Our research shows that healthcare organizations (including hospitals) were the most attacked in 2024. The financial, retail, and construction sectors, along with professional and technical service providers (such as accounting, marketing, legal, and consulting firms), made up the rest of the top five. Notably, various government entities also ranked among the top 10 targets.

Figure 4 | Ransomware attacks in Brazil in 2024. Top-10 industries

Chapter 2

Volcanic eruption

Initial access market



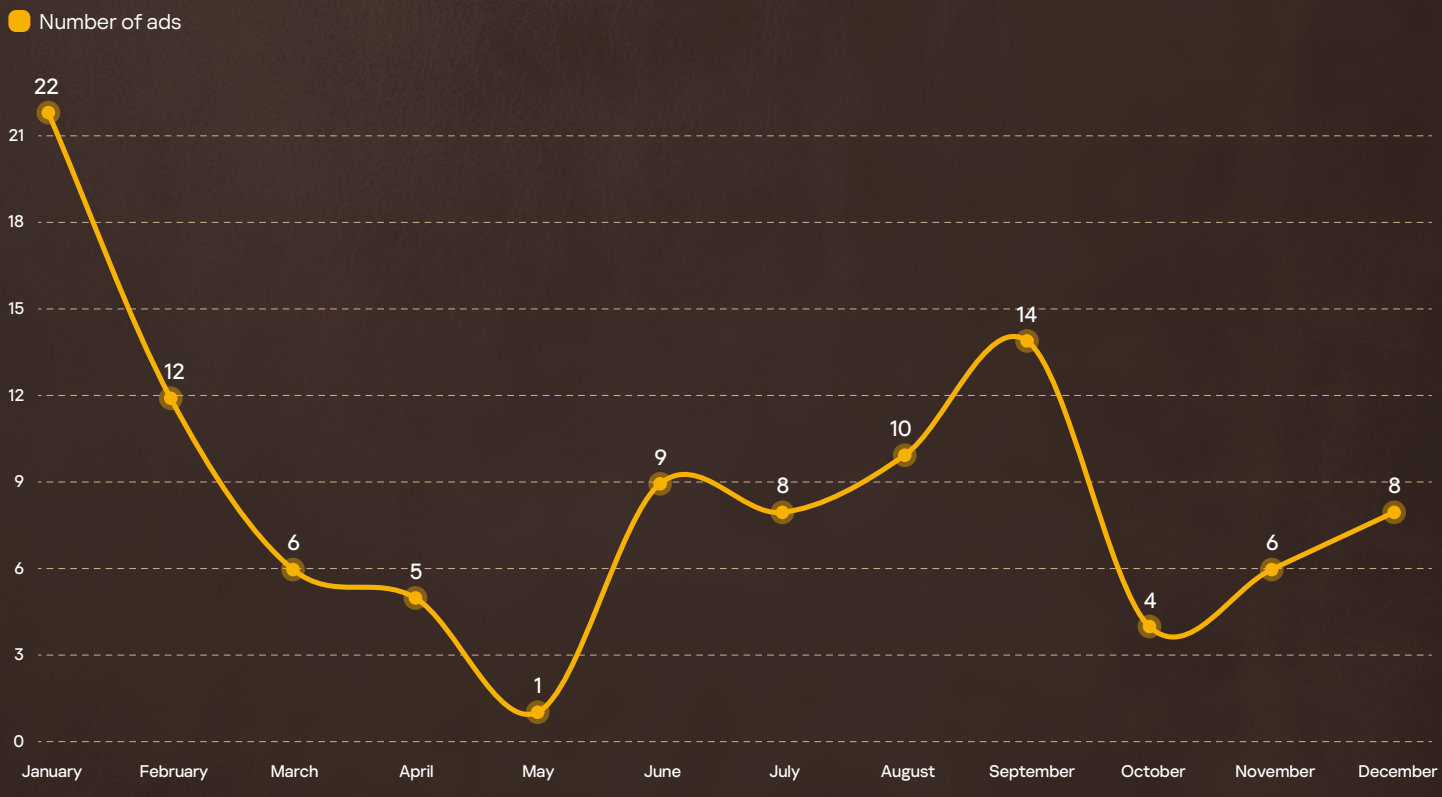
Volcanic eruption

Initial access market

Another infamous activity among the cybercrime community is the sale of initial access — attack entry points into internal networks, systems or devices belonging to various companies. Cybercriminals who obtain and sell initial access are known as initial access brokers. Typically, these brokers do not develop targeted attacks for a variety of reasons — lack of motivation, insufficient technical skills, or a believes that their role is somewhat less of a legal risk.

In total, we discovered 105 ads offering initial access to Brazilian companies and organizations. Some of these listings sell access packs, providing entry points to multiple systems, servers, devices (such as corporate VPN clients or exposed SSH services) or websites.

Figure 5 | Ads on initial access in Brazil published on the dark web in 2024



However, it's worth noting that some deals may take place without being published on dark web resources. Malicious actors, including ransomware gangs, frequently cooperate with well-known initial access brokers trusted within the community. We observe related requests from time to time.

Figure 6 | Searching for an initial access broker for cooperation in ransomware attacks

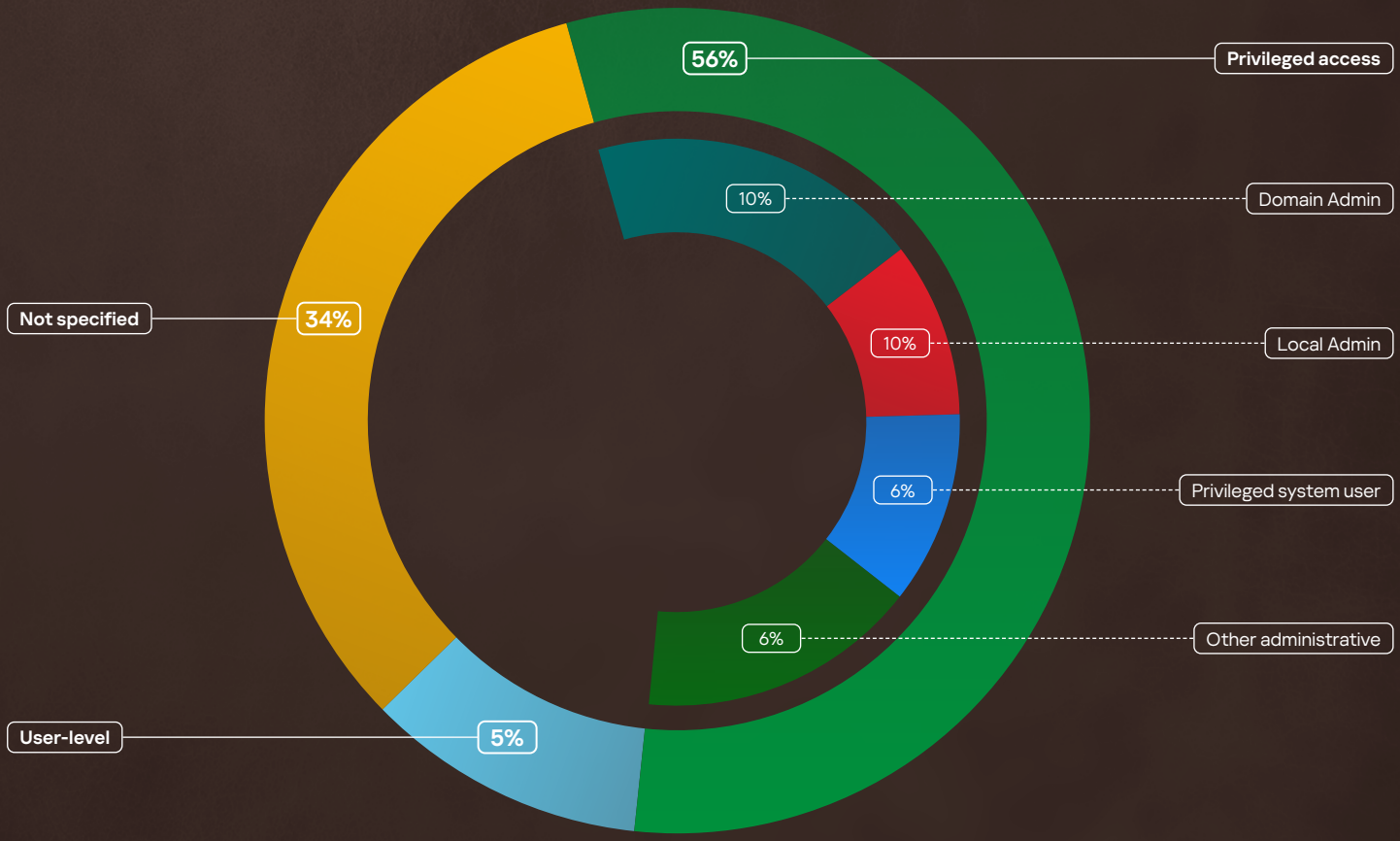
Common types of initial corporate access include:

Internal network access through a combination of valid VPN accounts to enter the corporate network, followed by remote management interfaces (e.g., RDP, SSH, or software like ScreenConnect, VNC, and AnyDesk) to access specific hosts or devices.

Access to individual corporate devices, servers, services or systems exposed to external networks (such as control panels, firewalls, databases, websites and CRM systems) using valid credentials, via shells (e.g. web or reverse), or by exploiting critical vulnerabilities like remote code execution (RCE) or SQL injection. Even if attackers fail to breach the internal network, they can still exfiltrate sensitive data from compromised victim resources.

In both cases, more privileged access commands a higher price as it enables further attack development. However, in a third of ads cybercriminals do not even specify this information.

Figure 7 | Level of initial access in Brazil traded in 2024



Information about initial access is quite sensitive for both sides — cybercriminals and the security professionals responsible for protecting enterprise, corporate and public sector IT infrastructure in the region. Cybercriminals avoid revealing explicit information in ads, that could identify targeted organizations and potentially thwart further attacks. Instead, they usually specify only general info, such as the country of the headquarters, industry, estimated revenue, number of employees, network hosts, or antivirus software in use.

To briefly summarize the initial access market in 2024, Brazilian healthcare and government organizations were among the most affected. No industry was specified for a fifth part of ads.

Figure 8 | Top 10 industries by the number of offers of initial access published on the dark web in 2024

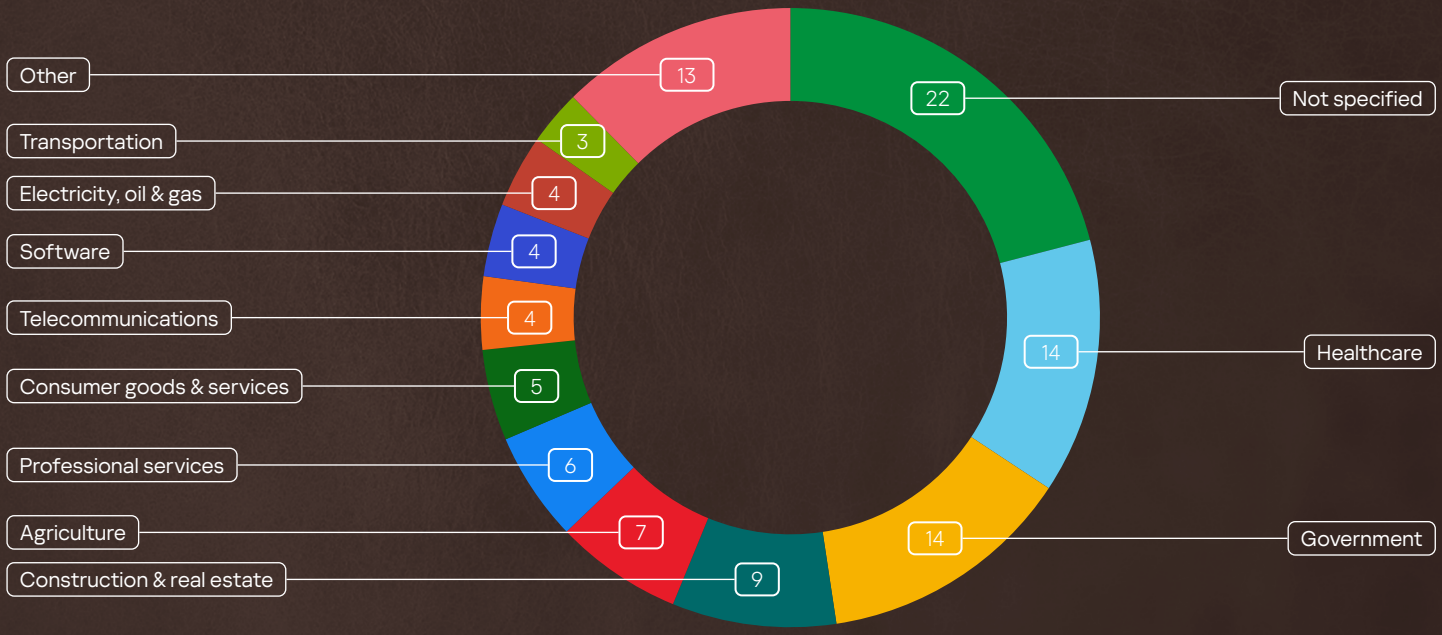
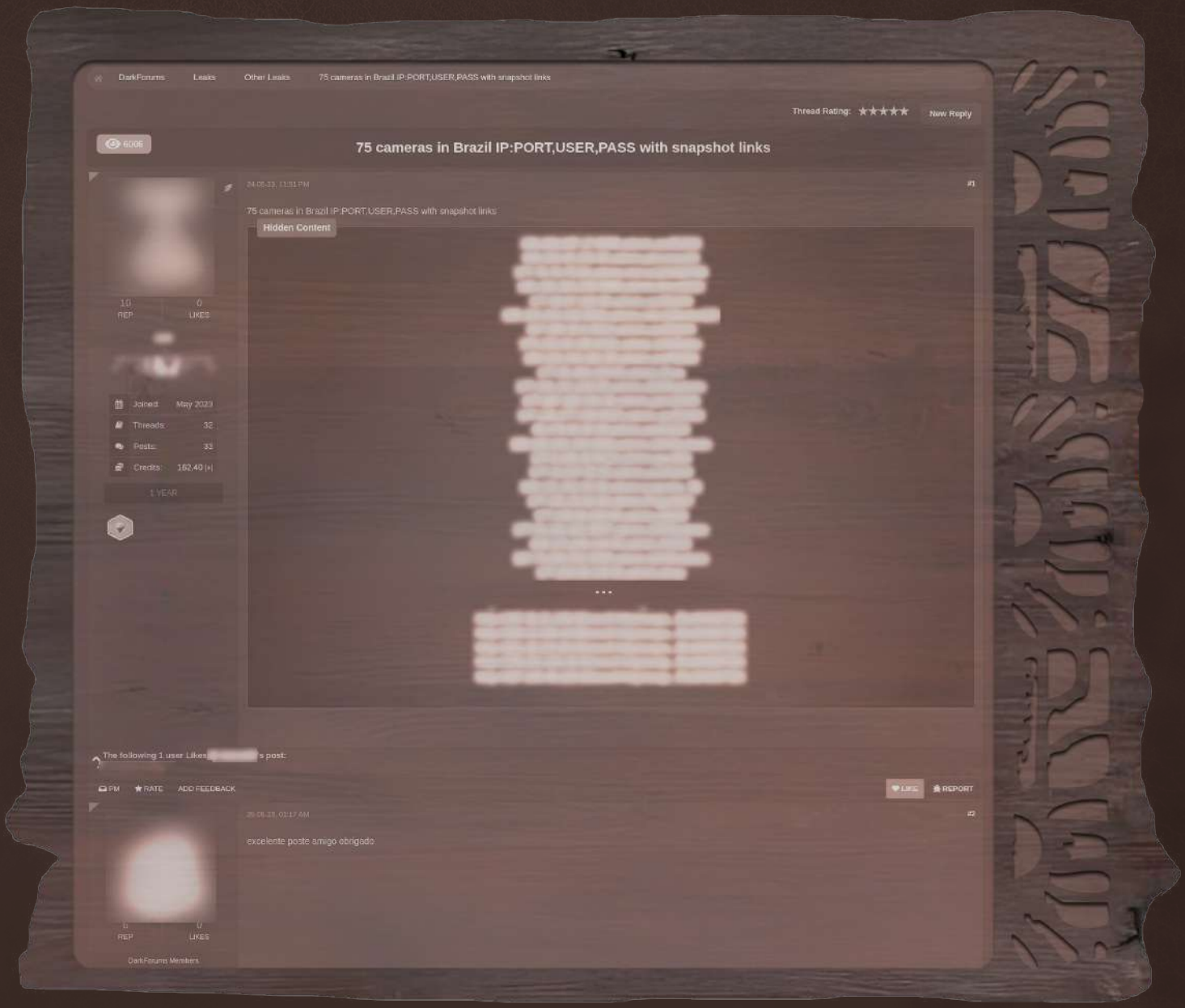


Figure 9 | Example of an ad trading initial corporate access

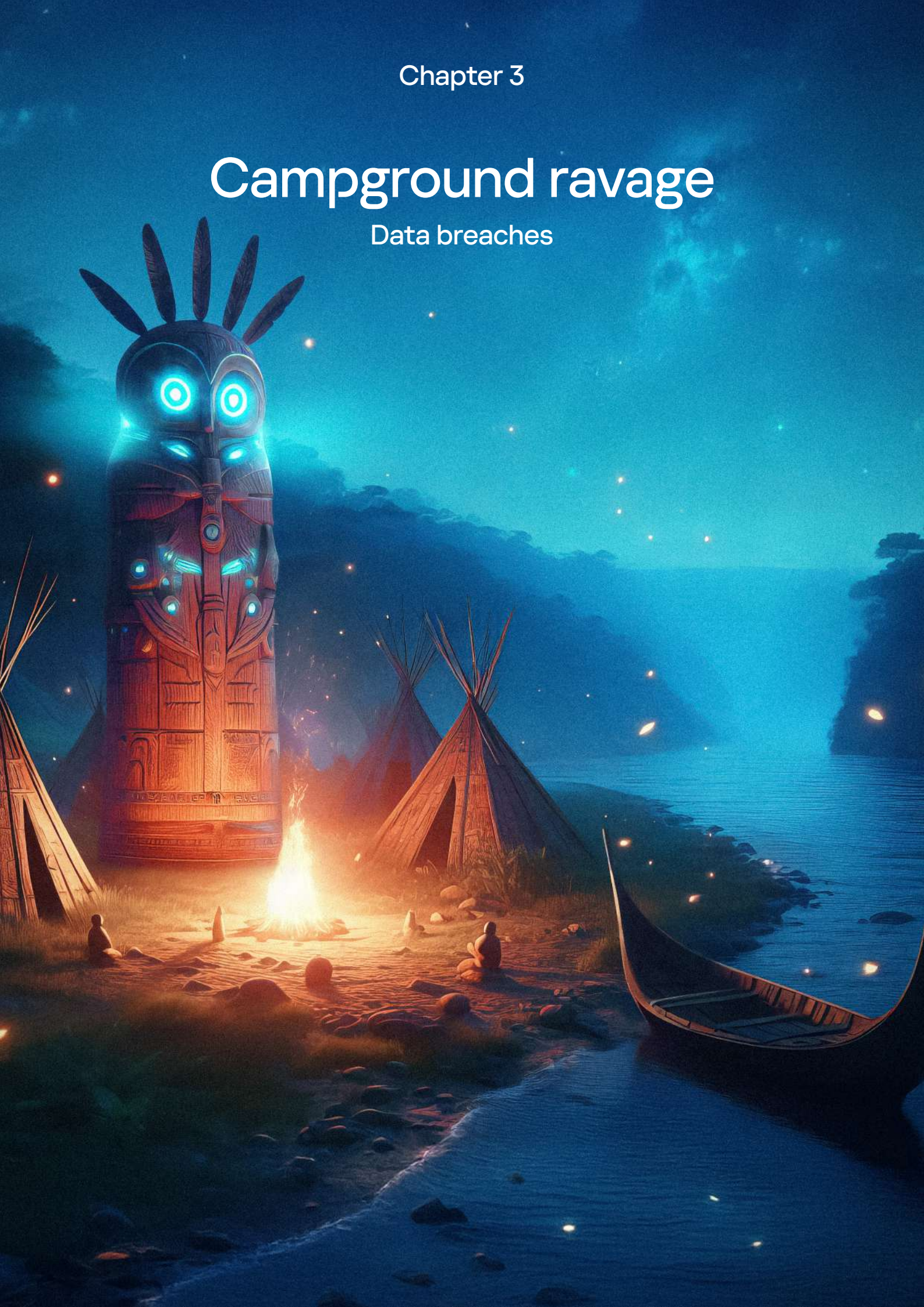
Figure 10 | Sale of access to IP cameras



Chapter 3

Campground ravage

Data breaches



Campground ravage

Data breaches

We examined dark web resources to find posts and messages related to the distribution and sales of databases, documents, lists of compromised credentials, and any other information likely to be useful to cybercriminals for further attacks. Here we can observe three main types of data on offer, according to their relevance and severity.

Data breaches

The most valuable and reliable data provides more attack opportunities — databases or documents stolen directly from organizations, their applications or systems as a result of successful intrusions, intentional activity of malicious employees — insiders or accidental leakage — by 'the human factor' (e.g. developer mistakes or insecure employee behavior).

Reposts of and combinations from previous leakages

Two main reasons for demand are:

1. Distributed database may have not been previously available for free
2. Attackers missed out on downloading the data due to short expiration time of the links to the shared files, usually set after publication

Combo and target lists

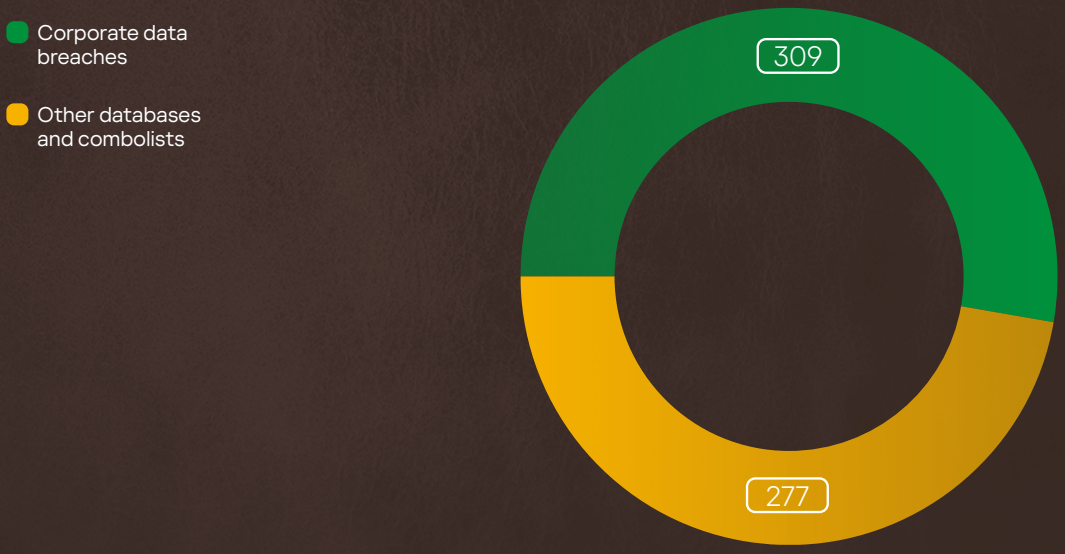
Specially crafted databases with info on specific groups of victims — by citizenship, residence, level of income, type of property, sector of work, etc. This data is less valued but commonly used for phishing and other fraud targeted at particular victim groups.

It's worth mentioning that data or document leaks pose more than just cybersecurity and reputations risks for the affected company — they also increase the risk of future attacks on staff, partners, customers, clients, any other affiliated individuals or organizations. Cybercriminals use breaches to commit a huge range of fraud: from simple spam and phishing to targeted attacks using victim profiling, supply-chain attacks and blackmailing of high-ranking employees.

For the whole of 2024, we observed 586 ads in various dark web forums offering data breaches or other databases containing information on Brazilian organizations, public entities, citizens or users. According to the descriptions, more than a half (53%) came from corporate data breaches affecting 185 companies or state institutions (Some databases were republished several times during the year)[3].

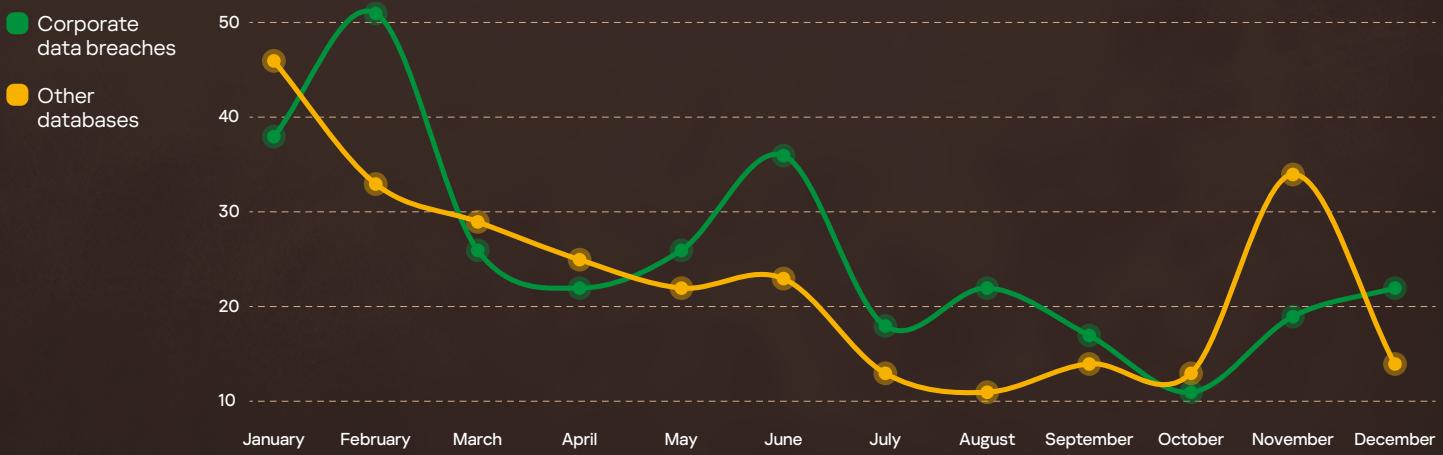
Other databases contained information on individual citizen — here we observed several unspecified databases with personal information as well as mixed or targeted lists combined in different ways. This substantial rate of general databases (47%) indicates broad, non-targeted cybercriminal activity in Brazil is at a high level.

Figure 11 | Types of databases distributed on the dark web in 2024



On average, there were 49 posts per month, with 25.5 of those related to corporate data breaches. Incidentally, at the beginning of the year, there were more posts offering databases related to Brazilian citizens or organizations, although overall activity remained relatively stable throughout the year, with a slight dip in the third quarter.

Figure 12 | Ads offering Brazil-related databases in 2024



3 The statistics are based on information from posts made by threat actors on the dark web. To prevent unauthorized access to the affected companies' data during the research, the compromised information was not verified in any way.

When it comes to corporate data breaches, we observed that public institutions, including different regional administrations, were the most affected. Government-related databases accounted for 16% of all ads in this category. Telecommunications organizations and professional services companies rounded out the top 3. It's also worth noting the trend of attacks on medical organizations, including hospitals. As mentioned in the ransomware overview, healthcare organizations are also represented in the top 10 most targeted sectors.

Figure 13 | Distribution of corporate data breaches in Brazil in 2024. Top-10 industries

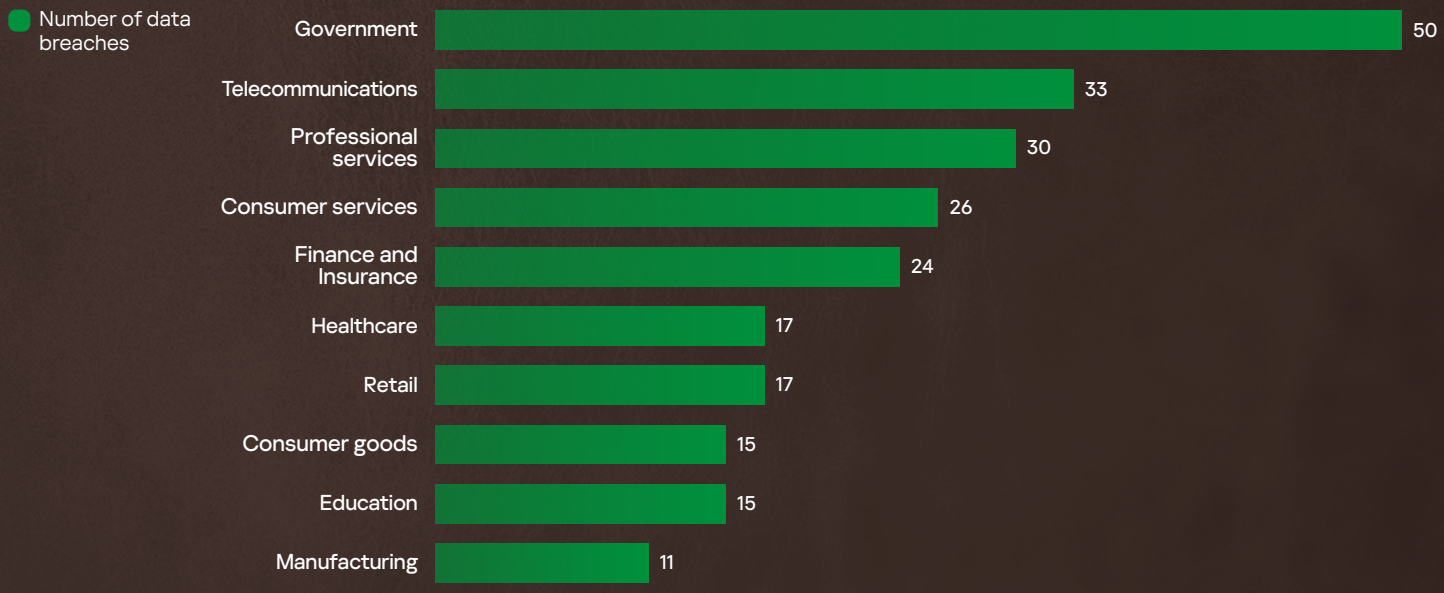
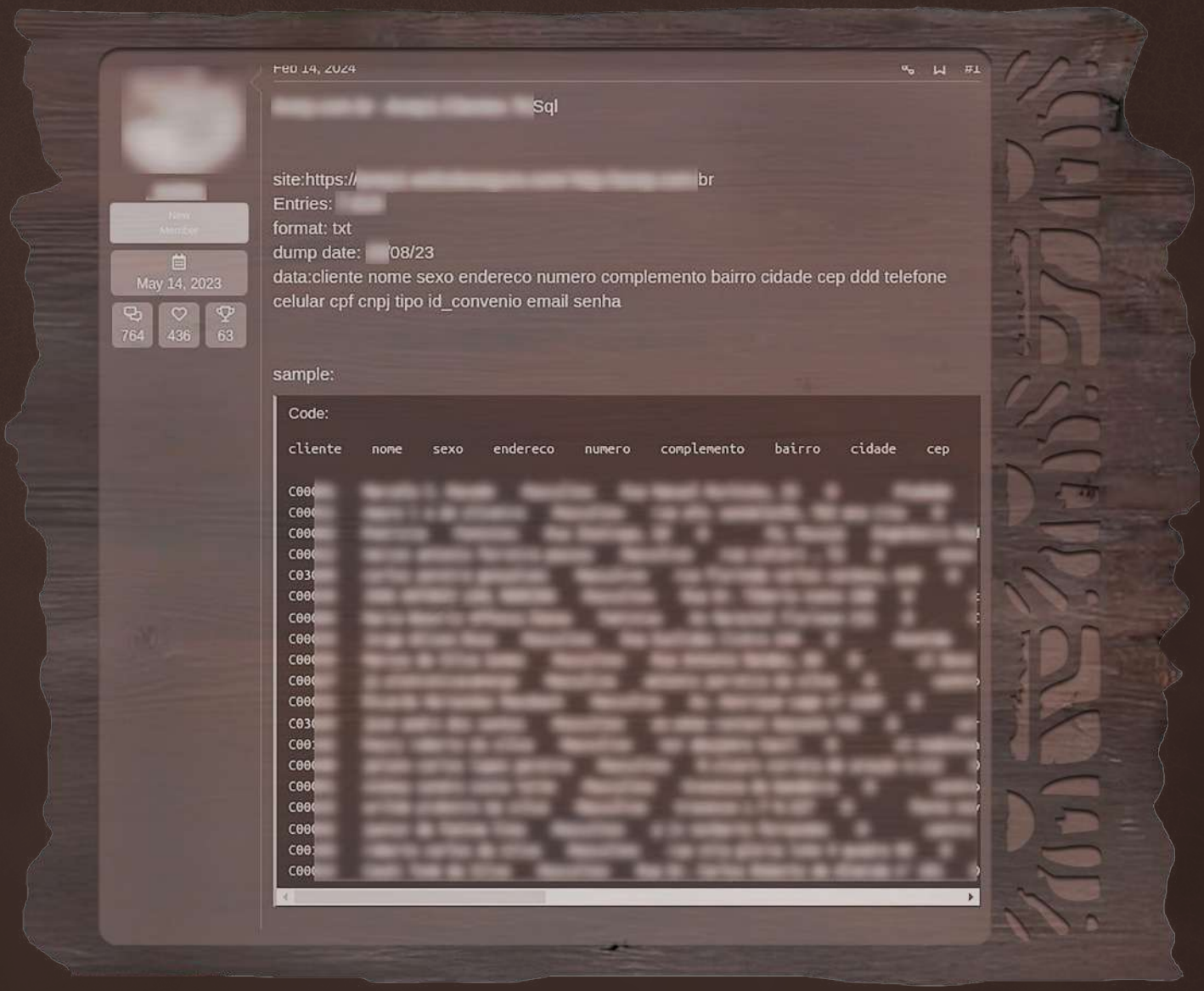


Figure 14 | Example of an ad on Telegram sharing data leaked from a government resource (source — the Threat Lookup service of the Kaspersky Threat Intelligence portal)

Figure 15 | Example of an ad on a dark web forum sharing a corporate data breach



Chapter 4

Ubiquitous and dreadful piranhas

Activity of info stealers

Ubiquitous and dreadful piranhas

Activity of info stealers

Each year, millions of devices worldwide are compromised by various types of malware designed to covertly steal sensitive and confidential data. Depending on their functionality, these programs collect information stored on the device (such as browser history and stored passwords), intercept inputted data, including user credentials, banking card details or e-wallets, gather cookies, tokens, API keys, take screenshots and so on.

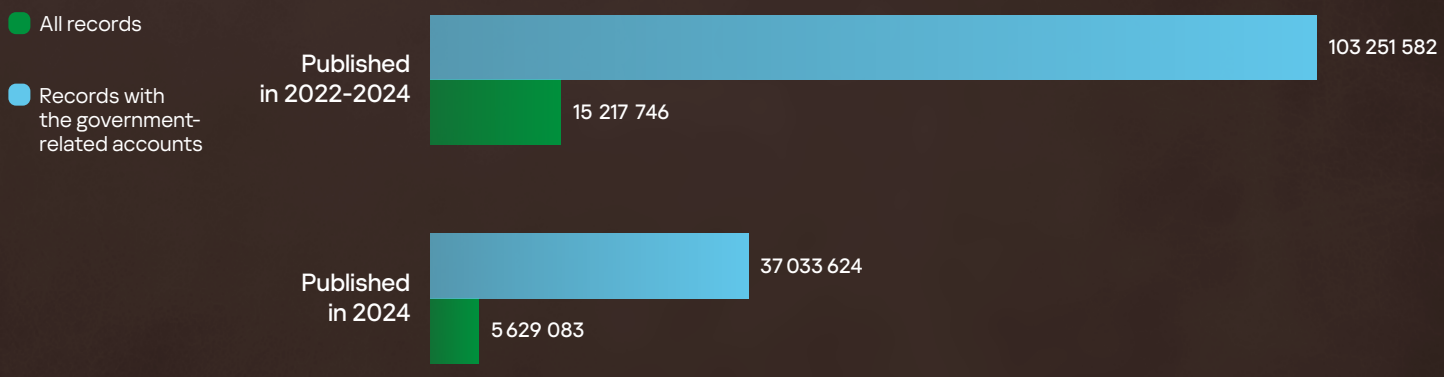
All the stolen data is assembled into log files and sent to control servers managed by malware operators. In fact, there is a delay between when the information is stolen and when it appears on the dark web. It is common to see data leaked in 2022 or earlier only surface in logs published in 2024. This is because malware operators first analyze the retrieved information to extract anything particularly useful for their activities — such as valid accounts for corporate systems and services, financial data — before selling or sharing the logs among other cybercriminals via darknet markets or other dark web channels.

We analyzed info stealer logs to identify records containing compromised accounts related to Brazilian regional top-level domain (.br). The total number of such records published in malware logs over the last four years is more than 103 million — with over a third (about 37 million lines) published in 2024 alone.

We also prepared a detailed research report, "Data-Stealing Storm" in which we explored the dark web market for compromised credentials published on info stealer logs in 2024. This follows our previous report analyzing data from info stealer logs published from 2021 to 2023. Among other findings, the analysis reveals that Brazilian resources led in info stealer infections in 2023.

A special analysis of the records from major government entities shows that 15% of all records in logs — representing 5.6 million lines published in 2024 and over 15 million across the last three years — contain accounts belonging to employees of major Brazilian state agencies or those used to access various government services for citizens and corporations.

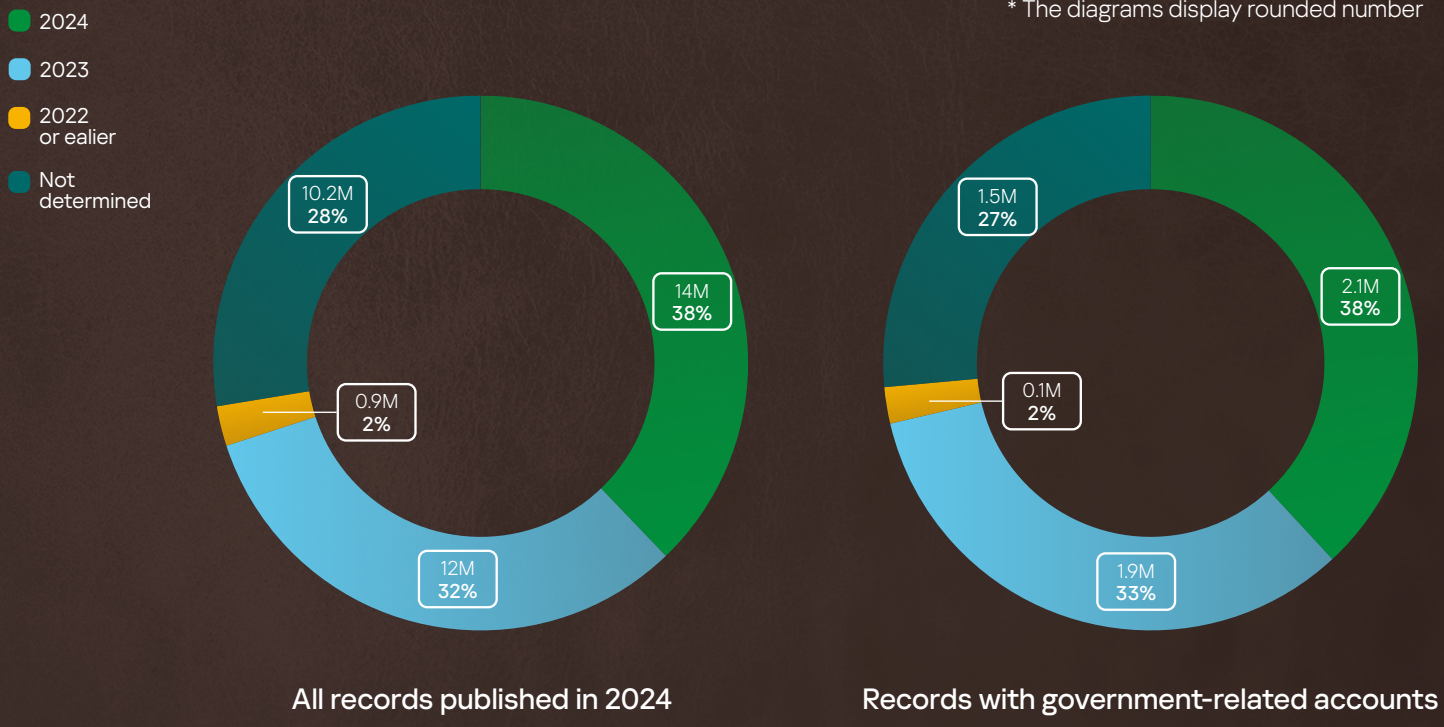
Figure 16 | Records from info stealer logs. General statistics



The following diagrams show that 38% of all records published in malware logs in 2024 contain accounts that were leaked that year, while one-third are from 2023, and a smaller portion dating back to 2022, 2021, or earlier.

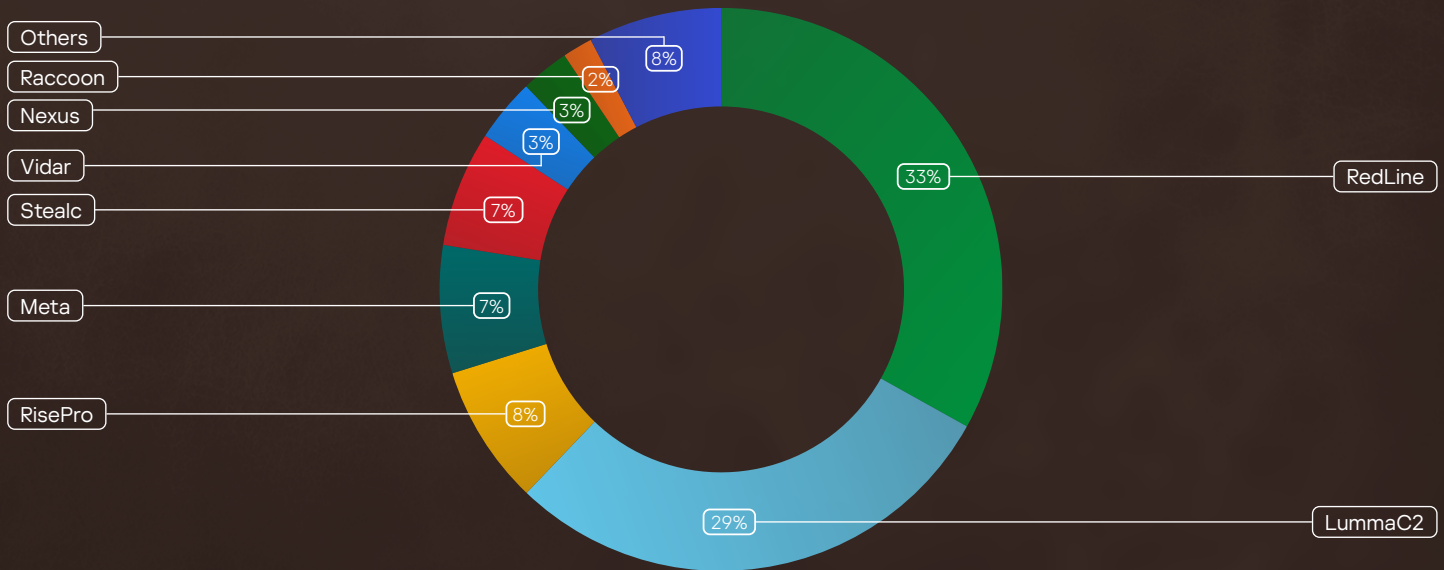
Figure 17 | Statistics on years of accounts compromise. Records published in 2024*

* The diagrams display rounded number



More than 60% of all info stealer activity in Brazil involves RedLine and LummaC2 (or just Lumma) malware. RisePro, Meta (an “improved” version of RedLine that emerged in 2022), and Stealc also rank in the top-5 based on the number of compromised accounts published in the dark web in 2024.

Figure 18 | Info stealers activity in Brazil in 2024



Journey outcomes

Journey outcomes

The entire threat landscape posed by dark web cybercriminals to Brazilian businesses and public institutions cannot be fully covered in a single report, as activities vary widely across sectors and have evolved significantly in recent years. Among other factors, wider implementation and constant development of malware-as-a-service and ransomware-as-a-service models have driven a sharp increase in related malicious activity and attacks. These models enable a broader range of cybercriminals without advanced technical skills to carry out attacks on more and more targets.

Brazil is increasingly in the crosshairs of cybercriminals more so than many other countries for a variety of reasons, including its large population, economic growth and diverse business landscape. The volume of attacks and cybercrime activity in general is intense. As such, there is a need to support economic growth in the region by strengthening IT and cybersecurity. In this way, governments, enterprises and other organizations can safeguard themselves from ever-evolving cyberattacks and threats emerging from the dark web.

It is therefore increasingly important to take a proactive and rapid approach to defending against cyberthreats, attacks and other cybersecurity incidents — in other words, to stay one step ahead of potential adversaries. This is undoubtedly challenging, but crucial. We recommend a clear protection strategy to secure corporate IT infrastructure and digital environments.

To inquire about threat monitoring services for your organization, please contact us via the **Kaspersky Digital Footprint Intelligence** website or directly at dfi@kaspersky.com.

Digital Footprint Intelligence

If you are already facing an incident, our **Kaspersky Incident Response** service will help you respond and minimize the consequences, particularly by identifying compromised nodes and protecting your infrastructure from similar attacks in the future.

Incident Response

To uncover hidden cyberattacks or ensure that your environment has not been penetrated, consider our **Kaspersky Compromise Assessment** service.

Compromise Assessment

If you plan to evaluate and improve the security posture of your organization, a **Kaspersky Security Assessment** includes a variety of services, including penetration tests and red teaming.

Security Assessment

Protection strategy

IT asset inventory and patch management

Primarily, identify all assets you need to protect, implement regular software updates and ensure that attackers do not have opportunities to exploit known vulnerabilities.

Comprehensive security solutions

Use multi-layered security controls across all components of your network infrastructure to gain better visibility across your environment and enable timely detection and prevention of various types of attacks.

Maintain security awareness among staff

Regardless of the security controls used, the human factor remains one of the most serious and common vulnerabilities leading to security breaches.

Continuously monitoring and assessment

Closely monitor all devices, servers, systems, services, applications, and traffic for any suspicious activity — early detection of a malicious activity is key.

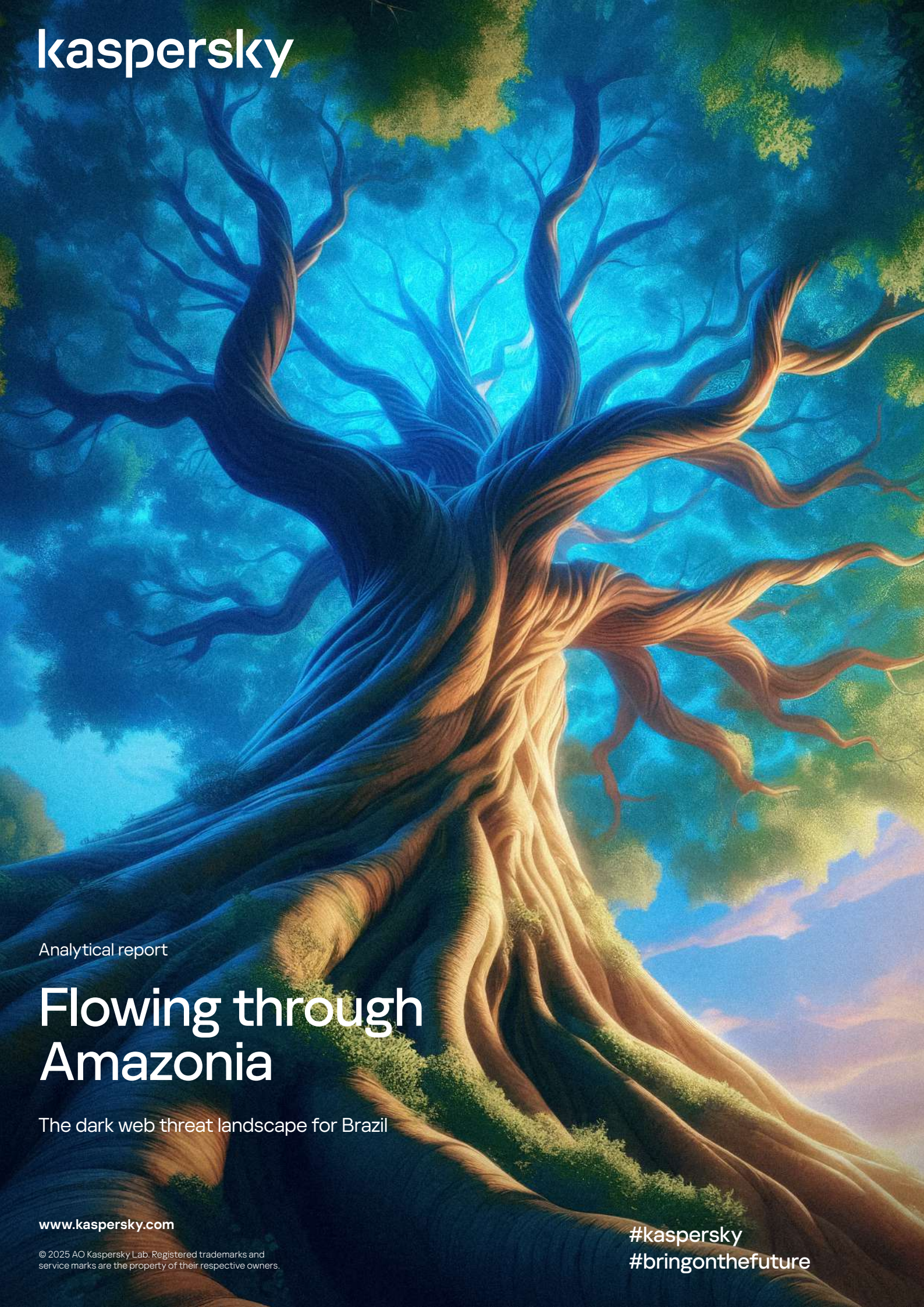
Up-to-date Threat Intelligence (TI)

Regularly review TI data to understand the latest tactics, techniques, and procedures used by attackers, and tailor your defenses accordingly.

The dark web monitoring

Stay informed about potential attack vectors, cybercriminal interests and plans, and emerging threats. Knowledge is power — it strengthens your defenses and enables proactive, timely reactive responses.

kaspersky



Analytical report

Flowing through Amazonia

The dark web threat landscape for Brazil

www.kaspersky.com

© 2025 AO Kaspersky Lab. Registered trademarks and service marks are the property of their respective owners.

#kaspersky
#bringonthefuture