BRANDEFENSE COUNTRY REPORT · BRAZIL 2026

Brandefense Brazil: Cyber Threat Landscape Report 2026

Identity, payment authority and service continuity in a connected economy

Odin by Brandefense
Research window: 1 January–22 November 2026
Version 1.0 · Public Research Edition · TLP:CLEAR · 8–22 November 2026

131 of 250
selected domains had an associated credential advertised for sale when checked

10
selected claim cases with authentic, redacted post excerpts

206
Brazil-associated ransomware listings during the reporting window

30 / 60 / 90
days for validation, exercised controls and management review

CONTENTS

Contents

01	Executive summary	05
	Report map	10
02	Brazil's digital and operating context	11
03	National exposure: a selected 250-domain portfolio	15
04	Dark-web activity: from an advertisement to an owned decision	22
05	Incidents and targeting by sector	38
06	Disruption, defacement and public-service trust	56
07	Ransomware, financially motivated groups and espionage	62
08	Fraud, personal data and payment-card material	77
09	Banking and payments: protect the authority to act	83
10	Regulatory and national response	90
11	Outlook and conditional planning	95
12	Action plan	99
A	Appendix A. Scope and evidence boundaries	106
B	Appendix B. Evidence register	111
C	Appendix C. Sources	116
D	Appendix D. Glossary	121

Board and executives	01 05 11 12
CISO and security leads	03 04 05 07 12
SOC, endpoint and identity	04 06 07 B
Payments, fraud and customer protection	05 08 09
Legal and communications	05 06 10 12

About this edition

Prepared with AI assistance. Evidence, attribution and limitations are stated beside the findings.

Brazil's evidence connects copied registration records, advertised access, payment fraud and administrative recovery. The priority is to validate the affected authority and protect the essential service and its users.

206

Brazil-associated ransomware listings; claims, not confirmed intrusions

80/100 (F)

national Atlas headline for the selected 250-domain portfolio

26

evidence cases; ten claims and sixteen disclosure or investigation cases

4

decisions for leaders, each linked to completion evidence

Contents and reading routes

Chapter	Question
1 Executive summary	Which decisions should come first?
2 Brazil's context	Which operating conditions shape the response?
3 National exposure	What does the selected portfolio establish?
4 Dark-web activity	What do the advertisements actually say?
5 Incidents by sector	What did organisations and authorities report?
6 Disruption and trust	Was a service unavailable, altered or merely named?
7 Actors and campaigns	Which labels and relationships have supporting evidence?
8 Fraud and personal data	How can information enable another harmful request?
9 Banking and payments	Who controls the authority to act?
10 Regulation	Which entity, trigger and communication route apply?
11 Outlook	Which conditional scenarios justify preparation?
12 Action plan	Who acts, and what demonstrates completion?
Appendices A–D	Scope, evidence register, sources and plain definitions

CHAPTER 01

Executive summary

01

THIS CHAPTER ANSWERS

Which findings justify immediate decisions for Brazilian organisations?

206

ransomware listings, each recording an extortion assertion

Six findings 06

Four decisions for leaders 07

The year in numbers 07

What remains unavailable 08

CHAPTER 01

Executive summary

IN SHORT

Brazil's evidence supports four priorities: validate identities, protect payment authority, involve suppliers and test continuity. Public notices describe registration-data copying, altered payment instructions and administrative recovery. Ransompedia records 206 Brazil-associated listings across 55 group labels. Technical research separately describes banking malware, payment-identity theft and attributed espionage. These are different populations, with no national attack total. Assign accountable owners to current access, customer protection, minimum service and reporting decisions.

This report combines Brandefense Blackhole observations, Ransompedia listings, Atlas exposure results for a selected domain portfolio and verified public reporting. Posts, advertisements, listings, public cases and record associations are separate units. They are never added into a national attack count. [S1][S2][S3][S4]

The requested cut-off is 22 November. Evidence reflects what was available when reviewed that day, while the day was still in progress. The closing fortnight appears separately in §5.7. Publication, incident, discovery and recovery dates remain distinct.

Six findings

1. Extortion visibility is spread across many labels. Ransompedia records 206 Brazil-associated listings in the window, compared with 160 in the full year 2025. Thegentlemen, Lockbit5 and INC Ransom account for 72, or 35.0%, of the current-window total. The remaining 134 belong to 52 labels. This is not a matched-period annual growth rate or confirmation of encryption. [S2]

2. Registration exposure requires a customer response of its own. CVP confirms copied registration data in a database including all 7.6 million active customers, as well as former customers. Treasury identifies approximately 30,000 service registrations and a separate base with approximately 4,000 Pix keys. Neither supports an added national unique-person total or an automatic payment-access inference. [S126][S127]

3. Payment integrity can fail within an otherwise genuine workflow. Belo Horizonte says some guides issued during 14–16 November carried altered payment information. About 250 taxpayers paid affected guides. The municipality says funds were blocked and refunds began on 17 November. The notice establishes neither complete refunds nor a national Pix infrastructure intrusion. [S233][S234]

4. Administrative recovery and physical operations need separate tests. Santos describes a 6 November systems incident and staged recovery. APS states that cargo capacity and access were maintained, while wider reporting describes slower administrative handling. Those statements concern different measures. Test the essential user task, its fallback and later reconciliation. [S128][S229][S228]

5. An access advertisement needs validation before disruptive containment. The selected posts claim financial leads, education records, municipal data and payment-related access. A November Pix advertisement explicitly calls its material 2025 data. A February virtual-assistant narrative has an inconsistent date range. These details justify scrutiny, not a declaration of fresh intrusion. [S1]

6. Actor research supports several distinct control questions. Google's payment research, Elastic's banking-malware account and IBM's browser-session research support separate identity and endpoint controls. Kaspersky includes Brazil in an information-theft and espionage campaign, attributed to Armored Likho with medium confidence. None establishes a common operator across this report's cases. [S18][S19][S20][S161]

Four decisions for leaders

1. **Validate identity and access evidence.** Assign each relevant lead to an owned service, establish account status and privileges, and record the containment or closure decision. Historical records require a different response from active unsafe access (§3–4, §12).
2. **Protect transactional authority.** Map payment-signing identities, provider permissions and beneficiary-change approval. Demonstrate revocation and independent verification using synthetic transactions (§5, §9, §12).
3. **Bring suppliers and customer protection into the same response.** Identify the controller, service owner, affected categories and trusted support route. Rehearse a supplier notice with incomplete facts (§5, §8, §10).
4. **Test minimum service and reporting together.** Demonstrate a fallback, reconcile its records and preserve the awareness chronology for each applicable notification route (§6, §10, §12).

The year in numbers

206

Brazil-associated Ransompedia listings in the 2026 window

WHAT IT DOES NOT MEASURE

Confirmed intrusions, encryption or payment

160

Brazil-associated listings for all of 2025

WHAT IT DOES NOT MEASURE

A matched-period baseline

55

Group labels represented in the current-window listings

WHAT IT DOES NOT MEASURE

Unique operators or criminal organisations

72 of 206

Listings under the three leading labels, 35.0%

WHAT IT DOES NOT MEASURE

Their share of all Brazilian incidents

102 / 41 / 74 / 108

Current-window listings for Argentina / Chile / Colombia / Mexico

WHAT IT DOES NOT MEASURE

Population-adjusted risk or national security performance

250

Assessed primary domains across ten sector groups

WHAT IT DOES NOT MEASURE

Independent legal entities or national exposure prevalence

80/100 (F)

National Atlas headline for the selected portfolio

WHAT IT DOES NOT MEASURE

A breach percentage, intrusion probability or sector ranking

131 of 250

Selected domains with an associated credential advertised for sale when checked

WHAT IT DOES NOT MEASURE

Tested access, completed sales or confirmed intrusions

26

Report cases: ten claims and sixteen disclosure or investigation cases

WHAT IT DOES NOT MEASURE

Twenty-six confirmed intrusions

7.6 million

CVP's active-customer population included in the affected base

WHAT IT DOES NOT MEASURE

Total unique people, including former customers

About 30,000 / 4,000

Treasury service registrations / Pix keys in separate bases

WHAT IT DOES NOT MEASURE

A combined count of unique people or authorised transfers

About 250

Taxpayers reported to have paid altered municipal guides

WHAT IT DOES NOT MEASURE

Every taxpayer or every municipal payment

Comparison countries were selected as examples to provide context only; they do not imply a ranking or political assessment.

Sources: own observations [S1][S2][S3], official notices [S126][S127][S233] and their cited scope. Payment-card aggregates are discussed only with their narrow scope in §8.2.

What remains unavailable

Atlas provides a national headline of 80/100 (F) for the selected portfolio. No complete passive-hygiene dataset or hygiene index is available. Missing control observations are not failed controls. Sector ratings and national control-prevalence estimates are not published. [S3]

Several original notices and official archive segments remain unresolved. The report does not claim exhaustive national incident coverage. It also makes no finding about election integrity or political responsibility from a website claim, a party-related dataset offer or a source's rhetoric.

KEY TAKEAWAYS

01

Keep listings, posts, official cases and record populations separate.

02

Validate the authority involved before deciding containment or customer action.

03

Exercise payment integrity, supplier notification and minimum service with accountable owners.

Report map

Twelve chapters, five reader paths. Follow the decision that belongs to your role; the evidence limits travel with every finding.

Board and executives	Fund the response and test critical dependencies	01 05 11 12
CISO and security leads	Prioritise access, supplier and recovery work	03 04 05 07 12
SOC, endpoint and identity	Validate behaviour and current authority	04 06 07 B
Payments, fraud and customer protection	Prevent a plausible request becoming a harmful action	05 08 09
Legal and communications	Establish the correct scope, clock and public message	05 06 10 12

Chapter group	What it establishes
1–3	Decisions, context and the measured or unavailable portfolio scope
4–5	Actor assertions beside official disclosures and investigations
6–7	Service evidence, campaign research and bounded relationships
8–10	Fraud, payment authority and entity-specific reporting duties
11–12	Conditional planning and reviewable completion evidence
Appendices	Population limits, case register, supporting sources and definitions

The evidence labels distinguish observation, claim, official confirmation, attributed research and analyst inference. An observed offer remains a claim about its contents. A confirmed incident can leave actor identity, entry route and affected-person totals unresolved.

CHAPTER 02

Brazil's digital and operating context

THIS CHAPTER ANSWERS

Which features of Brazil's digital economy change the security decisions in this report?

185 million

internet users in the October 2026 contextual estimate

2.1 A large digital population, with distinct units 12

2.2 Payment identities connect several organisations 12

2.3 Public services have several continuity boundaries 13

2.4 The October election is context, not attribution 13

2.5 National coordination and sector duties coexist 13

CHAPTER 02

Brazil's digital and operating context

IN SHORT

Brazil's connected services create several routes from identity data to operational harm. A copied registration record, a stolen browser session and an authorised payment credential require different responses. Public cases also show why administrative recovery and physical operations must be assessed separately. Treat the October election as a communications context, with every attribution tied to its source. Map identity, payment and supplier dependencies before choosing containment.

2.1 A large digital population, with distinct units

DataReportal's October 2026 snapshot estimates 185 million internet users and 86.5% penetration. It reports 218 million mobile connections and 154 million social-media user identities. Connections and platform identities do not count unique people. [S16]

Those figures provide context for customer-facing services. They do not explain the origin of a stolen dataset or establish how often Brazilian users experience fraud. Underground advertisements can name Brazil as a customer market, a claimed data origin or one entry in a multinational catalogue.

The operational implication is to protect the transaction and recovery process alongside the login. A familiar name, taxpayer identifier or telephone number should not, by itself, authorise a sensitive account change. Service owners should identify the stronger evidence required for that change.

2.2 Payment identities connect several organisations

Google Threat Intelligence Group's September research describes financially motivated activity against organisations able to issue payment instructions. Its account includes banks, payment processors, retailers and financial-software providers. The research spans activity beginning before 2026; publication does not date every observed intrusion to this year. [S18]

For defenders, a payment dependency map should identify the institution, technical provider, signing identity, approval process and recovery owner. A supplier may operate technology without owning the funds. A retailer may possess a transactional credential without being a bank.

This is a planning interpretation, not an assertion that the selected organisations share a particular architecture. Validate the actual relationships before assigning an incident to a whole financial group or every customer of a provider.

2.3 Public services have several continuity boundaries

The Santos disclosures distinguish administrative-system recovery from continued port operations. The Treasury disclosure distinguishes affected personal-data stores from structural systems and financial impact. Each statement supports a specific operational boundary. Neither supports a general conclusion that all public services were unaffected. [S127][S128][S229]

An incident plan should therefore define the minimum service in business terms. For a port, that includes authorised access and cargo procedures. For a public service, it includes a working route for citizens while digital administration is restricted.

Manual procedures also produce records that must later be reconciled. The recovery owner should specify who checks those records, resolves duplicates and approves the return to normal operation. A responding website is one milestone, not the complete recovery test.

2.4 The October election is context, not attribution

The electoral authority's calendar places the general election's first round on 4 October and any second round on 25 October 2026. Those dates fall inside this report's observation window. They do not establish that an adjacent cyber claim was election-related. [S17]

The report draws no conclusion about election integrity or outcomes from website availability, leaked-record advertising or an actor's political language. A claim about a court, party or public figure must establish its own evidence. Language and self-description do not establish nationality or state direction.

For communications planning, use the same verification and protection standards across political affiliations. Prepare a trusted status channel and an update schedule. Separate a claim about information services from any claim about voting, counting or judicial systems.

2.5 National coordination and sector duties coexist

The national cybersecurity strategy established by Decree 12.573 in August 2025 covers citizen protection, essential services, cooperation and governance. It is a strategic framework. The report does not treat it as a universal incident-notification deadline for every organisation. [S21]

Data protection, financial supervision, telecommunications and government incident coordination have different purposes. Chapter 10 sets out the reporting decisions supported by the cited texts. A police report, a technical notification and a personal-data notice should not be assumed interchangeable.

KEY TAKEAWAYS

01

Identity, session and payment authority are separate control boundaries.

02

Election dates and political rhetoric do not establish attribution or electoral impact.

03

Define minimum service and reporting ownership across suppliers and legal entities.

CHAPTER 03

National exposure: a selected 250-domain portfolio

03

THIS CHAPTER ANSWERS

Which external signals justify validation across the selected portfolio?

131 of 250

selected domains had an associated credential advertised for sale when checked

3.1 Universe card 16
3.2 The national headline and its decision boundary 17
3.3 Device and credential associations 17
3.4 Current offers, documents and similar domain names 19
3.5 Account validation before containment 20
3.6 Passive controls retain their own denominator 20
3.7 Turn evidence into owned work 20

CHAPTER 03

National exposure: a selected 250-domain portfolio

IN SHORT

In the selected portfolio, 131 of 250 domains had an associated credential advertised for sale when checked. The national Atlas headline is 80/100 (F). The snapshot contains at least 2,022,570 device associations and 12,126,465 credential-record associations. These overlapping records describe the selected domains, not unique people, confirmed intrusions or national prevalence. Assign owners to current-account validation, employee-device investigation and data review.

3.1 Universe card

Item	Definition
Selected population	250 domains across ten sector groups
Selection	Purposive coverage of public services, banks, infrastructure, major enterprises and universities
Unit	A candidate primary domain; legal ownership and organisational independence remain unvalidated
Exposure snapshot	22 November 2026
Mention context	23 November 2025–22 November 2026
Publication	National Atlas headline and anonymous sector signal counts
Passive controls	No completed hygiene dataset available
Representativeness	No revenue ranking, random sample or national prevalence estimate
Overlap	Related services can share an operator; record associations can overlap across domains

The selected domains are the assessment units. Some can represent related brands, services or legal entities. The portfolio therefore supports bounded validation work rather than a count of independently owned businesses. [S3]

3.2 The national headline and its decision boundary

The national Atlas headline is 80/100 (F). Higher values indicate greater observed exposure within this portfolio. The rating is not a breach percentage, an intrusion probability or a certification of control effectiveness. [S3]

Only the national headline is published. Sector rows contain measured signal counts and their denominators. They do not rank sectors by security, and no organisation or sector rating is disclosed.

The exposure snapshot and mention context differ from the report's publication window. Historical records can remain visible after remediation. The headline does not establish that every associated record first appeared during 2026 or remains usable.

3.3 Device and credential associations

The portfolio contains at least 2,022,570 device associations, including 108,555 employee-device associations, and 12,126,465 credential-record associations. Device and credential associations each concern 246 of the 250 domains. Employee-device associations concern 229 domains. [S3]

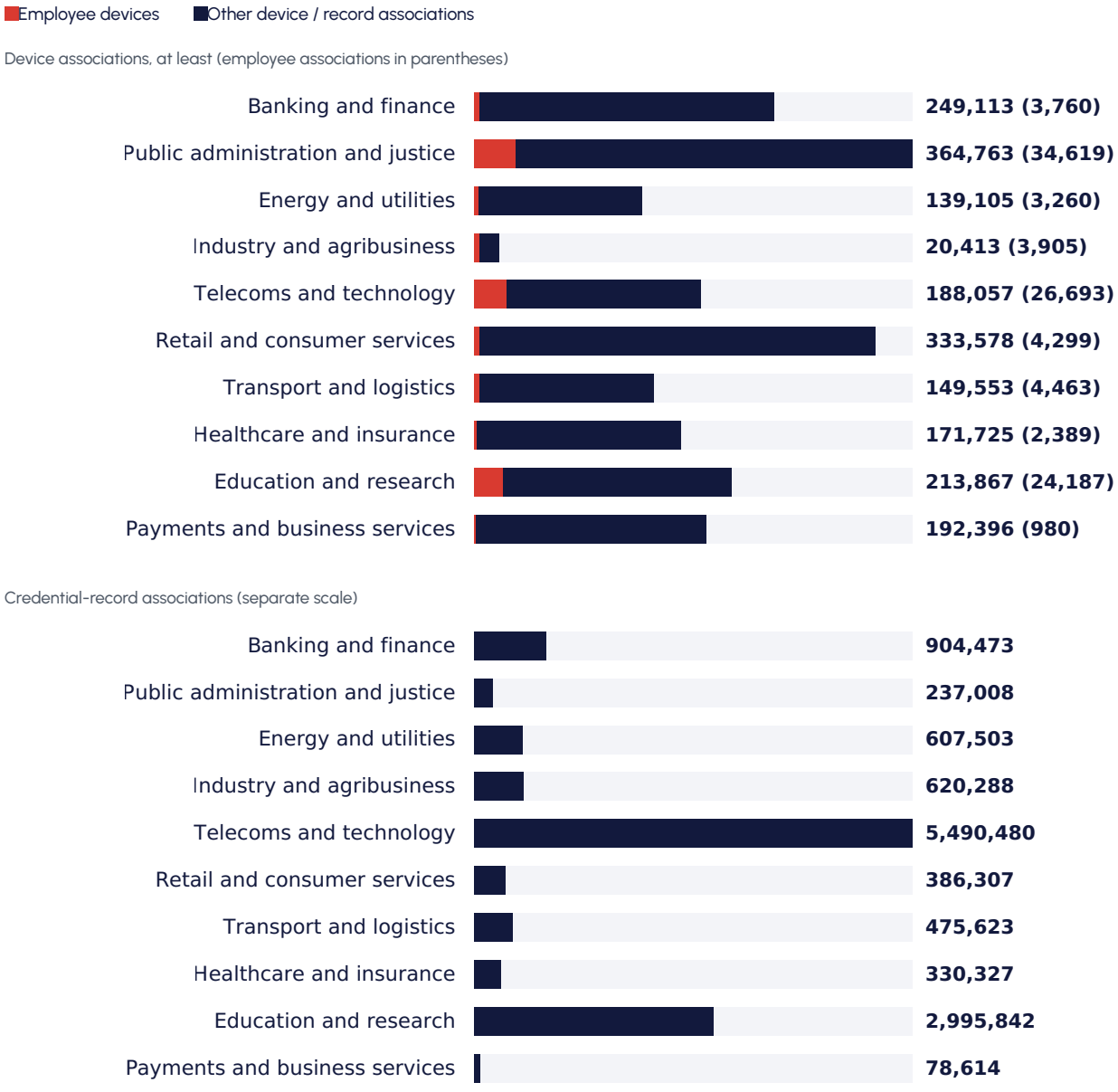
Sector	Domains	Devices, at least	Employee devices	Credential records
Banking and finance	28	249,113	3,760	904,473
Public administration and justice	30	364,763	34,619	237,008
Energy and utilities	27	139,105	3,260	607,503
Industry and agribusiness	27	20,413	3,905	620,288
Telecoms and technology	22	188,057	26,693	5,490,480
Retail and consumer services	24	333,578	4,299	386,307
Transport and logistics	25	149,553	4,463	475,623
Healthcare and insurance	24	171,725	2,389	330,327
Education and research	25	213,867	24,187	2,995,842
Payments and business services	18	192,396	980	78,614
Total	250	2,022,570	108,555	12,126,465

Employee-device associations are part of the device view and must not be added to it. Associations can overlap across domains. These totals are neither distinct national endpoints nor unique people.

Telecoms and technology account for 5,490,480 credential-record associations, while education and research account for 2,995,842. Public administration and justice account for at least 364,763 device associations. These concentrations support owner-specific validation, without establishing sector compromise rates.

A device associated with a customer-facing domain need not belong to the service provider. A credential record can concern an employee, customer, student, contractor or unresolved relationship. Establish that relationship before selecting containment.

Sector device and credential populations differ in scale and meaning



Source: exposure observations for 250 selected domains, 22 November 2026 [S3]. Associations can overlap and include historical material; not unique people, current intrusions or national prevalence.

3.4 Current offers, documents and similar domain names

In this snapshot, 131 of the 250 selected domains had an associated credential advertised for sale when checked. Document associations concern 201 domains; similar-domain observations concern 206. These populations can overlap and are not added together. [S3]

Sector	Domains	Domains with credential offers	Documents	Similar domain names
Banking and finance	28	17	1,475	2,780
Public administration and justice	30	14	3,666	9,184
Energy and utilities	27	9	488	655
Industry and agribusiness	27	6	461	2,774
Telecoms and technology	22	15	668	2,442
Retail and consumer services	24	18	168	880
Transport and logistics	25	10	234	581
Healthcare and insurance	24	13	150	1,235
Education and research	25	18	339	574
Payments and business services	18	11	75	2,520
Total	250	131	7,724	23,625

Current listings establish an advertisement, not tested access, a completed sale or an intrusion into the organisation's infrastructure. Validate the advertised account, service and evidence date with the responsible owner.

The 7,724 document associations do not establish confidential content, unlawful acquisition or adversary downloads. Public or repeated documents remain plausible explanations. A data owner must establish ownership and sensitivity.

The 23,625 similar-domain observations are recent observations. Similarity alone does not establish impersonation or phishing. Ambiguous matches remain unresolved until brand and abuse teams validate the relevant content and relationship.

3.5 Account validation before containment

For an owned account, establish whether it is active and whether the evidence is recent. Check privileges, sign-ins, session grants, recovery methods and earlier remediation. Record whether the relationship concerns an employee, contractor, customer, student or unresolved party.

An active privileged identity can justify urgent session revocation and access review. A historical disabled account may require documentation of earlier closure. A password change alone does not establish that delegated access and persistent sessions ended.

Customer-device observations can require fraud or customer-protection work. They do not automatically justify a provider-infrastructure incident. The anonymous banking view in Chapter 9 keeps these response boundaries separate.

3.6 Passive controls retain their own denominator

No DMARC, SPF, DKIM, DNSSEC, TLS or web-header prevalence is published here. No complete hygiene dataset or hygiene index is available. Unavailable observations are not failed controls and are not replaced with zeros.

Owners should validate legitimate mail senders and authentication alignment before tightening enforcement. They should review certificate validity and service dependencies within their own environment. The exposure snapshot does not supply the missing configuration assessment.

3.7 Turn evidence into owned work

Queue	First decision	Closure evidence
Account evidence	Does this identity belong to an active owned service?	Dated validation and account disposition
Endpoint evidence	Is the device relationship relevant and current?	Endpoint investigation and response record
Customer protection	Does the evidence create a specific fraud risk?	Fraud assessment and trusted support route
Configuration	Is the reported control state accurate?	Owner-verified configuration record
Data ownership	Does the material belong to the organisation?	Category, age and access assessment

KEY TAKEAWAYS

01

The national Atlas headline describes the selected portfolio rather than national prevalence.

02

Device, credential, listing and document populations require separate validation.

03

Assign account, endpoint, data and configuration evidence to separate owners with dated closure evidence.

CHAPTER 04

Dark-web activity: from an advertisement to an owned decision

THIS CHAPTER ANSWERS

What is being offered, and what would make it actionable?

10 selected claim cases with authentic, redacted post excerpts

4.1 Reading the post population 23
4.2 Case A: public-body document archive 24
4.3 Case B: customer, order and delivery records 25
4.4 Case C: municipal fiscal-data claims 26
4.5 Case D: guardians and student financial history 27
4.6 Case E: virtual-assistant data and inconsistent chronology 28
4.7 Case F: recent bank-associated leads 30
4.8 Case G: a November Pix offer labelled 2025 31
4.9 Case H: business-software customer table 32
4.10 Case I: certificates and internal-network access 33
4.11 Case J: fintech infrastructure access 34
4.12 Claim versus evidence 35
4.13 Additional narratives and deliberate boundaries 35
4.14 Publication context and the language boundary 36

CHAPTER 04

Dark-web activity: from an advertisement to an owned decision

IN SHORT

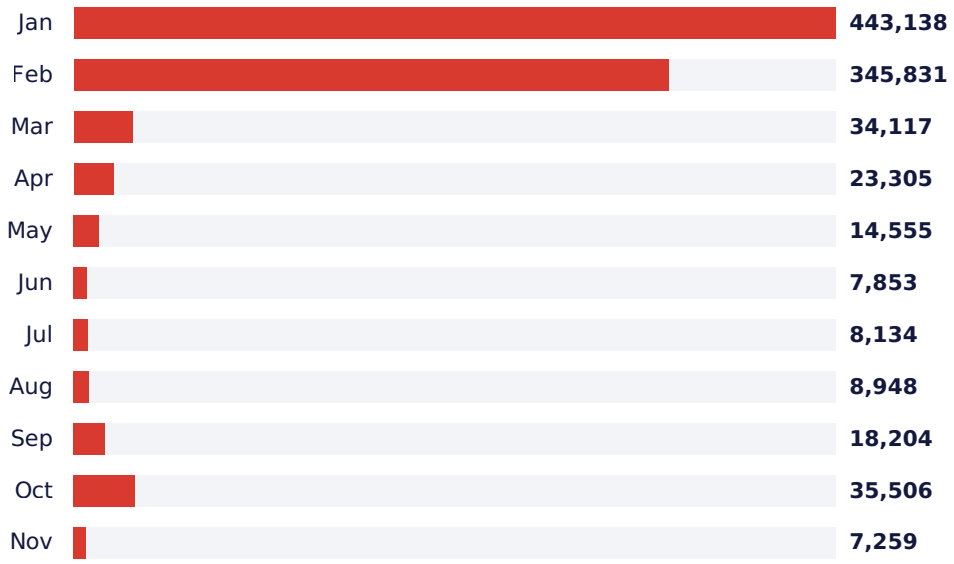
The selected posts advertise public records, customer workflows, education data, financial leads and payment-related access. The post is evidence that the claim circulated. It does not authenticate the data, establish a fresh intrusion or verify a completed sale. Repetitions and inconsistent dates deserve attention without becoming additional incidents. Read each offer as a scoped lead, then ask the responsible owner to validate the data, identity or permission involved.

4.1 Reading the post population

Brandefense Blackhole observations cover Brazil-associated posts within 1 January–22 November 2026. A Brazil association can describe a claimed target, a customer market, a data field or discussion of public events. It is not automatically evidence of targeting. [S1]

Blackhole records 946,850 Brazil-associated posts in the window. January and February together account for 788,969, or 83.3% of that publication population. Later months have different visibility. This pattern does not establish a corresponding change in criminal activity or losses. [S1]

Monthly Brazil-associated publication observations; posts are not incidents



Source: Brazil-associated publication observations, 1 January–22 November 2026; closing day partial. Posts are not incidents [S1].

The broader content coverage is incomplete. The ten case narratives below are supported by the retained excerpts, without an estimate that they represent every event in the larger post population. Platforms and language labels describe publication context, not nationality or operational control.

The selected cases are not the ten largest incidents in Brazil. They are illustrations of distinct decisions supported by retained posts. The accompanying public excerpts remove subject locators, contacts, personal details and retrieval routes while retaining the meaning of the claim.

An advertisement is evidence of an advertisement. An advertised database may be historical, partly public, assembled from several origins or misrepresented. An access offer may be obsolete, limited or fabricated. Confirmation requires evidence from the relevant organisation or another competent source.

The chapter therefore separates what is held from what is not established. The same separation governs the incident register and evidence record. A source's confident language does not raise the report's confidence in the underlying access.

4.2 Case A: public-body document archive

A 3 January post claims an incomplete archive of documents associated with a public-sector body. The excerpt describes 2.9GB and labels the material confidential. These are the poster's descriptions, not authenticated document findings. [S1]

Evidence card B01 — 3 Jan 2026

Forum poster | Leak forum | Forum | English

ORIGINAL

SIZE : 2.9GB (not complete) THIS FOLDER CONTAINS DOCUMENTS ONLY [...] confidential documents related to the [public-sector body].

Held
A poster asserts release of documents connected to a public-sector body and advertises an incomplete archive.

Not established
Observed claim, not authenticated files, proven confidential content, current access, actor identity or a verified intrusion date.

CASE A

A

Public-body document archive

Public administration

Claim unverified

OBSERVED	A dated archive claim and broad document description circulated.
NOT ESTABLISHED	Authenticity, actual confidentiality, current system access, unique people or an intrusion date.
ALTERNATIVE	An old export, public material or a misleading archive label could produce a similar advertisement.
OWNER AND ACTION	The data owner should validate relevant document categories and age, then review the corresponding authorised access records.

Bottom line

Validate document ownership, age and sensitivity.

A file size cannot establish operational impact. If the owner validates a sensitive document, the response should follow that document's contents and permitted readership. It should not assume that every system of the body was entered.

4.3 Case B: customer, order and delivery records

A 4 January retail-associated offer lists Contacts, Orders and Deliverylogs. That combination describes a customer workflow rather than a verified number of people. A quoted response repeats the advertisement and supplies no independent confirmation. [S1]

Evidence card B02 — 4 Jan 2026

Forum poster | Leak forum | Forum | English

ORIGINAL

Offering a dataset originating from [a retail business]. [...] including Contacts, Orders, Deliverylogs.

Held

A dataset advertisement combines customer-contact, order and delivery categories.

Not established

The claimed field list is held; possession, freshness, organisation origin, record count and completed sale are not verified. A quoted reply repeats the advertisement.

CASE B

B

Customer, order and delivery records

Retail

Claim unverified

OBSERVED	The field-category claims and sale language are present in the post.
NOT ESTABLISHED	Possession, source organisation, data age, a completed sale or a unique customer count.
ALTERNATIVE	The material could come from a contractor, an older export or copied advertising.
OWNER AND ACTION	The service and data owners should validate relevant categories and prepare trusted verification for delivery and payment contacts.

Bottom line

Validate source and customer-workflow categories.

A retailer, delivery operator and software provider may each hold related records. Establish which organisation controlled the relevant data before assigning responsibility. A credible-looking delivery detail should not authenticate a request to pay an unexpected charge.

4.4 Case C: municipal fiscal-data claims

A 14 January narrative advertises multiple municipal tax databases, naming taxpayer records, NFSe invoices, declarations, access logs and payment guides. Related municipal-data advertisements recur in the retained material. Similar wording is not proof of the same operator or event. [S1]

Evidence card B03 — 14 Jan 2026

Forum poster | Leak forum | Forum | English

ORIGINAL

multiple Brazilian municipal tax databases [...] The dataset includes taxpayer records, NFSe invoices, declarations, access logs, payment guides, and more.

Held

The poster claims a multi-database fiscal-data release associated with municipal services.

Not established

Claimed rows span multiple databases; they do not establish unique people, separate municipal intrusions, current access or authenticated invoice data. A parallel forum post carries similar wording.

CASE C

C

Municipal fiscal-data claims

Municipal services

Claim unverified

OBSERVED	A multi-database fiscal-data claim and an advertised category list.
NOT ESTABLISHED	Separate municipal intrusions, unique taxpayers, current access or authentic invoice records.
ALTERNATIVE	Several databases can contain overlapping records from a common service or historical export.
OWNER AND ACTION	Map the service and supplier boundaries, validate relevant records and test how payment instructions are authenticated.

Bottom line

Map fiscal services and verify payment instructions.

Do not add table-row claims into a count of people. A taxpayer can appear in an invoice, declaration, access record and payment guide. The same material may also be advertised more than once.

The response should connect data protection and payment integrity without confusing them. A copied payment guide may support impersonation. It does not establish the ability to alter the municipality's live guides or redirect a transaction.

4.5 Case D: guardians and student financial history

A 2 February post advertises approximately 763,000 personal and financial records associated with an education service provider. The poster describes guardian profiles, CPF identifiers and student financial histories. The number remains an advertised row claim. [S1]

Evidence card B04 — 2 Feb 2026

Forum poster | Leak forum | Forum | English

ORIGINAL

approximately 763,000 personal and financial records from [an education service provider] (Brazil). The dataset contains sensitive guardian profiles, national ID numbers (CPF), and detailed student financial histories.

Held

An offer links guardian identifiers to student-related financial records.

Not established

Advertised rows are not unique students or guardians. Possession, acquisition date, data accuracy and source-system access remain unverified.

CASE D

D

Guardians and student financial history

Education

Claim unverified

OBSERVED	A provider-associated claim linking family identifiers to education-finance context.
NOT ESTABLISHED	A unique student or guardian total, accurate records, acquisition date or provider-system access.
ALTERNATIVE	The categories could combine several service periods or repeated family relationships.
OWNER AND ACTION	Validate the provider relationship and review trusted routes for tuition, debt and account-recovery messages.

Bottom line

Validate provider scope and trusted tuition contacts.

Education organisations should know who answers family questions if a provider disclosure occurs. A parent's correct name or a plausible tuition detail must not replace verification. The appropriate support message depends on validated categories, not the advertised headline number.

4.6 Case E: virtual-assistant data and inconsistent chronology

A 6 February post claims a partial virtual-assistant dump associated with financial services. It describes an export extending from September 2022 to April 2026. The claimed end date follows the stored post date, so the chronology requires validation. [S1]

Evidence card B05 — 6 Feb 2026

Forum poster | Leak forum | Forum | English

ORIGINAL

today we release [a financial services provider]'s [virtual assistant] partial dump. [...] exported all data from Sept 2022 to April 2026.

Held

A partial virtual-assistant data advertisement mixes conversation and identity counts and claims a data period ending after its stored post date.

Not established

The post is dated 6 February 2026 but says data extend to April 2026. This inconsistency requires validation; it neither authenticates the dataset nor establishes fabrication. Identity-category counts cannot be added as unique people.

CASE E

E

Virtual-assistant data and inconsistent chronology

Financial services

Claim unverified

OBSERVED	The partial-dump narrative and its inconsistent time claim.
NOT ESTABLISHED	The true data interval, source, current access or unique identities.
ALTERNATIVE	A date error, reused description or misrepresentation could explain the inconsistency; the record does not settle which.
OWNER AND ACTION	Validate service ownership, chronology and record categories before adopting the quantity or declaring a platform incident.

Bottom line

Resolve chronology before adopting a quantity.

The inconsistency neither authenticates the material nor establishes fabrication. It is a reason to retain uncertainty. Conversation counts and identity counts also measure different populations and cannot be added as people.

Related wording appears in later posts. That establishes continued circulation of a narrative. It does not show that a seller retained live access throughout the period or that every reposter held the data.

4.7 Case F: recent bank-associated leads

An 11 November seller claims 22,705,600 bank-associated leads, says they were exported a week earlier and offers whole or segmented sales. The acquisition timing and quantity are the seller's assertions. The report does not repeat the advertised share of bank accounts as a bank statistic. [S1]

Evidence card B06 — 11 Nov 2026

Forum poster | Leak forum | Forum | English

ORIGINAL

I have 22,705,600 leads that I exported one week ago directly from [a bank]. [...] I am looking to sell this database, either in its entirety or in segments.

Held

A November seller claims a large bank-associated lead list and offers full or segmented sales.

Not established

No organisation confirmation, authenticated record population, acquisition date, current access, ownership or completed sale is established. The asserted proportion of the bank's accounts is unverified and should not be repeated as a bank statistic.

CASE F

F

Recent bank-associated leads

Banking

Claim unverified

OBSERVED	A recent advertisement offering bank-associated leads and segmentation.
NOT ESTABLISHED	Organisation confirmation, record accuracy, source, freshness, current access or a completed sale.
ALTERNATIVE	A contact list may combine old, public, brokered or unrelated records while using a bank name as a sales category.
OWNER AND ACTION	Validate provenance and categories, then assess customer-contact risk separately from bank-system access.

Bottom line

Separate lead-list claims from bank-system access.

The advertisement is relevant to plausible impersonation. It is not evidence that every named or counted lead is an active customer, holds a funded account or has experienced financial harm. Customer protection should use the validated scope.

4.8 Case G: a November Pix offer labelled 2025

A 17 November advertisement calls itself a Pix database for 2025, claims more than 4M entries and asks US$100. Its own description supplies a historical-data boundary. The price is an asking price, with no completed sale established. [S1]

Evidence card B07 — 17 Nov 2026

Forum poster | Leak forum | Forum | English

ORIGINAL

PIX DATABASE 2025 [...] Year: 2025 Records: 4M+ entries Country: Brazil [...] Price: $100 USD

Held

A November advertisement explicitly labels its Pix-related data as 2025 material.

Not established

The post date does not establish a 2026 intrusion. Entries are not verified people or transfers; no linkage to any particular official Pix disclosure, usable payment access or completed sale is established.

CASE G

G · A November Pix offer labelled 2025

Payments

Claim unverified

OBSERVED	A Brazil-labelled payment-data offer with an explicit 2025 label.
NOT ESTABLISHED	A 2026 intrusion, unique people, usable payment access or a connection to a specific official Pix notice.
ALTERNATIVE	Historical aggregation and resale can explain current circulation without current access.
OWNER AND ACTION	Check age and origin, and independently authenticate requests that quote payment-related identifiers.

Bottom line

Historical payment data does not establish current authority.

An entry associated with Pix is not necessarily a secret that authorises a transfer. Equally, a historical identifier can remain useful for impersonation. Keep the payment-authority assessment separate from the data-protection assessment.

4.9 Case H: business-software customer table

A 19 November post claims Brazil-associated material dated November 2026 and identifies a customer-table file. It associates the data with business software. Those labels remain claims and do not establish when records were obtained. [S1]

Evidence card B08 — 19 Nov 2026

Forum poster | Leak forum | Forum | English

ORIGINAL

Country: Brazil Date: Nov 2026 [...] Table_Name:customers.csv

Held

A November offer describes customer data associated with a business-management service.

Not established

The table name and advertised service role do not establish a current provider intrusion, downstream client incidents, authentic records, affected-person count or completed sale.

CASE H

H

Business-software customer table

Business software

Claim unverified

OBSERVED	A dated provider-associated customer-data advertisement.
NOT ESTABLISHED	A provider intrusion, current access, unique people or separate incidents at downstream businesses.
ALTERNATIVE	A customer export, an older dataset or a relabelled collection could appear under similar wording.
OWNER AND ACTION	Validate the provider and client boundaries, relevant data categories and the incident-notification route.

Bottom line

Validate provider and downstream boundaries separately.

Earlier restaurant-software advertisements describe users, leads and customer rows. They are separately recorded claims. Their overlapping categories are not added to the November offer as a national hospitality victim count.

4.10 Case I: certificates and internal-network access

A 24 March post offers certificates associated with a payment-services intermediary and separately advertises internal-network access. It does not authenticate the material or demonstrate that the certificates could authorise a payment. [S1]

Evidence card B09 — 24 Mar 2026

Forum poster | Leak forum | Forum | English

ORIGINAL

I am offering access to certificates belonging to [a payment services intermediary]. [...] Additionally, access to an internal network is available.

Held

An access advertisement pairs payment-related certificates with alleged internal-network access.

Not established

No certificate file, trust status, transaction authority, usability, current network access, sale or linkage to a named campaign is established by the advertisement.

CASE I

Certificates and internal-network access

Payment services

Claim unverified

OBSERVED	Certificate and internal-access sale language in a dated offer.
NOT ESTABLISHED	Certificate role, validity, privileges, current access, transfer capability or a completed sale.
ALTERNATIVE	Obsolete, test or limited-purpose material could carry a convincing description without production payment authority.
OWNER AND ACTION	Ask the payment and provider owners to validate identity scope and demonstrate the relevant revocation process.

Bottom line

Establish certificate scope and revocation authority.

The public research on payment-identity theft makes this a useful control question. It does not link this seller to BREEZE COMET or any confirmed financial incident. Similar subject matter alone does not establish an operational relationship. [S18]

4.11 Case J: fintech infrastructure access

A 6 July offer describes access associated with a Brazilian fintech infrastructure and banking-service provider. Its wider permission claims require validation against the actual environment. The source's sector label does not establish the identity of every client. [S1]

Evidence card B10 — 6 Jul 2026

Forum poster | Leak forum | Forum | English

ORIGINAL

Currently selling an access within a brazilian fintech company. SECTOR: Fintech/Infratech/BaaS REGION: Brazil

Held

A seller advertises access spanning website and code administration, databases, object storage, monitoring and production exports.

Not established

The advertised roles do not establish effective permissions, a production intrusion, transfer authority or a sale.

CASE J

J

Fintech infrastructure access

Financial infrastructure

Claim unverified

OBSERVED	An access advertisement with a financial-infrastructure description.
NOT ESTABLISHED	Current administrative authority, production access, fund movement, client impact or any completed transaction.
ALTERNATIVE	Access may be restricted, historical, shared incorrectly or misrepresented.
OWNER AND ACTION	Confirm the provider relationship, relevant environment and actual permissions, then coordinate scoped containment with the accountable service owner.

Bottom line

Validate environment and effective permissions.

An infrastructure provider can serve many organisations, but a provider-associated offer does not establish an incident at each one. The first response should locate the authority that can validate or revoke the alleged access.

4.12 Claim versus evidence

Actor claim	Evidence held	Responsible interpretation
"Millions of records"	A post contains the quantity	Rows, people and accounts remain different units
"Fresh export"	A relative date in seller text	Acquisition time requires validation
"Admin access"	Advertised permission language	Current privilege and environment remain unverified
"Certificates"	An offer refers to certificate material	Payment-signing authority is not established
"Pix database"	A payment-related label and claimed year	No automatic connection to a disclosed Pix incident
"Confidential documents"	The poster's description	Content classification and ownership require validation
A repeated advertisement	The narrative reappears	Neither a new incident nor an independent confirmation

The panel is an interpretation guide. It does not deny the possibility of real harm. It identifies which proposition the held evidence can support, so the next action is specific and reviewable.

4.13 Additional narratives and deliberate boundaries

The incident register also records alleged residential-camera access, resident and employee records, investigative-service logins, a white-label payment platform and a retail-linked financial dataset. Each retains its own action and uncertainty. None becomes a confirmed intrusion merely by appearing beside an official case. [S1]

A KYC-related advertisement explicitly says it is not a leak. It is treated as a service or demand narrative, with no automatic incident inference. Vehicle-related material explicitly dated to 2024 is treated as historical, despite a 2026 post date.

A political-party membership offer remains an unverified data claim. It provides no basis for an election-interference finding or any verdict on a party. A November operational-logistics claim similarly does not establish control of physical systems or an actual interruption.

Additional posts advertise public-sector webshells and a cloud-mail account. Advertised sale labels, a bot payment message and an unexplained stock quantity do not verify a transaction, account validity or current permissions. Treat the access proposition as an owned-service validation lead. [S1]

Keep these leads available to the correct owners without reproducing personal records or enabling contact with sellers. Validate owned evidence and preserve the disposition. Relevance to a country report and confirmation of a harmful event remain separate decisions.

A 22 November post describes a purported professional-contact export associated with a business-information provider. Its directory, profile and support-request categories remain the poster's assertions. They do not authenticate the records or establish patient-data exposure, an intrusion, fresh acquisition or current access. Validate ownership and permitted use before treating a directory claim as a confidential-data incident. [S1]

An 18 August relay describes a purported public-sector database release rather than a sale. It does not authenticate possession or distribution, or establish that the material matches the earlier archive offer in Case A. [S1]

A separate 22 November offer describes a purported export from a hosted customer-management and retail-services provider. It names contact, website-project and support-case categories. The description does not verify data origin, records, current access, customer impact, an acquisition date or a completed sale. Provider and customer boundaries need separate validation. [S1]

4.14 Publication context and the language boundary

Context	Label	Posts observed
Platform	Telegram	896,534
Platform	Leak forum	1,840
Language	Portuguese	116,772
Language	English	60,682
Language	Spanish	7,177
Language	Russian	26,878
Language	Turkish	724,456

These are publication-label observations in the 22 November snapshot, rather than an incident classification. Language labels do not form a count of distinct people or actors. Platform and language observations must not be added together. [S1]

Turkish is the most numerous of these language labels. That does not establish Turkish operator nationality, control or targeting. A Brazil association can appear in multilingual circulation, including repeated material. The retained case evidence supplies the narrower security question.

For a defender, the consequence is practical: assess the relevant content and owned asset before escalating a country or language association. Neither a large publication total nor a familiar bank name authenticates an advertised database.

KEY TAKEAWAYS

01

A post establishes circulation of a claim, with its original time and limits.

02

Row claims, repeated narratives and advertised permissions do not establish unique victims or current access.

03

Give each relevant lead a data, identity, payment or service owner and a documented disposition.

CHAPTER 05

Incidents and targeting by sector

THIS CHAPTER ANSWERS

Which disclosures change a defender's decision, and what remains a claim?

10

named examples supported by official confirmation and wider reporting

5.1 Sector decision table 39
5.2 Confirmed registration-data incidents 40
5.3 Payment integrity and financial service availability 41
5.4 Administrative recovery and operational continuity 43
5.5 Additional official cases and campaigns 44
5.6 Additional disclosures across services 46
5.7 Recent activity: 8–22 November 50
5.8 Important exclusions and historical context 53
5.9 Other bounded disclosures and reports 53

CHAPTER 05

Incidents and targeting by sector

IN SHORT

Public disclosures show copied registration data, altered payment instructions and prolonged administrative recovery. They do not describe one common intrusion. The named cases below meet the report's confirmation and reporting bar; other subjects retain broad roles. Discovery, disclosure, investigation and restoration are separate dates. Start with the affected function and the established access, then choose containment, customer support and continuity measures that fit that evidence.

5.1 Sector decision table

The rows combine different evidence types without turning them into sector incident rates.

Sector	Evidence in this edition	Type and boundary	First decision
Banking and payments	Pix-service incident; payment-guide alteration; access and lead advertisements	Official incidents and separate unverified offers	Protect transactional authority and validate account evidence
Insurance	CVP registration database copied	Company-confirmed categories; preliminary exclusions remain dated	Prepare customer protection and scoped communication
Public administration	Treasury disclosure; historical registration base; website campaign warnings	Confirmed notices and campaign guidance	Assign data owners and minimum-service arrangements
Transport and logistics	Santos administrative systems and manual access procedures	Authority-confirmed incident; port capacity assurance is source-attributed	Exercise administrative fallback and reconciliation
Healthcare	Clinical-data investigation, portal disclosure and care-continuity incidents	Official notices and police allegations; separate populations	Review data access, clinical fallback and administration
Education	Guardian and student-finance data advertised	Unverified field and row claims	Validate provider scope and tuition-message verification
Retail and services	Customer, order, camera and resident-data advertisements	Claims, including demand and historical material	Separate service ownership from customer-data provenance
Industry and energy	Utility customer-data disclosure, listing observations and attributed research	Company disclosure and separate claims; no representative sector intrusion rate	Validate applicable access paths and recovery dependencies

Sources: retained posts [S1], Ransompedia [S2] and the official or original sources identified below. No sector is assigned an Atlas rating.

5.2 Confirmed registration-data incidents

CASE K

K

CVP registration records and customer protection

Insurance

Organisation-confirmed incident

CONFIRMED	Caixa Seguridade's market notice says CVP identified unauthorised access and copied registration data on 6 November. The affected database includes all 7.6 million active customers, as well as former customers. [S126] [S226]
CATEGORIES	The notice confirms names and CPF identifiers. Some records also contain contact details and dates of birth. Its preliminary assessment found no evidence of financial or authentication-data impact. [S126]
BOUNDARY	The active-customer population is not the total unique-person count. The notice does not establish an actor or authenticate an underground offer. The financial-data assessment remains the company's preliminary finding.
RESPONSE	Scope the affected categories, use trusted customer contacts and prepare for impersonation that quotes genuine registration information.

Bottom line

Scope copied categories and customer protection.

The response should distinguish an affected database from every system sharing the parent brand. A statement about the investee does not establish an intrusion into a related bank. The naming approval applies to this disclosed case and its stated scope.

CASE L

L

Treasury service registrations and a separate analytical base

Public administration

Organisation-confirmed incident

CONFIRMED	The Ministry of Finance says Tesouro Nacional detected unauthorised personal-data access on 4 November. Its 13 November notice identifies about 30,000 service registrations and a separate base with about 4,000 Pix keys. [S127][S227]
BOUNDARY	The bases are not a disjoint count of people. The ministry states there was no financial impact and no structural system was affected. Those are the ministry's findings, not a conclusion about every government service.
RESPONSE	Review the affected data categories and relevant access. Authenticate contacts that use genuine payment context through an independent route.

Bottom line

Keep registration records and Pix keys as separate populations.

The presence of a Pix key does not itself establish the ability to initiate a transfer. The notice's payment-related context creates a customer-protection question without proving a payment-system intrusion. Keep the two propositions separate in the incident record.

5.3 Payment integrity and financial service availability

CASE M

M

Belo Horizonte payment guides were altered

Municipal payments

Organisation-confirmed incident

CONFIRMED	Belo Horizonte's updated official notice says payment information on some guides issued during 14–16 November was changed. About 250 taxpayers paid using altered Pix guides, so the funds did not reach the municipality. [S233][S234]
UPDATE	The municipality says the affected funds were blocked and automatic refunds began on 17 November. The notice does not establish that every refund was already completed. [S233]

BOUNDARY	The confirmed issue is payment-instruction integrity. No actor, entry route or compromise of the Pix core is established by the notice.
RESPONSE	Verify beneficiaries, identify the affected instruction interval and reconcile refunds and replacement payments through the authorised process.

Bottom line

Reconcile beneficiaries, blocked funds and refunds begun.

This case changes the control question. A payment can begin through a genuine service while the instruction presented to the payer is wrong. Test who can change that instruction and how the payer or payment team detects an unauthorised beneficiary.

N

CASE N

Banco do Nordeste's temporary Pix suspension

Banking

Organisation-confirmed incident

CONFIRMED	The bank's 26 January market notice identifies a cybersecurity incident in its Pix transaction infrastructure and temporary service suspension. It says no data leak or customer-account harm had been identified at that stage. [S101][S201]
BOUNDARY	The initial customer-account statement is not a finding of no institutional financial loss. It does not identify an actor or show that the payment system itself was entered nationally.
RESPONSE	Separate customer balances, the institution's own funds, payment availability and data access. Give each outcome a responsible evidence owner.

Bottom line

Keep customer and institutional outcomes separate over time.

According to the indexed passage of the bank's later first-half management report, January cyber-fraud caused a loss of R$292 million, with R$148 million recovered through June. The full document could not be reviewed. [S231]

Those figures are the bank's reported loss and recovery at that time. They are not a Brazilian financial-sector loss estimate. The report does not infer a final net loss or connect the incident to any particular access advertisement.

5.4 Administrative recovery and operational continuity

CASE O

Santos administrative systems and manual procedures

Port administration

Organisation-confirmed incident

CONFIRMED	APS says its systems were affected on 6 November. Updates on 16–17 November describe staged administrative recovery and alternative service channels. The 17 November account describes data deletion discovered after systems restarted. [S128][S229]
OPERATIONAL BOUNDARY	APS states that cargo-movement capacity and ship, truck and train access were maintained. Folha separately reports user concerns about slower handling and manual processes. These are different measures. [S229][S228]
BOUNDARY	The sequence does not establish that an electrical outage caused the intrusion. No named ransomware family, entry route or verified personal-data total is established here.
RESPONSE	Test minimum service, manual authorisation and later reconciliation. Track actual user tasks while administrative systems recover.

Bottom line

Test administrative fallback and actual user tasks.

The 19 November authority update describes contingency access and registration procedures and states that no related public-security incident had been recorded. That assurance remains tied to the update date. It does not mean the administrative recovery was complete. [S230]

5.5 Additional official cases and campaigns

P

CASE P

Historical registration data at a federal agency

Public administration

Organisation-confirmed incident

CONFIRMED	A September agency notice describes a 12 June attack involving a static registration database with historical information through 2019. It distinguishes that base from separately controlled current information and tax-secret data. [S119]
BOUNDARY	Historical data can remain sensitive, but the notice does not establish a current live-register intrusion, a verified person total or a named actor.
RESPONSE	Identify retained historical exports, their owners and access rights. Prepare communications matched to the actual categories rather than assuming age removes the risk.

Bottom line

Review historical exports without assuming live-register access.

Q

CASE Q

A public warning service and alternate channels

Public warning services

Authority-reported incident

REPORTED	State and municipal authorities described suspension of a public warning platform after unauthorised false alerts in June. Their notices identify alternative communication and continued local monitoring. [S113]
BOUNDARY	The notices do not establish a named operator, entry route or political motive. A false alert is not evidence that a real physical emergency occurred.
RESPONSE	Rehearse authorised alert release, revocation and a trusted alternate channel. Preserve a clear explanation of which message is genuine.

Bottom line

Authenticate warnings and rehearse alternate channels.

CASE R

R Police investigate an institutional extortion event

Institutional services

Police investigation; allegations

REPORTED	PF's 7 October Operação Insidioso notice says an institution reported a July cyberattack, sensitive-data extraction and later payment demands. The action targeted an alleged facilitator. [S122]
BOUNDARY	The investigation does not establish a ransomware family, successful encryption, a named institution or a conviction. An extortion demand and encryption are separate propositions.
RESPONSE	Preserve the demand and relevant data-access evidence. Exercise both restoration and a data-loss response without waiting for a family label.

Bottom line

Prepare restoration and data-loss response separately.

CASE S

S Police investigate sensitive health-data commercialisation

Healthcare data

Police investigation; allegations

REPORTED	PF's February Operação Glycon announcement concerns alleged unauthorised access, processing and commercial use of clinical information through a service marketed to health professionals. [S102]
BOUNDARY	Police allegations are not a conviction. No national record total, intrusion route or responsibility of every participating professional is established here.
RESPONSE	Validate legitimate data sources and permissions. Review sensitive-data exports and the support route for affected people.

Bottom line

Validate lawful data sources and sensitive-data permissions.

The two police cases describe different alleged conduct. Neither is joined to the report's advertisements or malware families without supporting evidence. Their enforcement dates also do not establish when all underlying conduct began.

5.6 Additional disclosures across services

T

CASE T

Unimed Natal keeps care separate from system recovery

Healthcare

Organisation-confirmed incident

CONFIRMED	The cooperative's 14 November notice says it is investigating a cybersecurity incident, applying containment protocols and restoring affected systems with specialist support. It says hospital and assistential services continued, with alternative procedures where needed. [S166][S266]
BOUNDARY	The primary notice does not confirm data theft, an actor, a ransomware family, an affected-person count or completed restoration. Its scope concerns Unimed Natal, without establishing an incident at every organisation sharing the wider brand.
RESPONSE	Test clinical and administrative workflows separately. Keep a trusted route for authorisations and customer support while normal applications recover.

Bottom line

Separate clinical continuity from application recovery.

Later local reporting describes gradual recovery and application unavailability. Those details remain press-reported, rather than a replacement for the dated first-party care statement. No patient harm or hospital closure is inferred. [S266]

U

CASE U

An October portal incident disclosed in November

Health benefits

Official notice; full text not reviewed

REPORTED	An indexed first-party provider notice dated 19 November describes unauthorised health-benefits portal access on 18 October and phishing using incident-derived information the next day. Its verified corporate-provider categories include legal name, CNPJ, email, banking data and password hash. [S165]
BOUNDARY	The full document could not be reviewed. Individual-provider and beneficiary populations are not reconstructed from other notices. No affected-provider total, plaintext password exposure or medical-record disclosure is established here.

RESPONSE	Validate provider contacts, payment details and relevant access. Treat a password hash separately from a plaintext password and establish the appropriate account response.

Bottom line

Validate corporate-provider scope and follow-on phishing.

The notice's preliminary assessment points to privileged-credential theft through phishing or another method outside the portal infrastructure. That assessment is attributed and provisional. The case does not establish access to any payment or supervisory system. [S165]

CASE V

V

SES-MT and shared health-licensing continuity

Public health administration

Authority-confirmed shared-service incident

CONFIRMED	SES-MT's 2 November statement describes an attack detected on 1 November and temporary suspension of unit systems for security checks. It says hospital, urgency and emergency care continued with network-access limitations, while restoration would be gradual. [S268][S269]
SHARED-SERVICE EFFECT	Cuiabá's 9 November notice identifies an unavailable state sanitary-surveillance platform from 3 November. Protocols, service orders, inspector routing and sanitary licences were affected, with administrative deadlines extended automatically. [S167][S270]
BOUNDARY	These are phases and downstream effects of one state incident. They do not establish a second intrusion into Cuiabá, patient-data theft, a ransomware family, a victim count or completed restoration.
RESPONSE	Map licensing and administrative dependencies alongside clinical continuity. Record which fallback approvals and deadline changes require later reconciliation.

Bottom line

Map shared licensing dependencies without inventing another intrusion.

The state care assurance is tied to its statement date. The municipal notice establishes a particular administrative effect, without establishing harm to clinical care. No disputed quantities or attribution from a separate earlier event are imported into this case.

CASE W

W

BTG Pactual separates Pix availability from customer access

Banking

Issuer-authored mirror; dated findings

CONFIRMED	An issuer-authored letter dated 24 March describes atypical Pix activity on 22 March, a precautionary suspension and resumption early on 23 March. Wider reporting supports the incident and suspension. [S300][S301]
SOURCE LIMIT	The signed letter was read on a third-party host. Its official filing route was identified, but its contents could not be matched to a readable official-host copy.
BOUNDARY	The bank states that customer accounts were not accessed and account-holder data was not exposed. These are attributed findings, not a conclusion that the institution suffered no loss.
RESPONSE	Give service availability, customer-account access and institutional funds separate evidence owners. Reconcile the affected transactions before adopting any loss estimate.

Bottom line

Reconcile availability, customer access and institutional funds.

The letter's appended regulatory request quotes a preliminary press estimate. It does not establish a final net loss or recovered amount. This report adopts no monetary estimate and makes no judgement about disclosure materiality. [S300]

CASE X

X

Sírio-Libanês investigates possible access to project reports

Healthcare projects

Confirmed investigation; possible access

CONFIRMED INVESTIGATION	The hospital's official questions and answers identify possible unauthorised access to a social-project reporting system, discovered on 21 September. October reporting corroborates that investigation. [S302][S303]
CATEGORIES	The notice lists potentially affected identity, contact and programme-related health information. It does not confirm that every category was accessed or establish an affected-person total. [S302]
BOUNDARY	The hospital states that care continued and that no evidence of public disclosure or misuse had been identified. The possible access and exact extent remained under investigation.

RESPONSE	Separate programme reporting from clinical systems. Identify the actual data categories and notify people through a trusted channel appropriate to the established scope.

Bottom line

Validate programme scope without inferring general patient access.

Confirmation of the investigation is not confirmation of every allegation circulating online. The report does not infer a ransomware family, general patient-database access, completed recovery or a legal finding from the interval between discovery and public reporting.

Y

CASE Y

A digital-asset platform and an investor's subsequent-event notice

Digital-asset services

Investor-authored mirror; financial effect unresolved

REPORTED BY AN INVESTOR	An investor-authored financial statement identifies a cyberattack at a digital-asset platform on 2 November. The statement was authorised on 12 November and read on an independent mirror. [S169]
BOUNDARY	The investor says possible financial losses and valuation effects could not yet be estimated reliably. The mirror was not matched to a readable official-host copy. Final loss, recovery and customer reimbursement are not established here.
RESPONSE	Keep platform availability, asset reconciliation and customer obligations separate. Use the accountable operator's validated update before assuming a withdrawal or refund process is complete.

Bottom line

Reconcile assets and customer obligations from validated updates.

The platform retains a generic role. An unrelated 30 October distribution discussed in the same financial statement is not the cyberattack date. Press estimates are not adopted as a final financial outcome. [S169]

Z

CASE Z

A project portal with confirmed access to registration information

Financial project services

Official notice; name withheld

CONFIRMED	A financial institution's official portal notice says it identified and contained an incident on 4 October. It identifies unauthorised access involving identity and contact details, access credentials and project funding-account information. [S172]

BOUNDARY	The page does not establish its publication date, an affected-person total, a plaintext-password disclosure, an actor or a final financial outcome. Its statement that the portal would remain unavailable does not establish restoration by this cut-off.
RESPONSE	Contact affected users through a trusted route, validate relevant credentials and protect project-payment details. Define the minimum portal function and reconcile delayed work after recovery.

Bottom line

Validate credentials and project-payment information.

The report withholds the institution's name because broad independent reporting was insufficiently established. A separate December 2025 incident discussed in later financial reporting is not joined to this October event. [S172]

5.7 Recent activity: 8–22 November

The closing fortnight includes announcements, recovery updates, advertisements and operations concerning older conduct. It must not be read as a count of new November intrusions.

Published or updated	Item	Evidence and time boundary	First response
9 November	Cuiabá shared-service follow-up	State incident on 1 November; licensing effects, no second municipal intrusion [S167] [S268]	Reconcile licences and extended deadlines
11 November	Bank-associated lead advertisement	Unverified; claimed freshness belongs to the seller [S1]	Validate provenance and owned accounts
12 November	CVP market notice	Detection on 6 November; current and former customer populations [S126][S226]	Scope categories and customer protection
12 November	Investor financial statement	Describes 2 November digital-asset platform event; final financial effect unresolved [S169]	Reconcile assets and obligations
13 November	Treasury notice	Detection on 4 November; two distinct data populations [S127]	Validate access and trusted contact processes
13 November	Digital-commerce notification reporting	Company awareness reportedly 12 October; no new intrusion date or legal conclusion inferred [S173]	Establish categories and notification scope

Published or updated	Item	Evidence and time boundary	First response
13 November	Public-safety platform investigation reporting	Police and municipal accounts quoted by press; legitimate-user disclosure allegation and separate provider-camera reporting remain distinct [S323]	Validate permissions, data access and service boundaries
14 November	Unimed Natal notice	Care continued with alternative procedures; data theft and completed restoration not established [S166][S266]	Test clinical and administrative functions separately
15 November	Education website attempt reporting	Attributed ministerial account; no successful access or origin established [S309]	Validate service evidence
16–19 November	Santos recovery and contingency updates	One incident beginning on 6 November [S128][S229] [S230]	Test administration and operational fallback separately
16–19 November	Belo Horizonte guide and refund updates	Altered guides during 14–16 November; refund process subsequently started [S233]	Reconcile beneficiaries, refunds and replacement payments
16 November	Court file-exposure reporting	Court-attributed confirmation on 14 November; own-host notice unavailable, no established actor [S179]	Validate file scope and preserve the service boundary
16–19 November	CTIR security-guidance updates	Mail-client and web-server guidance updated; content-management guidance updated on 10 November; no incident count [S320][S321] [S322]	Match deployed services to current official guidance
17 November	Pix-labelled database advertisement	Explicitly labelled 2025 material; no new 2026 intrusion established [S1]	Check age and source before containment
17 November	PF international Radar announcement	Underlying actions during May–September; eight domains disabled in Brazil [S129]	Use relevant notifications without importing international totals
17 November	Social-benefit account investigation	Alleged unauthorised access and transfers; no conviction [S130]	Validate affected account and transaction scope
17 November notice	University academic-list investigation	Official statement confirms an investigation; separate equipment-failure downtime was not malicious per university [S196]	Keep data-exposure assessment and hardware restoration separate

Published or updated	Item	Evidence and time boundary	First response
18 November	Bank customer-data reporting	Press quotes a notice describing valid-credential misuse; direct statement unavailable [S131]	Preserve the distinction from a bank-system intrusion
18–19 November reporting	Bank customer-registration access	Bank notice quoted by press describes detection on 12 November and credential revocation; standalone notice unavailable [S194]	Separate registration access from the bank's no-system-intrusion and no-linked-transaction findings
19 November	Delivery-platform registration reporting	Press quotes a company response; categories and populations differ [S132]	Obtain an authoritative, population-specific scope
19 November	Health-benefits provider notice	October access and subsequent phishing; corporate-provider scope only [S165]	Validate contacts, payment details and access
19 November	Business-software customer-table advertisement	Unverified provider-associated data claim [S1]	Validate provider and client scope
19 November	Telephone-message facility investigation	Operation on 18 November; devices and alleged activity under investigation [S133]	Review message abuse and independent call verification
19 November reporting	Delivery-platform data notice	Company-attributed account identifies containment on 14 November, with categories varying by user role [S195]	Give population-specific guidance; do not infer payment-account access
20 November press note	Public-information website	Institution-authored note reproduced by press describes a possible attack and unavailable site [S197]	Preserve the uncertainty and validate current service status
22 November post	Business-information export claim [S1]	A forum post describes purported directory, professional-profile and support-request data	Source assertion only; no authenticated records, patient-data finding, intrusion or current access established
22 November post	Hosted customer-management export claim [S1]	Separate offer describes purported contact, website-project and support-case records	No authenticated origin, current access, acquisition date, customer impact or sale established
November research	Multicountry point-of-sale campaign	Research describes an August discovery, not new November infections [S232]	Validate affected software and investigate relevant endpoints

The bank and platform press accounts remain attributed reporting, with names withheld because the report did not establish a first-party source receipt. Their stated exclusions must travel with the event: no unsupported password, token or payment-data impact is added.

5.8 Important exclusions and historical context

Item	Treatment	Reason
March payment-provider laundering operation	Enforcement context [S104]	Alleged underlying intrusion occurred in August 2025
July health-operator regulatory proceeding	Regulatory context [S114]	Concerns 2025 ransomware; proceeding is not a final sanction
October municipal health-data action	Regulatory outcome [S125]	Underlying gazette disclosure occurred in September 2025
Cross-border laundering investigation	Enforcement context [S117]	Foreign institution and historical intrusion
Bank closure message	Excluded from malicious-incident examples [S112]	Source attributes it to an operational communication error
Preventive agency shutdown	Precautionary response [S124]	Authority says no intrusion or document leakage occurred at the agency
Unconfirmed recent aggregator entries	Not treated as confirmed incidents	Original disclosure and event identity remain unestablished
Fiction-labelled financial story	Excluded entirely [S189]	The article explicitly describes a fictitious scenario, not a verified incident
Historical university, utility, healthcare and logistics stories	Excluded as new events [S184][S190] [S191][S192][S193]	Earlier event dates or undated control changes; current search visibility does not establish a new intrusion
False-alert headline naming a regulator	Same warning-platform event [S187] [S113]	No separate regulator-system incident or additional case established

These exclusions preserve the meaning of the year. A current news page can describe an earlier intrusion, an investigation or a precautionary action. None should silently become another confirmed 2026 breach.

5.9 Other bounded disclosures and reports

Publication or event	Role and source	What can be retained	What remains separate
21 April reporting	Financial institution [S310]	Press reproduces a bank statement about a security incident and gradual service normalisation	No authoritative loss or affected-account total; name withheld

Publication or event	Role and source	What can be retained	What remains separate
1 June identification	Financial cooperative [S174]	Official notice identifies personal, contact and account-contract data	The cooperative excludes passwords and transaction-enabling data; publication date unresolved
21 July event; 27 July reporting	Retail financial-services network [S311]	Temporary restrictions followed reported atypical activity	Individual anecdotes are not a national loss total; direct notice unavailable
17 September incident; later court notices	Judicial-deposit platform [S175]	Court notices describe bank-reported staged service restoration	Court systems distinguished from the bank platform; loss estimates not adopted
4 August suspicion; 8 October statement	Hospital [S181]	Hospital-authored statement confirms access and obtaining patient data; care continued per institution	Primary reproduced by original recipient; count unknown, no public misuse identified then
May reporting	Public-benefits query service [S170]	Independent reporting quotes an operator account of data access	Population terminology and original operator evidence unresolved; not a named confirmed case
5 November update	Financial-sector institution [S177]	Official HTML confirms unauthorised access related to payment processes after 26 October suspicion	Investigation and individual notices continued; no affected total or final harm finding
21 September notice	Shared judiciary services [S178]	Official notice describes access detected on 18 August and 3 September, with both systems restored	Different system dates do not establish one actor or separate intrusions into every regional court
27 October reporting	Public-information portal [S180]	Operator-authored statement describes altered images and preventive suspension	No broader system or sensitive-data impact identified by operator at that time; investigation continued
23 February notice	Examination-services provider [S182]	Official notice confirms portal instability on 20 February and a deadline extension	No official ransomware, extraction or actor confirmation established
30 April reporting	Financial-services provider [S183]	Bank-attributed notice describes preventive suspension after atypical movement	The bank had not confirmed a hacker attack; no-loss and no-leak statements remain attributed
October interruption; 6 November follow-up	Electronic court-service platform [S185]	Professional body's own account describes external-access interruption and continuity measures	Participant statement, operator primary unavailable; intrusion and data theft not established

Publication or event	Role and source	What can be retained	What remains separate
Detected 12 November; reported 18–19 November	Bank [S194][S325]	Press quotes the bank's notice confirming unauthorised registration-data access through a misused valid credential, which was revoked	Standalone notice unavailable; no system invasion, password/token exposure or linked transactions identified, according to the bank; no population total
Identified 14 November; reported 19 November	Delivery platform [S195] [S326]	Company-attributed notice distinguishes customer phones, partner phone/CPF and varying courier registration or payout-account fields	Direct notice unavailable; do not assign all fields to everyone or infer account access; company excludes password/card impact and reports continued service
17 November notice; 21 November coverage	Public university [S196] [S327]	Official notice investigates an exposed list of names, courses and academic-performance coefficients	No intrusion, origin or affected total established; separate hardware-failure outage was not malicious per institution
20 November press note	Public-information website [S197][S328]	Full institution-authored note reproduced by two outlets describes a possible attack and unavailable portal	Original host unavailable; no confirmed theft, actor, broader system impact or completed recovery

Utility customer data: exposure and the operational boundary

Cemig's 14 May material fact identifies personal-data exposure affecting approximately 135,000 customers identified at that stage. The stated categories include registration and contact information, CPF identifiers and invoice values. Wider reporting corroborates the disclosure. [S314][S315]

The company says unauthorised database access was blocked after detection and operations were unaffected. These are the company's dated findings. They do not establish access to power-control systems, a service interruption, an actor or a final affected-person total. [S314]

For customer protection, genuine invoice and identity details can make an unauthorised collection request persuasive. Validate payment beneficiaries and support contacts independently. Keep that data-protection response separate from any operational-technology investigation unless supporting evidence connects them.

These entries preserve supported developments without treating every press report as a fully verified incident dossier. Their scope does not authenticate an underground advertisement or establish a common actor. No notification interval is used to decide legal compliance.

KEY TAKEAWAYS

01

Copied records, altered instructions and unavailable administration require different owners.

02

Recent publications often update earlier incidents or investigations.

03

Preserve initial and later findings without turning either into a broader assurance.

CHAPTER 06

Disruption, defacement and public-service trust

THIS CHAPTER ANSWERS

Was a service unavailable, altered or merely named?

2025

the event year stated inside a disruption claim circulated in 2026

6.1 A historical claim circulating in the current window 57
6.2 Three kinds of public-service harm 58
6.3 An evidence ladder for availability claims 59
6.4 The October calendar supplies context, not attribution 59
6.5 Timeline: dates with their evidence type 60
6.6 Continuity decisions that survive uncertain attribution 60
6.7 What would strengthen or change the assessment 61

CHAPTER 06

Disruption, defacement and public-service trust

IN SHORT

Disruption language is easy to repeat and hard to validate. A January forum narrative claims denial of service but dates the alleged outage to January 2025. Official sources separately describe false public alerts, upload-related defacement and administrative recovery. None supports an election-related national outage finding here. Measure the user task, preserve the relevant time and distinguish website availability from control of a service. Test an alternate public communication route before the next incident.

6.1 A historical claim circulating in the current window

A January post and an October repetition claim denial of service and data extraction at a state environmental body. The narrative explicitly dates the alleged inaccessibility to 9 January 2025. Its circulation belongs to this report's 2026 post window; the alleged disruption does not. [S1]

The material does not independently establish the duration, geographic reach, cause or operational effect. Its political accusations add no technical evidence and are omitted. The report withholds the subject's name because the incident naming requirements were not met.

A current post is not necessarily a current incident. The distinction changes both a timeline and a response. A fresh claim about an old event may justify checking records or monitoring impersonation. It does not justify announcing a new outage or attributing current user problems to the claimant.

Proposition	What is held	What is not established
A denial-of-service statement circulated in 2026	Dated forum narrative and repetitions	Independent traffic or service measurements
The narrative identifies an earlier date	The poster states January 2025	An authenticated event chronology
A data quantity is claimed	The advertisement's assertion	Authentic data, unique people or a verified transfer
Political language accompanies the narrative	The source contains advocacy	A technical attribution, public mandate or valid motive finding

The useful next step is an internal event check by the actual service owner. Match the time, user reports, supplier notifications and service records. An anonymous assertion alone cannot settle whether the failure was hostile, accidental or unrelated.

6.2 Three kinds of public-service harm

Availability is whether the intended user can complete a task. Integrity is whether the task presents and records the right information. Confidentiality is whether the information reached an unauthorised party. One incident can affect several, but evidence for one does not establish the others.

The public-warning case in chapter 5 concerns false messages and a suspended platform, with alternative channels described by authorities. It raises message authenticity and continuity questions. It does not establish a real emergency, an attacker identity or a failure of every local monitoring function. [S113]

CTIR's upload-related warning describes defacement behaviour on public-facing platforms. A changed web page is evidence about publication integrity when validated. It does not, by itself, establish access to the entire organisation, electoral systems or operational control. [S152]

The Santos updates concern administrative recovery and contingency access. The authority's statement about maintained cargo capacity must be read beside user reports about slower administration. Capacity, transaction delay and restoration status measure different things. [S229][S228]

A 5 November operator statement reproduced by industry reporting describes unusually high DDoS volumes over the preceding six months. The operator states that the government digital-service environment suffered no interruption or intrusion. No public traffic quantity or actor attribution is established here. [S171]

Separately, 15 November reporting quotes an education minister describing attempted attacks against an assessment website and saying they were controlled. The report supplies no successful-access finding, attempt total or established origin. Neither account establishes election-system impact. [S309]

A university's 22 October statement describes preventive digital-service restrictions following a security alert. It expressly says no intrusion or unauthorised system access had been identified at that stage. Preventive unavailability must remain separate from a confirmed hostile outcome. [S308]

A September union notice describes an attack against its online voting service and a rescheduled assembly. Although the participants were bank employees, the notice does not establish an incident in bank infrastructure or customer accounts. Keep the affected service owner separate from the employer of the participants. [S188]

6.3 An evidence ladder for availability claims

Evidence	Appropriate conclusion	Operational use
A claimant names a website	The claimant asserted targeting	Notify the owner through the agreed route and check relevance
A screenshot shows an error	A page failed in that displayed context	Reproduce the user task through authorised service monitoring
The owner confirms degradation	A scoped service problem was confirmed	Apply continuity priorities and publish a timed update
Service records show abnormal hostile traffic	The owner has technical evidence for investigation	Coordinate mitigations and preserve records
A competent investigation attributes the activity	An attribution is available with stated confidence	Attribute the conclusion to that source and retain its limits

These are analytical response stages, not a score or a statement that the final stage was reached in the historical forum case. A screenshot may show a genuine failure while leaving its cause unresolved. Avoid presenting it as a measurement of national availability.

6.4 The October calendar supplies context, not attribution

The official electoral calendar scheduled the first round for 4 October and a possible second round for 25 October. That timetable creates a predictable communication and continuity planning period. It establishes no relationship between the calendar and a cyber incident. [S17]

This edition identifies no source-verified national election DDoS event from the evidence presented. That coverage statement is not a claim that no attempted activity occurred. Public websites, campaigns, courts and electoral services are distinct subjects with different owners.

The report takes no position on candidates, parties, court decisions, government policy or foreign relations. A claimant's political description remains a claimant's statement when relevant. It cannot replace service evidence, and loaded accusations are not reproduced.

A responder should verify the affected function before invoking an election scenario. Is the issue a public information page, staff email, a campaign service or an electoral administration system? The answer sets the continuity owner and the appropriate public statement.

A 26 October relay says an actor released political-organisation data after an earlier breach claim. The attribution and release remain unverified. The post does not authenticate contents, origin, a unique-person total or election impact. No verified link to the earlier membership offer is established. Validate the actual organisation and affected service without adopting the claimant's political framing. [S1]

6.5 Timeline: dates with their evidence type

24 Jan 2026	**Forum poster** A forum narrative circulates a disruption allegation explicitly dated to January 2025 [S1]
21 May 2026	**Official source** CTIR publishes upload-related defacement guidance; campaign dates are not individually established [S152]
20 Jun 2026	**Official source** Public notices describe false alerts and alternative warning channels [S113]
8 Sep 2026	**Official source** CTIR warns about search-result poisoning involving public-sector web surfaces [S120]
4 Oct 2026	**Official source** Official calendar date for the first election round [S17]
7 Oct 2026	**Official source** PF announces an investigation into a July data-theft and extortion event [S122]
16 Nov 2026	**Official source** Santos publishes an administrative-recovery update about the 6 November incident [S128]
19 Nov 2026	**Official source** Belo Horizonte updates its payment-guide and refund notice [S233]

The entries distinguish claims, official guidance, calendar context and incident reporting. This is not an incident-count chart. Several publication dates concern earlier activity, and the entries must not be summed as simultaneous disruptions.

6.6 Continuity decisions that survive uncertain attribution

First, define the minimum public task. A port may need a safe registration and access process before every administrative application returns. A municipality may need a verified payment route before normal page design is restored. The priority belongs to the operational owner.

Second, establish a trusted alternate channel before the main one fails. Publish its purpose and authentication expectations in normal conditions. During an incident, time-stamp updates and explain which functions work, which are delayed and what users should avoid.

Third, preserve integrity during fallback. A manual process can maintain service while introducing reconciliation, approval or fraud risks. Assign who validates beneficiaries, records exceptions and reconciles the eventual system of record.

Fourth, test recovery against user tasks. A server being reachable does not show that an appointment, payment or shipment can be completed correctly. Ask operational staff to demonstrate the required task and record the result.

Finally, keep public statements proportionate to established facts. Say what the owner has confirmed, when that finding was made and when the next update is due. Separate a claim under investigation from an observed service condition.

6.7 What would strengthen or change the assessment

An independently confirmed current outage, a first-party incident notice, corroborated service records or a competent technical attribution would strengthen a specific finding. The evidence would need to identify the function and event date, not just repeat the same claim.

A later denial or a documented non-malicious cause would also change the assessment. Preserve that correction in the same incident record. Removing an earlier uncertainty without recording the new source makes the record less useful to defenders.

KEY TAKEAWAYS

01

Keep publication time separate from the alleged outage date.

02

Availability, message integrity and data access require different evidence.

03

Exercise trusted alternate channels and reconcile every fallback transaction.

CHAPTER 07

Ransomware, financially motivated groups and espionage

THIS CHAPTER ANSWERS

Which actor labels help a decision?

206

Brazil-associated ransomware listings during the reporting window

7.1 The ransomware listing population 63
7.2 Four regional comparators 66
7.3 Payment identities: BREEZE COMET 67
7.4 Banking malware: TCLBANKER 68
7.5 Browser identity: UnregStealer 69
7.6 Espionage and information theft: Armored Likho 70
7.7 Other Brazil-relevant financial research 71
7.8 Official campaign warnings and the control owner 73
7.9 Relationship map and technique view 74

CHAPTER 07

Ransomware, financially motivated groups and espionage

IN SHORT

Ransompedia records 206 Brazil-associated listings, distributed across 55 group labels. Three labels account for 72 listings, or 35.0% of the total. Listings remain claims. Separate research describes payment-identity theft, banking malware, browser-session theft and an attributed espionage campaign. Those sources do not establish common operators or a national victim total. Prioritise the access and recovery controls supported by each source rather than using the actor name as the control plan.

7.1 The ransomware listing population

The listing count describes public extortion visibility. Ransompedia records 206 Brazil-associated listings dated within 1 January–22 November 2026. It records 160 during the full calendar year 2025. These are different observation periods, not a like-for-like annual growth rate. [S2]

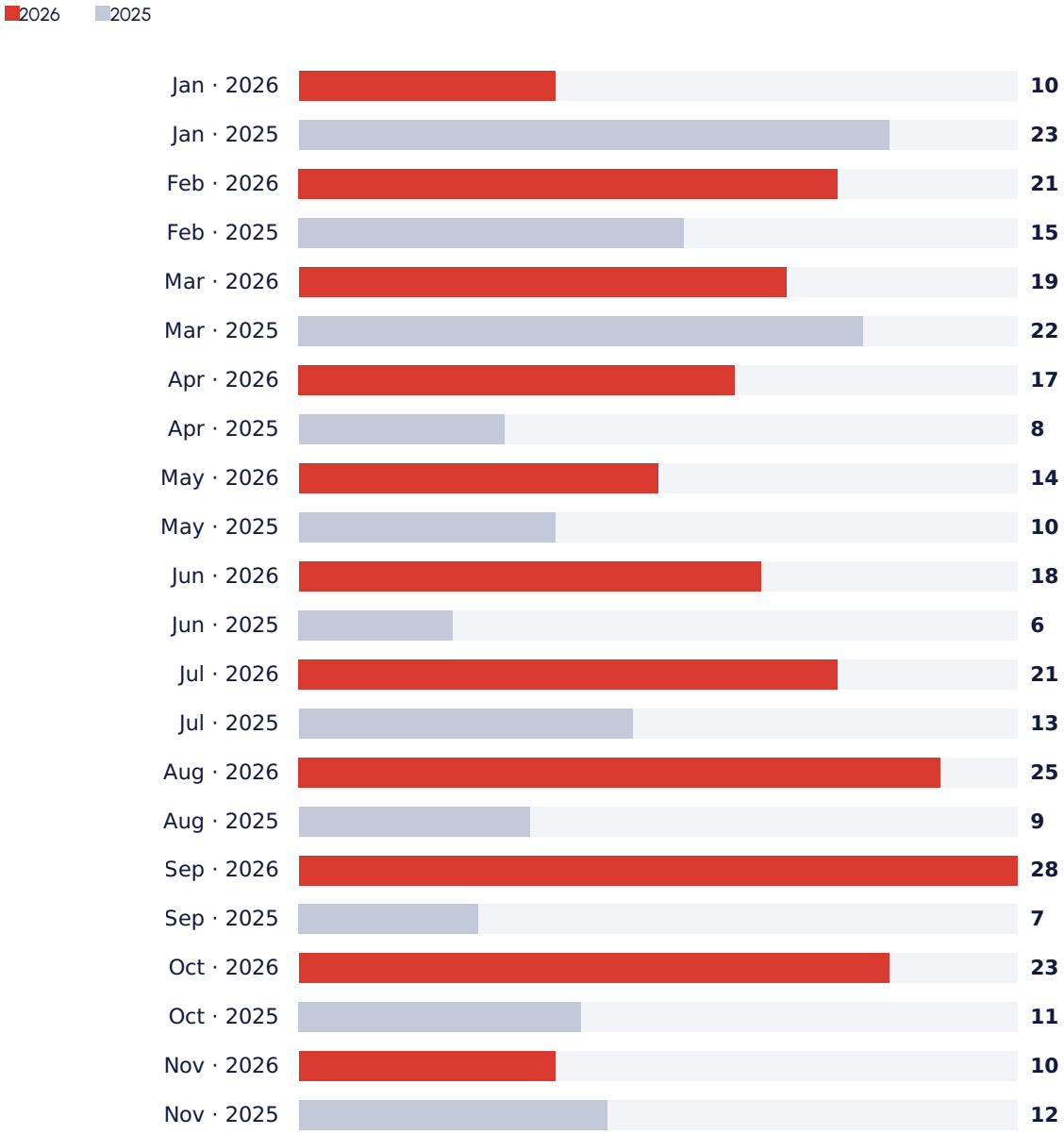
A listing does not independently establish encryption, the amount of copied data, payment of a demand or the date an intrusion began. It may concern a supplier, a subsidiary or historical material. The table therefore keeps the unit as listings throughout.

Ransompedia label	Listings in the window	Share of 206	Interpretation
Thegentlemen	34	16.5%	Largest label in this snapshot; no implication about every listed claim
Lockbit5	27	13.1%	Preserve this recorded label; no automatic identity continuity with other names
INC Ransom	11	5.3%	A listing label, not a confirmed incident count
Other labels	134	65.0%	Distributed across the remaining 52 labels
Total	206	100%	Brazil-associated listings in the defined window

The three leading labels total 72. Their combined share is 35.0%, calculated directly against 206. Rounded individual percentages need not reproduce the rounded combined share. Group labels do not establish common membership, infrastructure or command.

The monthly series is 10, 21, 19, 17, 14, 18, 21, 25, 28, 23 and 10 listings from January through November. November ends at the cut-off. September has the largest observed monthly count, but publication timing cannot establish peak intrusion activity. [S2]

Brazil-associated ransomware listings by month; November is partial



Source: Ransompedia Brazil-associated listing claims [S2]. January-November in each year; November 2026 covers 1-22 November, closing day partial; November 2025 is the full month. Unequal periods; not a matched-period growth rate.

The previous-year bars show the whole corresponding month of 2025. November 2026 is partial, so its bars are not a matched-period comparison. Listing publication dates do not establish intrusion dates. [S2]

The practical response is broader than following the leading names. A recovery exercise should test access to the identity service, backups, business data and external communications. An extortion response also needs a data owner even when restoration succeeds.

Thegentlemen

Ransomware/extortion listing label | No nationality or state attribution made

IN BRAZIL, 2026

2026-01-01–2026-11-22

34 Brazil-associated listings

CLAIMED TARGETS

Listed Brazil-associated organisations; outcomes unverified

SEEN IN PUBLIC REPORTING

[S2] 34 listing assertions, not confirmed intrusions or encryption outcomes.

OUR ASSESSMENT

34 listing assertions, not confirmed intrusions or encryption outcomes.

CONFIDENCE

High for retained listing count; underlying claims unverified

Lockbit5

Ransomware/extortion listing label | No nationality or state attribution made

IN BRAZIL, 2026

2026-01-01–2026-11-22

27 Brazil-associated listings

CLAIMED TARGETS

Listed Brazil-associated organisations; outcomes unverified

SEEN IN PUBLIC REPORTING

[S2] 27 listing assertions, not confirmed intrusions or encryption outcomes.

OUR ASSESSMENT

27 listing assertions, not confirmed intrusions or encryption outcomes.

CONFIDENCE

High for retained listing count; underlying claims unverified

INC Ransom

Ransomware/extortion listing label | No nationality or state attribution made

IN BRAZIL, 2026

2026-01-01–2026-11-22

11 Brazil-associated listings

CLAIMED TARGETS

Listed Brazil-associated organisations; outcomes unverified

SEEN IN PUBLIC REPORTING

[S2] 11 listing assertions, not confirmed intrusions or encryption outcomes.

OUR ASSESSMENT

11 listing assertions, not confirmed intrusions or encryption outcomes.

CONFIDENCE

High for retained listing count; underlying claims unverified

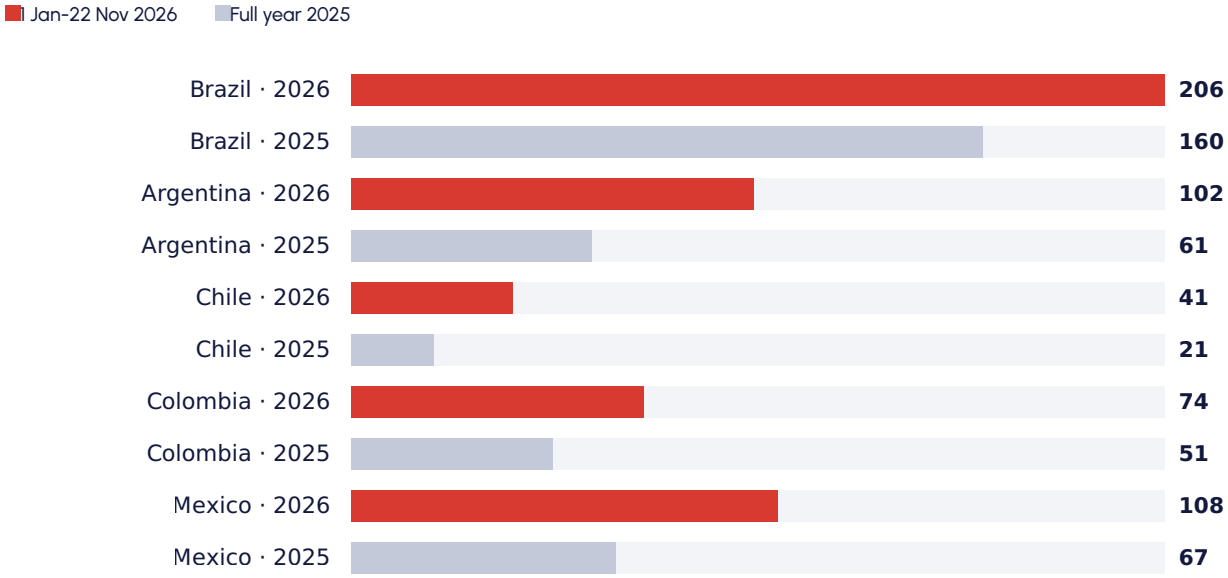
7.2 Four regional comparators

Country	2026 to cut-off	Full 2025	Why it provides context
Brazil	206	160	Report country; scale and disclosure conditions differ from peers
Argentina	102	61	Neighbouring large service and industrial economy
Chile	41	21	Regional finance, mining and infrastructure context
Colombia	74	51	Large regional services and financial market
Mexico	108	67	Large Latin American industrial and financial market

Comparison countries were selected as examples to provide context only; they do not imply a ranking or political assessment.

Source: the same Ransompedia observation snapshot and reporting dates. [S2]

Dated ransomware listings across Brazil and four regional peers



Source: Ransompedia country-associated listings, each an extortion claim [S2]. 2026: 1 January-22 November, closing day partial; 2025: full year. Unequal periods; not a national security ranking.

Brazil has the highest listing count among these selected peers in this snapshot. That statement concerns the recorded population. It is not a ranking of national security, institutional competence or per-organisation risk.

The table has no common denominator for economic size, connected organisations, reporting propensity or attacker coverage. Do not turn the absolute counts into a probability that a Brazilian organisation will suffer an incident. A business with suppliers across these markets should use the comparison to ask where continuity arrangements need testing.

7.3 Payment identities: BREEZE COMET

Google's September research describes BREEZE COMET as financially motivated and says its investigations began in 2024. Its Brazil-focused cases include financial institutions, retail and ecommerce, and payment-related service dependencies. The report covers activity extending through 2026. [S18]

A transaction identity can matter more than a login. Google describes theft and abuse of valid mutual-TLS material and payment-related secrets. It also describes social engineering, remote-management tools and access through supplier relationships. This is the vendor's account of investigated cases, not a claim that every payment provider shares the same route.

The defensive decision is to inventory who can obtain, copy, replace and revoke transaction certificates and signing material. Separate access to the application from authority to move money. Check the evidence behind beneficiary changes and emergency credential replacement.

A report about a supplier does not establish every downstream client as a victim. Nor does a forum offer containing certificate language establish a relationship with this campaign. The private offer and public technical research remain separate evidence streams in this edition.

BREEZE COMET

Previously tracked by Google as UNC5669

Financially motivated activity | Financial motive according to Google

IN BRAZIL, 2026

2026-09-01
Research covers investigations beginning in 2024 and activity through 2026

CLAIMED TARGETS

Financial and payment-related services

SEEN IN PUBLIC REPORTING

[S18] Review transaction identities and supplier authority; no link to selected sellers is established.

OUR ASSESSMENT

Review transaction identities and supplier authority; no link to selected sellers is established.

CONFIDENCE
Vendor research; no nationwide prevalence

7.4 Banking malware: TCLBANKER

Elastic's May research describes TCLBANKER, tracked in its REF3076 activity, as banking malware with communications and credential-related capabilities. It describes malicious installation, DLL loading and spread through authenticated messaging and email contexts. [S19]

The article's monitored banking-domain list describes what the malware recognises. It does not establish that each listed bank suffered an intrusion. A customer-device infection and a bank infrastructure incident require different response owners.

The business implication is that a message from a familiar account may still be hostile. Banks, merchants and employers should test how staff report unexpected attachments from trusted contacts. Device isolation must be coordinated with invalidation of affected sessions and review of subsequent activity.

Elastic discusses similarities with earlier malware. Those relationships remain the vendor's technical assessment. The report does not infer a single operator behind all similarly behaving tools or join them to anonymous data sellers.

TCLBANKER / REF3076

Banking-malware campaign | Financial activity described by Elastic

IN BRAZIL, 2026

2026-05-07
Campaign research published

CLAIMED TARGETS

Banking users and authenticated communications

SEEN IN PUBLIC REPORTING

[S19] Validate relevant installation and session evidence; monitored bank domains are not bank victims.

OUR ASSESSMENT

Validate relevant installation and session evidence; monitored bank domains are not bank victims.

CONFIDENCE
Vendor research; bank-infrastructure impact not inferred

7.5 Browser identity: UnregStealer

IBM's June publication describes UnregStealer as a human-operated browser-credential theft campaign targeting Brazilian banking users. The research describes a malicious extension, session material and operator interaction, following its discovery in May. [S20]

The response cannot end at changing a password. A malicious extension may retain access to browser activity, and a still-valid session may outlive the password change. Review browser policy, extension provenance, session revocation and transaction activity together.

This is a campaign description, not evidence that the named banking brands' own systems were entered. It also gives no basis for a nationwide count of affected customers. A detection should be validated against the endpoint and account evidence for that customer.

UnregStealer

Browser-credential theft | Financial targeting described by IBM

IN BRAZIL, 2026

2026-06-16

Publication follows May discovery

CLAIMED TARGETS

Brazilian banking users

SEEN IN PUBLIC REPORTING

[S20] Review browser extensions and invalidate affected sessions alongside account containment.

OUR ASSESSMENT

Review browser extensions and invalidate affected sessions alongside account containment.

CONFIDENCE

Vendor research; no national affected-user total

7.6 Espionage and information theft: Armored Likho

Kaspersky's 3 July research identifies victims in Brazil, Russia and Kazakhstan, mainly in government and electrical-power infrastructure. It attributes the BusySnake Stealer campaign to Armored Likho with medium confidence, based on tools and network activity. [S161]

The attribution is the vendor's, with its stated confidence. The article describes phishing archives, modular credential and session theft, and remote access. It characterises the activity as mixing financial targeting of individuals with espionage against organisations.

The research gives no named Brazilian organisation, Brazilian victim count, state sponsor or nationality attribution. It establishes no disruption of power operations. Its circumstantial association with another actor is insufficient to create a confirmed operational relationship in this report.

Government and energy defenders should review privileged-session exposure, remote access and separation of administrative systems from operational environments. A country appearing in a victim geography is a reason to assess the described behaviour, not evidence that a specific national facility was affected.

Armored Likho

BusySnake Stealer campaign

Information theft and espionage | Financial and espionage activity according to Kaspersky; no state attribution

IN BRAZIL, 2026

2026-07-03

Original research includes Brazil among victim countries

CLAIMED TARGETS

Government and electrical-power infrastructure; no named Brazilian subject

SEEN IN PUBLIC REPORTING

[S161] Review privileged sessions and remote access; no power-operational disruption established.

OUR ASSESSMENT

Review privileged sessions and remote access; no power-operational disruption established.

CONFIDENCE

Medium-confidence attribution by Kaspersky

7.7 Other Brazil-relevant financial research

Kaspersky's March GoPix research describes clipboard-related payment fraud affecting Brazilian users. The relevant control is verification of the final beneficiary and payment details through a trusted display or process. Brand recognition alone does not validate the destination. [S105]

Its April JanelaRAT article describes a financial threat in Latin America. The Brazil detection figure discussed there belongs to 2025, so this report does not present it as a 2026 count. The research remains useful for reviewing endpoint and account controls. [S106]

A financial motive inferred from observed theft should not become a nationality attribution. These campaigns are included because the primary research supports Brazilian relevance and useful defensive actions. Similar language or market geography does not establish cooperation between them.

Kaspersky's March BeatBanker research describes Android malware affecting users in Brazil, including banking and mining functions and later BTMOB remote-access variants. Its delivery impersonates familiar applications. This supports checking application provenance and device permissions, without a bank-infrastructure intrusion finding. [S23]

Its June research describes malicious WhatsApp attachments installing legitimate remote-management software across several countries, including Brazil. The original account dates observation to June, despite later forum circulation. Attribution remains low confidence, with no known group established. Review unsolicited installation and remote-support permissions. [S24]

Check Point's September Gambling Goblin research describes Brazilian government and education web servers used for search-related fraud, in a campaign tracked since mid-2025. It describes malicious Apache modules. Its Earth Berberoka link is the vendor's medium-to-high-confidence assessment; no state sponsorship is inferred. Review server modules and delegated publishing. [S25]

Gambling Goblin

Web-server abuse and search-related fraud | Criminal activity according to Check Point; no state attribution

IN BRAZIL, 2026

2026-09-02
Campaign tracked since mid-2025

CLAIMED TARGETS

Government and education web servers

SEEN IN PUBLIC REPORTING

[S25] Review server modules and publishing authority; the Earth Berberoka link is the vendor assessment.

OUR ASSESSMENT

Review server modules and publishing authority; the Earth Berberoka link is the vendor assessment.

CONFIDENCE
Medium-to-high-confidence link per Check Point

KREMLIN: banking sessions and misleading names

Elastic's 14 September research describes REF9334 and its KREMLIN toolkit, tracked since May 2025. The operation uses document lures and malicious browser extensions to steal credentials and session information. The name supplies no Russian-state attribution. [S304]

The relevant owner is the endpoint and browser-identity team. Validate unexpected extensions, preserve relevant installation evidence and invalidate affected sessions. A bank-themed lure does not establish access to that bank's infrastructure. No common operator with UnregStealer or TCLBANKER is established here.

PhantomEnigma: trusted infrastructure can carry an unsafe document

ANY.RUN's 16 July investigation describes Brazilian government-hosted delivery infrastructure and police-themed lures. The researcher distinguishes abused delivery hosts from confirmed campaign targets. Its link between the specific backdoor arm and PhantomEnigma carries medium-to-high confidence. [S305]

This supports reviewing publishing authority, suspicious attachments and downstream execution even when a message passes sender authentication. It does not make every cited public body a named incident subject. The report adopts no national victim count or shared-operator link to other campaigns.

Banking integration packages and certificate authority

Socket's 28 May research identifies a malicious package impersonating a banking integration library. The researcher describes theft of client identifiers, PFX certificate archives and their passwords. That material could enable integration impersonation, depending on permissions and the financial service's controls. [S313]

Validate the publisher and delivered package, then establish whether real authentication material was used. Revoke and replace exposed certificates and relevant credentials. The finding does not establish an intrusion into the impersonated institution or a link to the certificate advertisement in Case I.

7.8 Official campaign warnings and the control owner

Official warning	What the source supports	Decision for the owner
False government-service pages	CTIR describes phishing using service-related lures [S147]	Verify service messages through the authorised service route
Legitimate subdomain abuse	CTIR describes malicious material under government-associated addresses [S148]	Review delegated publishing and unused subdomains
ClickFix prompts	CTIR describes false verification and error instructions [S149]	Teach staff to stop unexpected requests to run local commands
Device-code and token theft	CTIR describes abuse of cloud authentication and session material [S150]	Review sign-in context, session lifetime and token revocation
Possible hands-on-keyboard activity	CTIR explicitly describes a possible campaign [S151]	Investigate relevant evidence without declaring encryption
Upload-related defacement	CTIR describes executable content in upload locations [S152]	Enforce upload policy and separate content from executable services
Gateway credential campaign	CTIR warns of exposed authentication material [S153]	Assess affected access and replace relevant credentials
Search-result poisoning	CTIR describes abuse of government-site visibility [S120]	Check search results, content ownership and published changes

These warnings describe mechanisms or investigations. Their publication dates do not establish when every underlying event happened, and warning numbers are not victim totals. No political motive is inferred from the affected public-service context.

Provider information, cloud authority and public-web integrity

CTIR's 21 May warning describes provider data, internal documents and source-code exposure. Its 22 May recommendation adds integrity checks for updates and restrictions around administration. These are the authority's findings and recommendations, without confirmation of intrusion at every client. [S316][S317]

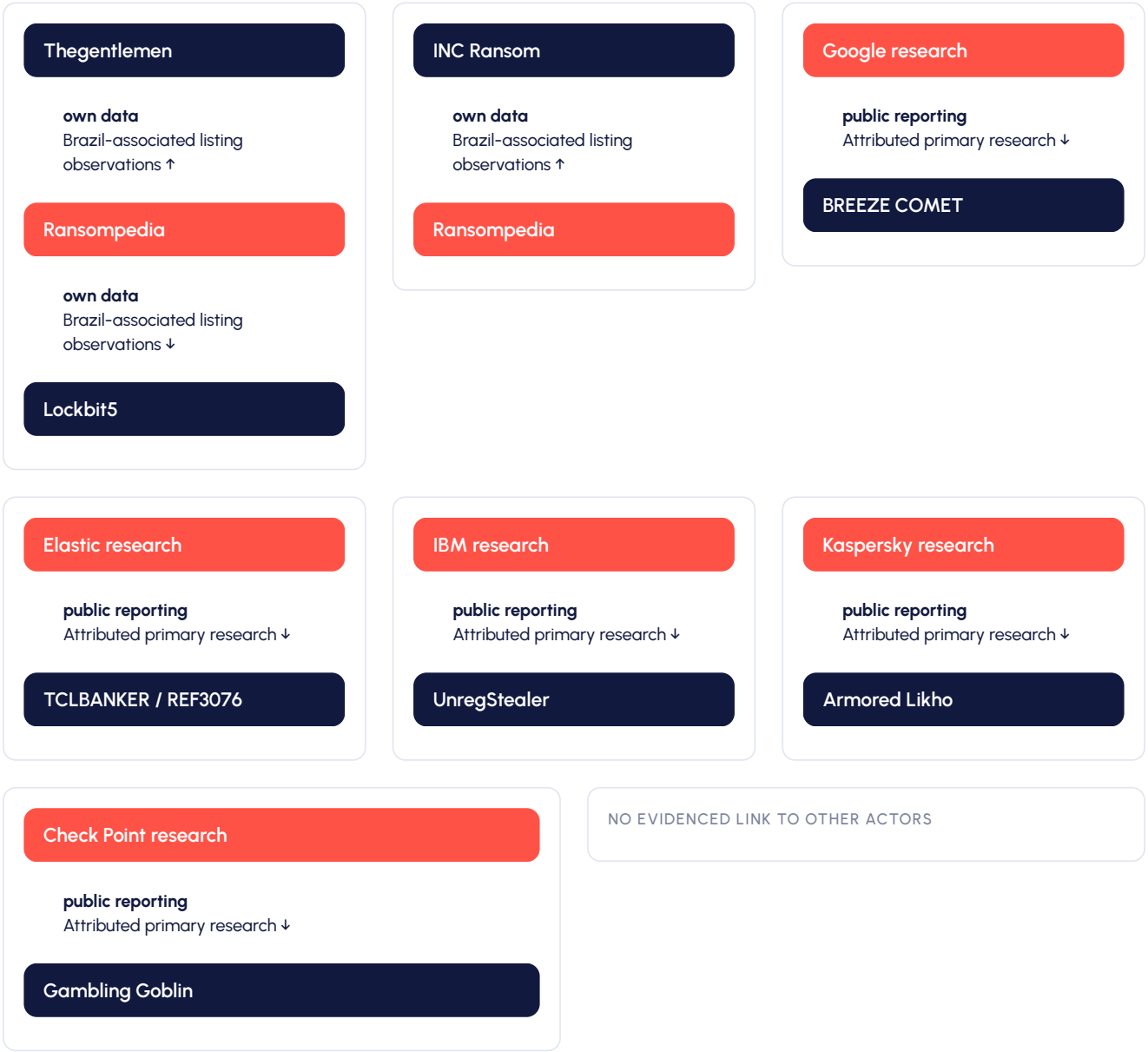
The provider retains a broad role. No affected-government total, new actor attribution or direct link to an access advertisement is inferred. Validate the relevant product, exposed secrets and permitted administration before applying the response to a client environment.

CTIR's 24 June cloud guidance describes privileged-identity and resource-abuse risks, including unauthorised cryptocurrency mining. For the cloud owner, account recovery should include application permissions and unexpected resource provisioning. The notice supplies no national victim or loss total. [S318]

The 14 August website warning describes unauthorised page alterations and calls for investigation of contextual service evidence. A suspicious file alone is insufficient to establish exploitation. This report does not adopt a technical version boundary or count every public site as an incident. [S319]

7.9 Relationship map and technique view

Own post Relay Official statement Public reporting Our observation



The relationship map separates Ransompedia's own listing observations from attributed public research. A research source connected to a campaign means that source described it. It does not mean the publisher participates in the activity.

The map contains no inferred coordination edge between the access sellers, banking malware and ransomware labels. A shared interest in Brazil or credentials is insufficient. A future relationship would need concrete technical or operational evidence and an explicit confidence statement.

TECHNIQUES NAMED IN THE VENDOR RESEARCH, BY TACTIC

Initial Access	Execution	Discovery	Collection
T1566.001 Spearphishing Attachment	T1059.001 PowerShell	T1082 System Information Discovery	T1113 Screen Capture

Behaviours named in Elastic TCLBANKER research [S19]; tactic and technique labels checked against MITRE [S26][S27][S28][S29]. Not a prevalence measurement. [S19]

Tactic	Technique	Control question	Definition source
Initial access	T1566.001, spearphishing attachment	Can staff report an unexpected attachment from a familiar account?	MITRE [S26]
Execution	T1059.001, PowerShell	Can the owner distinguish approved scripting from suspicious activity?	MITRE [S27]
Discovery	T1082, system information discovery	Can endpoint context explain unusual system inspection?	MITRE [S28]
Collection	T1113, screen capture	Can the team investigate unexpected capture activity?	MITRE [S29]

These are source-described behaviours with the technique definitions checked against MITRE. The control questions are analyst recommendations. [S19]

The technique view follows the behaviours described by Elastic for TCLBANKER. It is a focused review aid for one researched campaign, not a prevalence chart or an assertion that each behaviour occurred in every Brazilian case. [S19]

Ask whether the relevant control produces evidence a responder can use. For example, can the team identify an unexpected installation, validate the loaded component and revoke the associated communications session? A technique name without an evidence owner does not close the risk.

KEY TAKEAWAYS

01

Treat 206 listings as claims, with the observation period attached.

02

Separate payment authority, customer-device malware and espionage evidence.

03

Use actor labels to locate research, then assign controls to the behaviour it supports.

CHAPTER 08

Fraud, personal data and payment-card material

THIS CHAPTER ANSWERS

What can an observation establish about fraud?

3

distinct questions: published data, account access and actual financial harm

8.1 Data supports a story; it does not authenticate the caller 78

8.2 The payment-card observation scope 78

8.3 A point-of-sale campaign with a global denominator 79

8.4 Investigations show several fraud paths 79

8.5 Recent account-fraud enforcement 80

8.6 Control the next plausible request 81

8.7 Purpose-bound access and instructions inside documents 81

CHAPTER 08

Fraud, personal data and payment-card material

IN SHORT

Published identifiers, access offers and payment-card material create different response questions. An observed record does not establish a current usable account or a completed transaction. Police reporting shows investigations into impersonation, account abuse and misuse of legitimate access, while technical research describes customer-device theft. Keep each population and status separate. Validate relevant accounts through authorised internal records and provide a trusted route for customers to check unexpected requests.

8.1 Data supports a story; it does not authenticate the caller

The selected advertisements repeatedly combine identifiers with a practical context: a guardian and tuition history, a customer and delivery, a taxpayer and invoice, or a bank relationship. Those combinations are seller claims until validated. Their defensive relevance is the plausibility of an impersonation message. [S1]

A caller who knows a CPF identifier or a recent transaction is not necessarily authorised. Customer service should authenticate through the established process rather than use familiar facts as proof of identity. Do not ask customers to move money to a purported safe account or disclose an authentication code.

The confirmed CVP and Treasury notices make that distinction concrete. They identify registration information and dated exclusions or limitations. They do not establish that a forum seller holds those particular records or that every affected person experienced fraud. [S126][S127]

Exposure and loss require separate evidence. Record the source of a contact, the affected categories and any resulting account activity. Keep suspected fraud, attempted fraud and a confirmed unauthorised transfer distinct in both the customer record and executive reporting.

8.2 The payment-card observation scope

SCOPE OF THE CARD FIGURES

These figures describe a limited Brandefense payment-card observation set. They do not establish current validity, unique cardholders, national card theft or fraud losses.

The accompanying aggregate describes payment-card observations, with its stated units. A repeated card observation is not another cardholder. An advertised status is not an issuer authorisation record, and an advertised price is not evidence of a completed sale. [S4]

The observation set contains 1,229 distinct Brazil-associated card observations, with 1,411 occurrences. Distinct-card observations and occurrences are different units. These values do not establish current card validity or issuer losses. [S4]

The total cannot be joined to customer databases to infer a rate of fraud. It supplies no denominator of active cards issued in Brazil. An issuer comparison would also require validated identity, time and scope, so this edition does not publish named issuer rankings.

No card observation establishes the route by which the information originally left a system. An endpoint infection, checkout interception, old file, reseller and repeated advertisement may all produce similar material. Incident attribution requires additional evidence.

8.3 A point-of-sale campaign with a global denominator

Cybernews's original investigation describes discovery of a point-of-sale information-theft campaign in August 2026. It reports 782 affected systems globally and at least one million unique card records, with most systems described as Brazilian. [S232]

Those are the researchers' global quantities. The exact Brazil-only system count is not established consistently across the reporting, and this edition omits it. No named bank or retailer meets the report's independent confirmation requirements for that campaign.

The research describes use of CVE-2024-49138, a Windows privilege-escalation vulnerability. NVD records affected Windows release boundaries and links the vendor remediation. This is a previously patched vulnerability in a 2026 campaign account, not a newly disclosed vulnerability. [S5]

A useful response begins with the actual point-of-sale estate: operating-system release, patch state, installed components, remote support and payment-data handling. Validate relevant signs on authorised systems. A broad campaign description does not establish that a specific local store was affected.

The researchers observed the exposed server closed on 31 August and reported their findings to CTIR on 8 September. This does not establish that campaign activity ended or affected terminals were remediated. The November publication does not make the observed August activity a new November infection wave. [S232]

8.4 Investigations show several fraud paths

Official account	Supported allegation or finding	Boundary for this report	Response owner
Fake-lawyer operation in February	Police describe impersonation and induced remote access [S103]	Warrants and suspicions are not convictions	Customer protection and endpoint support
Pix Seguro in May	Authorities describe false messages, pages and alleged fraud [S107]	Blocked assets are not an established loss total	Fraud operations and verified communications

Official account	Supported allegation or finding	Boundary for this report	Response owner
Bank-manager impersonation in May	State police describe a false-manager scheme [S108]	Arrests do not establish guilt	Customer service and fraud response
Insider-related investigation in May	Police describe alleged misuse of access and asset blocks [S110]	Frozen assets do not equal stolen funds	Access owner, HR and investigators
Bank-file inquiry in July	PF describes alleged capture of internal information [S115]	No general bank-platform or customer total established	Data owner and privileged-access response
Social-account fraud inquiry in July	PF describes alleged credential misuse [S116]	No attribution to every staff account	Account owner and customer protection
Infostealer inquiry in August	PF describes suspected hosting and distribution of theft software [S154]	One investigation is not national prevalence	Endpoint and identity teams
November telephone facility	State police report equipment under investigation [S133]	Devices and SIMs are not a victim count	Messaging abuse and customer protection

Several cases involve impersonation or legitimate access rather than a remotely visible application flaw. The common response question is who is authorised to act and how that authority is independently checked. The table does not establish a single criminal network.

8.5 Recent account-fraud enforcement

PF's 9 November bank-fraud proceeds inquiry concerns an account allegedly receiving electronic-fraud funds. Its 11 November operation concerns suspected bank fraud, beneficiary accounts and laundering. Neither notice supplies a national victim or loss count. [S155][S156]

The 17 November social-benefit investigation also describes alleged account access and transfers. Those allegations should prompt a scoped account review where relevant. They cannot be added to the ransomware listing count or a count of intrusions into organisations. [S130]

PF's Radar announcement combines international actions carried out during May–September. The Brazil-specific result reported is eight fraudulent domains disabled. Its international case and arrest totals are not Brazilian totals. [S129]

A takedown or account block is an intervention outcome. It does not show that every victim was identified, every payment recovered or the underlying fraud ecosystem ended. A customer-protection plan needs a continuing route for reports and corrections.

8.6 Control the next plausible request

For consumer-facing services, write a short verification message before an incident. Tell customers where to verify contact and which actions the organisation will never request through an unsolicited conversation. Check that every support channel gives the same instruction.

For internal payments, separate the message from the payment authority. A genuine mailbox or supplier account can still deliver an unauthorised beneficiary change. Confirm the change through a trusted route established before the request.

For identity recovery, consider the data an impostor may already know. Do not let a CPF identifier, date of birth or correct contract detail replace the intended authentication process. Provide a recovery route that does not depend on the same exposed information.

For incident reporting, include the uncertainty. State whether the record concerns a published offer, a validated data exposure, a suspicious login or an unauthorised transfer. That distinction helps legal, fraud and service teams choose the right response.

8.7 Purpose-bound access and instructions inside documents

A 17 February STF press note describes a tax-record access investigation. It attributes the initial finding to a Receita Federal report that identified accesses without an established functional justification, followed by confidential-information disclosure. The police investigation was continuing. [S306]

This is an attributed investigative account, without a verdict on individuals, a court decision or political motive. It does not establish an intrusion into court infrastructure. The control question is whether sensitive-record access has a valid purpose and an independently reviewable trail.

A separate court's 20 May statement identifies hidden instructions in submitted documents intended to influence AI processing. The court says its safeguards neutralised the attempts and announced investigative measures. The statement does not establish successful influence over a decision. [S307]

Document content should remain evidence to analyse. Application owners should define trusted instructions, restrict tool authority and test whether embedded requests can alter the permitted task. Legal staff should validate the resulting work. These are analyst recommendations, without a view on any proceeding.

Public-safety platform reporting also describes an investigation into alleged disclosure by a legitimate user. The police and municipal accounts remain attributed. A separate provider-camera exposure report is not silently joined to it. No judgement about surveillance policy or individual guilt follows. [S323]

The indexed official account of a 7 May operation describes an investigation into suspected extraction, retention and sale of public-system data. Independent reporting supports the operation. The full document could not be reviewed. No final affected population, intrusion date or conviction is established here. [S186]

KEY TAKEAWAYS

01

Familiar personal details do not authenticate a payment request.

02

Payment-card observations and researcher totals have narrow, different populations.

03

Validate account activity and financial harm through the responsible service owner.

CHAPTER 09

Banking and payments: protect the authority to act

THIS CHAPTER ANSWERS

Which access can change a payment?

4

separate layers: customer, institution, provider and payment infrastructure

9.1 Keep the payment layers separate 84
9.2 What the selected offers actually say 85
9.3 Why transaction identities need their own inventory 85
9.4 Reconcile initial statements with later findings 86
9.5 Registration data and the Pix-key distinction 86
9.6 The municipal payment-guide lesson 86
9.7 Supplier questions for the payment owner 87
9.8 Endpoint, fraud and infrastructure teams need one record 87
9.9 The supervisor's separate incident population 88
9.10 An anonymous banking exposure view 88

CHAPTER 09

Banking and payments: protect the authority to act

IN SHORT

Brazil's payment evidence spans a bank's temporary Pix suspension, altered municipal payment guides, registration-data disclosures, endpoint malware and advertised provider access. These events do not establish one shared weakness or a national payment-system intrusion. The key question is what authority an identity carries. Map the customer, institution, provider and payment infrastructure separately, then test certificate revocation, beneficiary validation and continuity with the people who can actually stop an unsafe transaction.

9.1 Keep the payment layers separate

A customer can lose control of a session while a bank's infrastructure remains intact. An institution can suffer a financial incident without a confirmed loss from customer balances. A provider can expose access relevant to several clients without evidence that each client was affected.

The fourth layer is the payment infrastructure itself. A leak of Pix-related identifiers, an advertisement using the word Pix or an interruption at one participant does not establish a national infrastructure intrusion. Each assertion needs evidence for its actual system boundary.

Layer	Relevant evidence in this edition	What must be established internally
Customer device and session	Banking malware and browser-extension research [S19][S20]	Device state, valid sessions and subsequent account activity
Institution	Banco do Nordeste's dated incident and later financial reporting [S101][S231]	Institutional funds, customer balances, data and availability separately
Supplier or delegated operator	Advertised certificates and infrastructure access; Google's research [S1] [S18]	Permission scope, client boundary and revocation authority
Payment infrastructure	Evidence specific to the infrastructure is required	Actual system boundary, access and operational impact

Payment instructions and registration information are evidence categories that can cross these four layers. Keep their validation questions separate from the layer affected.

Evidence category	Relevant evidence in this edition	What must be established internally
Payment instructions	Belo Horizonte's altered guides [S233]	Intended beneficiary, authorised change and settlement reconciliation
Registration information	Treasury's separate data populations [S127]	Actual data categories and exposure period; no assumed payment authority

The layers can interact, but interaction is an analytical possibility until verified. A tabletop exercise should deliberately place the problem at a supplier and ask whether the institution can contain it promptly. It should also test what evidence the supplier must provide.

9.2 What the selected offers actually say

Case I advertises certificates associated with a payment-services intermediary and separately mentions internal-network access. Case J advertises access associated with a fintech infrastructure and banking-service provider. These are observations of offers, with no verified transfer capability. [S1]

A separate April offer claims access to communications and uploaded documents involving payment certificates. It also claims persistence and an earlier sale. The report does not authenticate those assertions, connect the offers to each other or infer a completed financial transaction.

A certificate reference is not proof of payment authority. Its role could differ by environment, permission and validity. A defender needs to establish what the material authenticates, whether it remains valid, who can revoke it and which activity it can authorise.

Do not validate the claim by contacting the seller or using the advertised access. The operational route is the responsible institution and provider's authorised evidence. It should establish whether any relevant identity, permission or secret requires containment.

9.3 Why transaction identities need their own inventory

Google's BREEZE COMET research describes valid mutual-TLS material and payment-related secrets in investigated financial activity. It provides a concrete reason to examine transaction identities separately from ordinary user passwords. [S18]

An inventory should identify the business function, system owner, authorised holder and emergency revocation route. It should also distinguish a production identity from a test identity. Without that distinction, an urgent replacement may either miss the real authority or disrupt an unaffected service.

Review approval for issuing, exporting and replacing certificates. Confirm that an emergency process does not silently remove separation of duties. Record how the counterparty learns that the old identity is no longer valid.

A secret can be absent from a workstation while remaining in a deployment system, support record or older repository. Ask each owner to demonstrate the relevant access review and replacement result. A policy statement alone is insufficient evidence that access ended.

This is a recommended control model, not a finding that every listed location contained Brazilian payment secrets. The supporting research justifies the control question; the organisation's own evidence determines the exposure.

9.4 Reconcile initial statements with later findings

Banco do Nordeste's initial statement concerns a temporary Pix suspension and says no customer-account harm or data leakage had been identified at that stage. Its later management reporting describes institutional cyber-fraud loss and recovery. Both statements can describe different outcomes and dates. [S101][S231]

An incident record should retain the original statement, its time and the later update. Do not replace an early assurance with a broader one. Equally, do not rewrite an early statement as if the institution already knew every later finding.

The same principle applies to CVP's preliminary exclusion of financial and authentication-data impact. That finding is dated and scoped to the company's investigation. It does not authenticate underground advertisements or establish an assurance about related brands. [S126]

For executive reporting, allocate separate rows to data, customer funds, institutional funds, service availability and recovery status. Each row needs a source and a time. An overall green status can otherwise hide an unresolved outcome in another row.

9.5 Registration data and the Pix-key distinction

The Treasury notice distinguishes roughly 30,000 service registrations from a separate analytical base containing about 4,000 Pix keys. These populations cannot be added as unique people. The presence of a key alone does not establish authority to initiate a payment. [S127]

The Banco Central registry also distinguishes personal-data exposure from access to money or authentication material in individual notices. Several entries reviewed here have clear incident intervals but unresolved original disclosure dates. They are not converted into a complete 2026 incident series. [S134][S135][S136][S137][S138][S139]

The safe customer message identifies the actual fields involved and the relevant protection route. Avoid telling every key holder that their balance was accessed when the notice does not support that. Avoid the opposite error of treating identifiers as harmless because they cannot alone initiate a transfer.

A targeted fraudster may combine a genuine identifier with a false request. The response is independent verification and account evidence, not a claim that the underlying identifier functions as a payment password.

9.6 The municipal payment-guide lesson

Belo Horizonte's notice says altered guides sent funds to a destination other than the municipality. The authority subsequently blocked affected funds and began refunds. The confirmed issue is integrity of the payment instruction presented to taxpayers. [S233]

An organisation accepting digital payments should test the complete path from authorised bill creation to displayed beneficiary. Check whether a change is visible to the payer and whether staff can reconcile the expected recipient with the actual settlement.

Manual reissue can introduce further confusion. Provide one authoritative instruction for replacement payments and refund status. Preserve which guides were affected rather than treating every outstanding municipal payment as suspect.

The case does not identify a payment-core intrusion, a specific criminal group or the initial access route. Its value is the concrete control question it establishes: who can alter the payable instruction and how is that alteration detected?

9.7 Supplier questions for the payment owner

Question	Reviewable evidence	Decision if evidence is absent
Which client and environment does this identity serve?	Named owner and environment record	Restrict use pending scoped validation
Who can issue, export or replace it?	Current permission review and approval record	Remove unneeded authority and confirm the change
Can we revoke it promptly?	A tested revocation and counterparty acknowledgement	Exercise the process before accepting the assurance
Which transactions used it?	Relevant authorised service records	Escalate the evidence gap to the payment owner
What happens during supplier isolation?	Demonstrated minimum-service procedure	Set an explicit continuity decision and owner
How are beneficiary changes checked?	Independent verification and reconciliation record	Require a trusted verification route
What notification can the supplier provide?	Contracted contact, event scope and update commitment	Correct the notification dependency

The table is a defensive review model. It makes no finding about a particular supplier's controls. Its purpose is to turn a vague access warning into a decision that the accountable payment owner can review.

9.8 Endpoint, fraud and infrastructure teams need one record

A banking-trojan alert may reach the endpoint team before fraud operations sees an unusual transfer. An exposed provider identity may reach the institution before an individual customer reports a problem. The teams need a common incident identifier and a clear escalation path.

Record what was observed, what was validated, which authority was revoked and what activity remains under review. Link customer support to the scoped facts. Do not distribute raw sensitive data merely to prove that a case exists.

Close the loop after containment. Confirm the replacement identity works, the previous identity no longer works and delayed payments are reconciled. Review whether an emergency exception remains active after the service returns.

The report's observations support that coordination priority. They do not measure the rate of Brazilian banking fraud, rank individual banks or establish the responsibility of any payment authority for an anonymous claim.

9.9 The supervisor's separate incident population

The BCB's October stability report records 99 incidents reported by supervised institutions through September 2026, against 76 in all of 2025 and 59 in all of 2024. It cautions that improved detection and reporting contribute to visibility. These are supervisory reports, a separate population from this report's cases, posts and listing observations. [S324]

9.10 An anonymous banking exposure view

The selected banking and finance group contains 28 domains. The issuer subset contains 13 card-issuing domains. These are selected populations, not a complete register of Brazilian banks. [S3][S4]

Observation	Whole group	Issuer subset
Selected domains	28	13
Domains with current credential listings	17	12
Employee-device associations	3,760	3,113
Credential-record associations	904,473	822,157

The issuer subset contains at least 180,783 device associations outside the employee category. Their ownership remains unresolved. Those observations do not establish infection of bank-operated infrastructure or authorised payment access. [S3]

The issuer-level distinct-card observations sum to 920 within the limited payment-card observation set. This sum is not a cross-issuer count of unique cards, customers, active accounts or losses. It must not be added to device or credential associations. [S4]

SCOPE OF THE CARD FIGURES

These figures describe a limited Brandefense payment-card observation set. They do not establish current validity, unique cardholders, national card theft or fraud losses.

Assign employee-related evidence to endpoint and identity teams. Assign customer-related evidence to fraud and customer protection after validation. Keep the same scoped incident record across teams without assuming that their populations represent the same people.

KEY TAKEAWAYS

01

A customer, bank, supplier and payment infrastructure have different boundaries.

02

Inventory and revoke transaction identities with the payment owner.

03

Reconcile beneficiary changes, incident updates and emergency exceptions before closing a case.

CHAPTER 10

Regulatory and national response

10

THIS CHAPTER ANSWERS

Which reporting decisions should a Brazilian incident team prepare before an event?

3 business days

general ANPD notification period, with scope and exceptions

10.1 Applicability before deadlines 91
10.2 The ANPD sequence 92
10.3 Supplier awareness is an operational dependency 92
10.4 Affected-person communication needs its own owner 93
10.5 Sanctions are not an incident-loss estimate 93
10.6 Rehearse one chronology across several routes 94

CHAPTER 10

Regulatory and national response

IN SHORT

Personal-data incidents, financial-service disruption and telecom incidents have different reporting routes. Under the cited ANPD regulation, the general notification period is three business days after the controller knows that personal data were affected. Scope, relevant harm and applicable exceptions still require assessment. Record that awareness point, identify the responsible legal entity and rehearse regulator and affected-person communications with the relevant supplier.

This chapter supports planning and does not determine an organisation's legal obligations. Read the applicable current instrument and obtain advice for the actual entity, activity and facts.

10.1 Applicability before deadlines

Framework	Relevant scope	Supported requirement	Owner
LGPD Articles 46–48	Processing subject to the law	Security measures and communication where an incident may cause relevant risk or harm to people [S10]	Controller and data-protection lead
ANPD Resolution 15/2024	Relevant personal-data incident	Authority and affected-person communication, awareness record and incident register [S11][S12]	Controller, legal and incident lead
CMN Resolution 4.893/2021	Institutions within its current scope	Cybersecurity policy and requirements for data-processing, storage and cloud-service arrangements [S14]	Financial compliance and accountable management
Telecom R-Ciber	Applicable providers and duties under the consolidated text	Relevant-incident notification; additional ANATEL notification where an ANPD communication is required [S13]	Telecom security and regulatory affairs
National cybersecurity strategy	National strategic coordination	Citizen protection, essential-service resilience, cooperation and governance [S21]	Leadership and coordination functions

The CMN instrument excludes specified institution categories that follow Banco Central regulation instead. Its scope should not be assigned to every organisation labelled financial in an analytical sample. A payment provider's applicable rule must be established separately. [S14]

The telecom text likewise has general provisions, scope exceptions and particular obligations that apply across provider sizes. Article 2-C requires ANATEL notification when a communication to ANPD is required. Article 17 separately addresses relevant incidents substantially affecting network and user-data security. [S13]

10.2 The ANPD sequence

Resolution 15 took effect on publication on 26 April 2024. Its general authority-notification period runs from the controller's knowledge that an incident affected personal data. Sector legislation can prescribe another period. [S11]

Stage	General rule	Operational record
Assess scope	Determine the incident, personal data and relevant risk or harm	Known facts, categories, people and uncertainty
Authority notice	Within 3 business days, subject to specific legislation	Awareness time, deadline and submission receipt
Affected-person notice	Within 3 business days from the relevant awareness	Accessible message and communication evidence
Complement authority information	Reasoned completion within 20 business days after the communication	Outstanding questions and updated submission
Retain incident record	At least 5 years from registration, subject to the stated exceptions	Incident record and retention decision

Qualifying small agents have doubled periods under the regulation's specified provisions. Eligibility must be checked under the small-agent framework. The report does not assume that a small organisation automatically qualifies. [S11]

For public entities within LGPD Article 23, the register-retention rule has a particular exception tied to the applicable permanent-document arrangements. Other duties can also require longer retention. Do not apply the general five-year rule without checking those conditions. [S11]

The regulation's relevant-risk assessment considers significant effects on interests and rights together with specified data or population criteria. Sensitive data, authentication information, financial data and vulnerable people can be relevant. Their presence should enter the assessment rather than become an unsupported prediction of misuse. [S11]

10.3 Supplier awareness is an operational dependency

ANPD's guidance says the operator should inform the controller without unjustified delay and provide information needed for the controller's communications. The controller's legal communication duty is not transferred simply because processing occurs at a supplier. [S12]

A contract should give that requirement an operational route. Identify the monitored contact, alternate contact, technical evidence owner and authority to escalate outside office hours. Test the route using a synthetic notification with incomplete facts.

The first supplier message may not establish every affected person or data category. Preserve what it does establish and assign the missing questions. Legal should record the awareness assessment from the actual information, rather than wait for a convenient final report.

10.4 Affected-person communication needs its own owner

Resolution 15 requires plain, understandable communication, directly and individually where the affected people can be identified. Its alternative public communication provisions have specific conditions, visibility and duration requirements. A general press release should not be assumed sufficient. [S11]

Separate the authority submission from the customer message. A technical incident description can contain necessary regulatory detail while being unsuitable for a person trying to decide whether to trust a call. Both should preserve the same established facts.

Customer operations should explain the genuine process for payment, account recovery and support. Use an established channel and avoid asking people to send additional sensitive data merely to discover whether they are affected. Escalate reports that suggest immediate fraud or personal harm.

10.5 Sanctions are not an incident-loss estimate

LGPD Article 52 provides several administrative sanctions. Its simple-fine provision concerns up to 2% of the relevant private entity, group or conglomerate's Brazilian revenue, excluding taxes, capped at R$50 million per infringement. Applicability and due process matter. [S10]

The law provides a different set of applicable sanctions for public bodies. An incident does not automatically produce the maximum fine, and a reported loss is not the regulator's penalty calculation. The report makes no finding about compliance or liability in any case.

ANPD's 2026 health-related proceeding and municipal corrective action concern earlier events. They illustrate regulatory follow-up after the original incident. They do not become new 2026 hacker intrusions because the regulator published an update this year. [S114][S125]

10.6 Rehearse one chronology across several routes

Exercise prompt	Required decision	Completion evidence
Supplier reports copied registration data	Which controller and people are affected?	Scoped assessment and awareness rationale
Payment service is unavailable	Which financial or operational route applies?	Entity-specific classification and contact
Telecom incident affects user data	Are ANPD and ANATEL duties engaged?	Separate determinations and receipts
Facts remain incomplete	What can be communicated now and supplemented later?	Reasoned initial notice and missing-information owner
Communication channel is unavailable	Which trusted alternative reaches affected people?	Tested alternate route and approved message
No notification is required	Why was that conclusion reached?	Recorded facts, rationale and retention decision

The completion test is a usable incident record. It should show who decided, when they knew, which route they used and what evidence remained missing. A deadline chart without those responsibilities is not an exercised response.

KEY TAKEAWAYS

01

Determine the entity, processing and reporting scope before applying a clock.

02

Preserve awareness times and separate authority, affected-person and sector communications.

03

Record the rationale even when an incident is not notified.

CHAPTER 11

Outlook and conditional planning

11

THIS CHAPTER ANSWERS

Which judgements support planning, and what evidence would change them?

4

conditional scenarios with explicit response triggers

11.1 Key judgements 96
11.2 Signals that should change the response 96
11.3 Conditional scenarios 97
11.4 What the evidence cannot project 97

CHAPTER 11

Outlook and conditional planning

IN SHORT

Plan around identity misuse, payment authority, copied records and service continuity. Ransomware listings support recovery preparation, while the public cases require separate customer and operational responses. The evidence does not establish a national attack probability or the next successful actor. Use the scenarios below as planning assumptions. Change the response when owned-account evidence, confirmed data categories or service-impact measurements change.

11.1 Key judgements

Judgement	Confidence and basis	Limit	Decision
Identity validation belongs alongside fraud response	High for the control need; registration disclosures and browser-session research [S126][S127][S19][S20]	Does not establish a shared source or successful transaction	Assign identity and customer-protection owners
Payment authority needs protection beyond customer passwords	High for the planning need; payment-guide incident and financial campaign research [S233][S18]	No national prevalence or common operator inferred	Test signing identities, approvals and beneficiary checks
Recovery includes business and customer work	High for the documented distinction; Santos recovery updates [S128][S229][S230]	Continued capacity is the authority's statement, not a timing measurement for every user	Exercise fallback and reconciliation
Extortion preparedness should cover many claimant labels	High for listing composition [S2]	A listing is not confirmation of intrusion or encryption	Test restoration and data-loss decisions independently of actor name
Political language needs a separate evidence assessment	High for the analytical boundary	No forecast of political violence, election impact or state direction	Keep public attribution tied to the actual source

Confidence attaches to the proposition in its row. It is not a certification of every statement made by a named group, researcher or institution. The same evidence can support a control decision while leaving the underlying intrusion mechanism unresolved.

11.2 Signals that should change the response

An advertisement becomes more operationally significant when the organisation validates current, owned information that the advertiser should not possess. A dated claim alone is insufficient. Preserve the difference between recognising an old record and finding a still-active account or session.

A service incident changes when the affected business function changes. If an administrative outage begins to prevent a critical operational task, the continuity owner should reassess the fallback. That decision should use current service evidence rather than the original incident label.

A personal-data case changes when the categories, people or likely harm become clearer. Additional information can require a revised communication. Equally, an initially suspected category may be excluded by a later scoped assessment. Preserve both the update and its effective date.

For an actor assessment, require a concrete connection before merging campaigns. A shared technique, country reference or nearby publication date does not establish common control. An actual shared infrastructure or source-supported relationship would justify a narrower, documented link.

11.3 Conditional scenarios

The following are planning assumptions, not predictions or attack probabilities.

If	Potential consequence	First validation	Owner and response
A current privileged credential is validated	Access could extend beyond the originally named application	Check account, privilege, sign-ins and sessions	Identity and incident response contain the validated access
A supplier confirms copied customer registration records	Contextual impersonation may continue during recovery	Establish categories, population and genuine contact process	Data protection and customer operations coordinate warnings
Payment-guide or signing data change without approval	Legitimate-looking instructions may send money to the wrong destination	Check beneficiary, authorisation history and affected interval	Treasury and fraud suspend the unsafe workflow under the approved procedure
A public claim coincides with service degradation	Customers may confuse an outage with proven data theft	Confirm essential user tasks and separate access evidence	Operations mitigates; communications publishes bounded status updates

In the payment scenario, do not infer that every transfer during the interval is fraudulent. In the supplier scenario, do not assume every customer has the same data categories. The response should narrow or expand as the owner establishes the facts.

11.4 What the evidence cannot project

Post volume cannot forecast losses or the probability that a particular organisation will be attacked. Asking prices cannot establish criminal revenue. Ransomware listing counts cannot determine whether the next incident will involve encryption, theft, both or neither.

The selected domain portfolio also cannot rank Brazilian sectors by security. Its selection is not representative. The national Atlas headline supports prioritisation within this portfolio, without measuring intrusion probability or the control effectiveness of Brazilian sectors.

Maintain a short judgement register. Record the proposition, supporting evidence, plausible alternative, trigger for change and accountable decision. Revisit it after a material incident, supplier notice or validated current exposure, not simply because an actor publishes another boast.

KEY TAKEAWAYS

01

Use scenarios as conditional planning assumptions, not probabilities.

02

Change the response when current account, data or service evidence changes.

03

Keep judgement owners and revision triggers alongside every assessment.

CHAPTER 12

Action plan

12

THIS CHAPTER ANSWERS

Who should act over the next 90 days, and what demonstrates completion?

30 / 60 / 90

days for validation, exercised controls and management review

12.1 The 30/60/90-day plan 100
12.2 Role-specific responsibilities 102
12.3 Leadership scorecard 103
12.4 How Brandefense can help 104

CHAPTER 12

Action plan

IN SHORT

Start by assigning owners to identities, payment authority, critical suppliers and minimum services. Then test the controls that separate an external claim from a confirmed incident. Complete the programme with witnessed recovery, customer-support and reporting exercises. The plan is conditional: contain validated unsafe access promptly, while recording why historical or unrelated evidence was closed. Report completion evidence and unresolved exceptions to management.

12.1 The 30/60/90-day plan

The periods are management targets for this plan, not statutory reporting deadlines. Urgent incident duties and validated unsafe access require the relevant immediate response.

30 days		
Assign an owner and triage route for credential and access alerts	ACCOUNTABLE OWNER CISO and identity lead	COMPLETION EVIDENCE Contact route, service inventory and disposition vocabulary
Validate new relevant account evidence for ownership, age, status and prior remediation	ACCOUNTABLE OWNER Identity operations	COMPLETION EVIDENCE Dated account decision and supporting access review
Map transaction-signing identities, service accounts and payment approval responsibilities	ACCOUNTABLE OWNER Payments and treasury	COMPLETION EVIDENCE Approved authority map with revocation contacts
Establish the genuine customer payment and recovery process	ACCOUNTABLE OWNER Fraud and customer operations	COMPLETION EVIDENCE Published verification route and approved support script
Map critical suppliers to service, controller, data categories and alternate contact	ACCOUNTABLE OWNER Procurement and data protection	COMPLETION EVIDENCE Usable dependency register and tested contact

Determine notification duties for each legal entity and activity

ACCOUNTABLE OWNER

Legal and regulatory affairs

COMPLETION EVIDENCE

Scope record, recipients, awareness triggers and accountable decision-makers

Check the applicability of the cited Windows vulnerability to owned systems

ACCOUNTABLE OWNER

Endpoint and merchant-technology leads

COMPLETION EVIDENCE

Asset-to-version assessment and applicable remediation record

260 days

Deploy phishing-resistant authentication for the prioritised privileged and remote-access population

ACCOUNTABLE OWNER

Identity and infrastructure

COMPLETION EVIDENCE

Coverage record, tested recovery and documented exceptions

Revoke validated unsafe sessions and review recovery methods and delegated access

ACCOUNTABLE OWNER

Identity and incident response

COMPLETION EVIDENCE

Session invalidation test and account-change assessment

Exercise a payment-destination alteration using synthetic instructions

ACCOUNTABLE OWNER

Treasury and fraud

COMPLETION EVIDENCE

Independent beneficiary check, escalation and stop decision

Restrict unnecessary remote-support and browser-extension installation

ACCOUNTABLE OWNER

Endpoint and service owners

COMPLETION EVIDENCE

Approved allowlist and a tested exception process

Review service-account secrets and transaction-signing access across critical providers

ACCOUNTABLE OWNER

Payments and platform engineering

COMPLETION EVIDENCE

Owner-verified access list and rotation/revocation rehearsal

Test a critical service's manual or alternate operating mode

ACCOUNTABLE OWNER

Business continuity and operations

COMPLETION EVIDENCE

Witnessed minimum-service exercise and reconciliation plan

Rehearse an incomplete supplier incident notice and the controller's awareness decision

ACCOUNTABLE OWNER

Legal, data protection and supplier owner

COMPLETION EVIDENCE

Chronology, initial notice draft and missing-information responsibilities

Test public status messages against a simulated claim and outage

ACCOUNTABLE OWNER

Communications and service owner

COMPLETION EVIDENCE

Approved statement separating impact, data and attribution

390 days

Restore a critical service with recovery identities separated from production administration

ACCOUNTABLE OWNER

Infrastructure and business owner

COMPLETION EVIDENCE

Witnessed restoration, integrity checks and business sign-off

Exercise customer support after copied registration data

ACCOUNTABLE OWNER

Fraud and customer operations

COMPLETION EVIDENCE

Staff scenario results, trusted contact route and escalation evidence

Review exposure-alert dispositions and unresolved ownership questions

ACCOUNTABLE OWNER

CISO and identity lead

COMPLETION EVIDENCE

Closed-case sample, unresolved queue and exception owners

Report tested outcomes and remaining dependencies to management

ACCOUNTABLE OWNER

CISO and executive sponsor

COMPLETION EVIDENCE

Decision record with resources, owners and next review dates

The plan links to the evidence rather than an actor's reputation. Identity research supports account and session checks. The municipal payment case supports beneficiary verification. Santos supports minimum-service and reconciliation exercises. Listing observations support recovery preparation. [S18][S19][S20][S233][S229][S2]

12.2 Role-specific responsibilities

Leadership and the CISO. Approve the services whose interruption would create an unacceptable business consequence. Fund the response capabilities attached to them. Require a named owner and an exercised fallback rather than accepting an untested policy as completion.

Identity and incident response. Establish whether external account evidence maps to a current owned identity. Review privilege, sessions and recovery methods where relevant. Record a disposition even when evidence is historical, unrelated or already remediated.

Payments and treasury. Protect transactional authority and independent approval. Know which provider can submit an instruction, who can change its credential and how that authority is revoked. Test beneficiary checks without using live customer funds.

SOC and endpoint teams. Investigate suspicious remote-support installation, browser-extension policy changes and relevant endpoint activity. Use organisational context to distinguish approved administration from misuse. A tool name alone should not decide the outcome.

Data protection and legal. Preserve awareness times, determine the actual controller and assess relevant risk or harm. Keep authority, affected-person, sector and police routes separate. Ensure supplier notices provide enough information for those decisions.

Customer operations and communications. Provide a trusted way to verify contacts and payment requests. Explain confirmed categories and current service state in plain language. Preserve uncertainty instead of borrowing an actor's quantity or a preliminary assurance without its date.

Procurement and supplier owners. Keep incident contacts usable outside normal conditions. Rehearse the exchange of scope, logs and customer-impact information. Record what the supplier could not establish and who follows up.

12.3 Leadership scorecard

Decision area	Evidence to present	Avoid substituting
Identity	Relevant alerts with validated dispositions and unresolved owners	Total leaked-record volume
Payment authority	Approved identities and passed destination-change exercise	Number of security products installed
Supplier response	Tested contacts and a scoped notification exercise	Contract count alone
Recovery	Witnessed minimum service and restoration sign-off	Successful backup-job count
Customer protection	Staff exercise and trusted verification process	Number of warning messages sent
Reporting	Awareness chronology, applicability decisions and receipts	One universal notification deadline

Use denominators that match each decision. Authentication coverage concerns the prioritised account population. Restoration concerns a defined service. Customer support concerns a stated scenario. Do not combine these into an invented national or corporate incident probability.

Review the unresolved queue as well as completed work. An exception should state its owner, reason, compensating action and next decision date. The scorecard should make a resource decision possible, rather than reward a larger volume of alerts.

12.4 How Brandefense can help

Brandefense provides Cyber Threat Intelligence, Digital Risk Protection and External Attack Surface Management. These capabilities can support relevant exposure monitoring, investigation and response workflows. They do not replace an organisation's account validation, incident decisions or legal duties. [S22]

Bring a concrete workflow to the discussion: an owned-domain alert, a supplier dependency, a brand-impersonation queue or a customer-protection scenario. Agree the evidence, response owner and closure test before judging the service by alert volume.

Request a Brandefense demo.

KEY TAKEAWAYS

01

Validate identities and transactional authority with accountable owners.

02

Test supplier communication, minimum service and recovery using synthetic scenarios.

03

Report witnessed outcomes and unresolved exceptions by day 90.

APPENDICES

Appendices

A–D

THIS CHAPTER ANSWERS

Which dates, populations and limits travel with the findings?

Separate

posts, listings, cases, domains, records and financial outcomes

Appendix A. Scope and evidence boundaries 106

Appendix B. Evidence register 111

Appendix C. Sources 116

Appendix D. Glossary 121

Appendix A. Scope and evidence boundaries

Comparison countries were selected as examples to provide context only; they do not imply a ranking or political assessment.

A.1 Observation window and cut-off

The requested window is 1 January–22 November 2026. Underground observations use post publication time. Ransompedia observations use the dated listing record. Public accounts retain incident, discovery, disclosure, operation and update dates separately where available. [S1][S2]

The observation cut-off was 22 November 2026; source verification continued on 23 November. The cut-off day was still in progress when observations ended. The report does not claim a completed end-of-day census. The recent-activity section covers 8–22 November and includes labelled recovery updates, research publications and enforcement concerning earlier conduct.

A source page's modification date can differ from its original publication date. Official archive migrations can also update many pages together. Such dates are not used to invent an incident month. An unresolved disclosure date remains unresolved.

A.2 Source populations

Population	What it describes	Essential limit
Underground posts	Brazil-associated publication observations and selected authentic excerpts [S1]	A country association is not necessarily targeting
Ransomware listings	Public extortion assertions associated with the country [S2]	No independent confirmation of encryption, theft or payment
Selected portfolio	250 assessed primary domains in ten groups [S3]	Ownership and organisational independence unvalidated; no national prevalence inference
Payment-card observations	Limited Brazil-associated payment-card observation set [S4]	No national card exposure or financial-loss estimate
Official disclosures	Findings stated by an organisation or authority	Confirmation applies to the stated proposition and date
Police notices	Investigations, suspicions and intervention outcomes	No conviction inferred from a search or arrest
Technical research	Attributed findings about a campaign or vulnerability	Geography, observation dates and confidence remain source-specific

These populations are not added into a total of Brazilian attacks. A single event can generate several posts, a listing, an official notice, a regulatory proceeding and a later police operation. Conversely, many events may never be publicly disclosed.

A.3 What a country comparison can support

The regional comparison uses Argentina, Chile, Colombia and Mexico as regional comparators. All four have significant regional services, industrial or infrastructure relationships. The table supplies absolute listing observations under one source and cut-off. [S2]

It does not control for population, economic activity, number of organisations, disclosure practices or attacker visibility. It therefore supports no national security ranking. Full-year 2025 and partial-year 2026 values must retain their different periods.

The Brazil group and monthly totals reconcile to 206 listings. Group names are the recorded labels and do not establish stable legal identities, common membership or operator continuity. Industry labels, when used, describe the source population rather than national sector prevalence.

A.4 Portfolio and passive-control limits

The 250-domain portfolio is purposive and covers important public and private services. It is not an official list ranked by revenue. Related domains or entities may share an operator, and a candidate primary domain is not proof of legal independence. [S3]

The exposure snapshot was read on 22 November 2026. Atlas supplies the national headline of 80/100 (F) for the selected portfolio. Only this national rating is published. Anonymous sector counts describe distinct signal populations, without organisation ratings or sector security rankings. [S3]

Read the sector CSV field `orgs_listed_for_sale_now` as "Domains with current credential offers". Its unit is a selected domain with an associated credential currently advertised for sale. It counts neither organisations offered for sale nor individual advertisements.

No complete passive-hygiene dataset or hygiene index is available. Missing configuration observations remain unavailable and do not establish a failed mail control or absent protection.

If an account association is later validated, record its category and time. Employee, contractor, customer and unresolved relationships have different implications. Historical credentials, current offers, device associations and document observations are not interchangeable measures.

A.5 Payment-card scope

SCOPE OF THE CARD FIGURES

These figures describe a limited Brandefense payment-card observation set. They do not establish current validity, unique cardholders, national card theft or fraud losses.

A card observation does not establish a unique person, active account, successful authorisation or original theft route. An advertised status remains an assertion unless validated through the responsible issuer. No issuer-level identifier or personal card data is published. [S4]

The researcher's global point-of-sale figures are a different population. They are neither added to the Brandefense payment-card aggregates nor presented as a Brazil-only total. [S232]

A.6 Incident coverage and unresolved discoveries

The register records confirmed disclosures, attributed campaigns, police investigations, advertisement claims, contextual items and exclusions. Those categories do not form one denominator of confirmed incidents. The case identifiers organise the report; they are not a national incident numbering system.

The official-source review spans CTIR Gov/GSI, CERT.br, ANPD, PF, Banco Central, ANATEL and selected state-police sources. Portuguese, English, Spanish and Russian reporting supplies additional discovery and corroboration. Coverage differs across archives and languages.

Several official archives, original notices and late discoveries could not be fully established. State-police coverage does not enumerate every state-month archive. An absent entry therefore means no supported item was established in that part of the evidence, not zero incidents in the country.

Some reports reproduce a company statement without a directly reviewed first-party notice. Such subjects remain role-based or excluded from named cases. Aggregator duplication and uncertain incident dates are not imported as confirmed totals.

A.7 Evidence and confidence language

Label	Meaning in this report
Observation	A retained record supports the stated publication or quantity
Claim	A source asserts possession, access or impact not independently established here
Official confirmation	The organisation or competent authority confirms the particular stated fact
Attributed research	A named researcher supplies a finding with its own scope and confidence
Analyst inference	A reasoned interpretation, with the supporting evidence and an alternative
Analytical model	A planning relationship or scenario without a proven shared operator

High confidence concerns a specified proposition. It does not authenticate every statement made by an actor or institution. Unverified does not mean false. An incident can be confirmed while its entry route, actor and affected-person total remain unresolved.

A current account validated by its owner warrants a different response from an old record recognised in an advertisement. A source's certainty is not the report's certainty. The difference is stated beside the case rather than left to this appendix alone.

A.8 Naming, privacy and neutrality

An incident subject is named only where official confirmation and wider reporting support the particular case. The public naming register records that basis. Authorities cited for guidance and publishers cited for research are not automatically approved as incident subjects.

Other subjects use broad roles that could describe several bodies. Source titles and article addresses that would defeat those roles are shortened in the public bibliography. Supporting passages remain available in the private evidence record.

Post excerpts retain authentic source wording with bracketed omissions and redactions. They contain no personal records, live credentials, criminal contact routes or victim access details. Portuguese translations are labelled and retain the original excerpt.

The report takes no political position on governments, parties, courts, elections, sanctions, tariffs or foreign relations. State or motive labels remain the source's attributed assessment when necessary. Actor slurs, accusations and recruitment language are omitted.

A.9 Legal and vulnerability verification

The legal chapter separates applicable entity, trigger, awareness point and communication route. It does not determine liability or certify compliance. Readers must check the current instrument for the actual entity and incident. [S10][S11][S12][S13][S14]

The vulnerability reference was checked against NVD, including affected-version boundaries and linked vendor remediation. CVE-2024-49138 is a Windows privilege-escalation record. Its presence in the cited research does not establish exploitation at any named Brazilian organisation. [S5][S232]

For example, the retained NVD record identifies Windows 10 22H2 before 10.0.19045.5247, Windows 11 23H2 before 10.0.22631.4602 and Windows Server 2022 before 10.0.20348.2966. These are selected product boundaries, not a complete applicability list. [S5]

The responsible owner should match the actual Windows release and current vendor guidance. A generic product name is insufficient to decide that a device is affected or remediated. Patch confirmation should be part of the endpoint record.

A.10 Edition integrity

The Brazilian Portuguese edition is translated from the English master and visibly marked "Traduzido com IA". It preserves the figures, case identifiers, source identifiers and report directives. The English edition prevails where the language editions differ.

Consistency checks validate the package's internal references and stated boundaries. They do not establish exhaustive national coverage, validate an anonymous actor's claims or constitute publication approval. Review and release status remain outside the analytical findings.

Appendix B. Evidence register

B.1 Twenty-six cases and their limits

The following register summarises ten claim cases and sixteen disclosure or investigation cases. It does not describe twenty-six confirmed intrusions. Several cases include multiple dates or unresolved outcomes.

Case	Date or phase	Sector	Evidence and boundary
A	3 January post	Public administration	Incomplete document-archive claim; content and current access unverified
B	4 January post	Retail	Contact/order/delivery claim; origin and customer population unverified
C	14 January and related posts	Municipal services	Fiscal-data claims; rows and databases do not count independent incidents
D	2 February post	Education	Guardian/student-finance offer; advertised records are not unique people
E	6 February and later circulation	Financial services	Virtual-assistant claim; data end date follows stored post date
F	11 November post	Banking	Bank-associated leads; freshness, acquisition and sale unverified
G	17 November post	Payments	Explicitly 2025-labelled offer; no new 2026 intrusion established
H	19 November post	Business software	Customer-table claim; provider and downstream access unverified
I	24 March post	Payment services	Certificate/internal-network offer; no verified transfer authority
J	6 July post	Financial infrastructure	Access offer; environment, permissions and client effect unverified
K	6 November discovery; 12 November notice	Insurance	CVP confirms registration-data copying; preliminary exclusions remain dated
L	4 November discovery; 13 November notice	Public administration	Treasury identifies two data populations; no combined unique-person total

Case	Date or phase	Sector	Evidence and boundary
M	14–16 November; later updates	Municipal payments	Altered guides; funds blocked and refunds started, completion not established
N	January; later first-half reporting	Banking	Temporary Pix suspension; customer and institutional outcomes kept separate
O	6–19 November	Port administration	Administrative incident and recovery; capacity assurance attributed to APS
P	June event; September notice	Public administration	Historical registration base; no live-register intrusion established
Q	June notices	Public warning services	False alerts and alternate channels; no actor or political motive established
R	July event; October police notice	Institutional services	Data-theft/extortion investigation; no family, encryption or conviction established
S	February police notice	Healthcare data	Alleged unauthorised processing and commercial use; investigation not conviction
T	14 November notice	Healthcare	Unimed Natal confirms incident response and continued care; no data-theft or completed-recovery finding
U	October event; 19 November notice	Health benefits	Indexed provider notice; corporate-provider fields only, full text not reviewed
V	1–9 November	Public health administration	State incident and shared licensing effects; no separate municipal intrusion
W	22–24 March	Banking	Issuer-authored mirror and wide reporting; customer and institutional outcomes distinct
X	21 September discovery; October reporting	Healthcare projects	Official investigation into possible access; no public misuse established
Y	2 November event; 12 November statement	Digital-asset services	Investor-authored mirror; financial effect not reliably estimable
Z	4 October event	Financial project services	Official portal notice; publication date and completed restoration unresolved

The first ten cases are observations of claims. The following cases retain the exact source status: an organisational disclosure, authority account or police investigation. Confirmation of an investigation is not a finding that every allegation is established.

B.2 Original post cards

Card	Case	Post date	Held proposition
B01	A	2026-01-03	A poster describes a document archive associated with a public body
B02	B	2026-01-04	A seller lists contact, order and delivery categories
B03	C	2026-01-14	A narrative advertises municipal fiscal databases
B04	D	2026-02-02	A seller claims guardian and education-finance records
B05	E	2026-02-06	A partial-dump narrative includes inconsistent date claims
B06	F	2026-11-11	A seller offers bank-associated leads in whole or segments
B07	G	2026-11-17	A Pix-labelled advertisement explicitly calls the material 2025 data
B08	H	2026-11-19	A business-software claim identifies a customer-table file
B09	I	2026-03-24	A seller offers certificates and separately internal-network access
B10	J	2026-07-06	A post advertises financial-infrastructure access

All ten excerpts use authentic English source fragments. Brackets identify omissions or redactions. The Portuguese edition provides a labelled translation beside the original. The excerpt is not an authenticated sample of the advertised data. [S1]

B.3 Campaigns and public notices

Evidence family	Supporting source	Proposition and limit
Ransomware composition	Ransompedia [S2]	206 listings, not verified intrusion outcomes
Payment-related campaign	Google [S18]	Vendor-investigated identity and supplier activity; no linkage to selected sellers
Banking malware	Elastic [S19]	Campaign behaviours; monitored bank domains are not bank victims
Browser theft	IBM [S20]	Customer browser/session activity; no bank-infrastructure inference
Espionage and information theft	Kaspersky [S161]	Brazil included; Armored Likho attribution is medium confidence, no state sponsor
Payment redirection	Kaspersky [S105]	GoPix mechanism context; no national fraud rate
Regional banking threat	Kaspersky [S106]	JanelaRAT context; Brazil detection quantity belongs to 2025
Public-sector warnings	CTIR [S147][S148][S149][S150][S151] [S152][S153]	Mechanisms and possible campaigns; warning numbers are not incidents
Point-of-sale research	Cybernews and NVD [S232][S5]	Global researcher quantities and vulnerability boundaries; no Brazil-only victim total

B.4 What would justify joining records

A shared subject name is insufficient to join an advertisement, official disclosure and ransomware listing. Dates can overlap by chance, and an actor can borrow public details. A join needs supporting evidence for the same event and an explicit statement of what is linked.

Likewise, a republished post can repeat a genuine claim without proving a new intrusion. Keep its circulation date and source relationship, then assign it to the existing narrative where supported. Do not add it as another affected organisation.

A supplier event may affect more than one client, but that relationship needs client-specific evidence. A provider's general service catalogue cannot supply the missing affected-client list. This is especially important for payment, education and business-software claims.

The hospital statement in the additional-disclosure table and the police extortion dossier retain different reported dates. They are not joined as the same incident. [S181][S122] For the financial-sector statement, the HTML date controls over an internally inconsistent PDF date. [S177]

B.5 Decision and correction record

Each important finding has an evidence-record entry identifying its source, evidence type, confidence, alternative and accountable action. The incident-coverage register records inclusion, mention, contextual use or exclusion; it is held in the private evidence record.

A future correction should identify the proposition that changed, the new source and the effective date. It should update both editions, relevant cards and aggregate explanations together. A new actor attribution should not silently revise older outcome statements.

Appendix C. Sources

Each entry gives its supporting-source review date. A shortened article address protects a role-based subject and is marked accordingly. An indexed supporting passage is explicitly distinguished from a full document reviewed.

S1: Odin by Brandefense. Retained Brazil-associated post observations, 1 January–22 November 2026. Verified on 2026-11-22.

S2: Ransompedia. Brazil and four regional peers, dated listing observations. Verified on 2026-11-22.

S3: Odin by Brandefense. Atlas exposure snapshot and selected 250-domain portfolio, read 22 November 2026. Verified on 2026-11-22.

S4: Odin by Brandefense. Limited Brazil-associated payment-card observation set. Verified on 2026-11-22.

S5: NIST National Vulnerability Database. CVE-2024-49138 record and affected-version boundaries. Verified on 2026-11-22.

S10: Presidência da República. Lei 13.709/2018, consolidated LGPD, Articles 46–52. Verified on 2026-11-22.

S11: ANPD. Resolution 15 of 24 April 2024, regulatory-process copy; published 26 April 2024. Verified on 2026-11-23.

S12: ANPD. Comunicação de Incidente de Segurança: procedure and questions. Verified on 2026-11-22.

S13: ANATEL. Resolution 740/2020, consolidated telecom cybersecurity regulation. Verified on 2026-11-22.

S14: Banco Central do Brasil. CMN Resolution 4.893 of 26 February 2021, current consolidated text. Verified on 2026-11-22. Indexed primary passage reviewed; full text not reviewed.

S16: DataReportal. Digital 2027: Brazil, October 2026 contextual figures. Verified on 2026-11-22.

S17: Tribunal Superior Eleitoral. Eleições 2026: confira as principais datas do calendário eleitoral. Verified on 2026-11-22.

S18: Google Threat Intelligence Group / Mandiant. Financially Motivated Threat Actor BREEZE COMET Targets Brazil, 1 September 2026. Verified on 2026-11-22.

S19: Elastic Security Labs. TCLBANKER: Brazilian Banking Trojan Spreading via WhatsApp and Outlook, 7 May 2026. Verified on 2026-11-22.

S20: IBM Trusteer. UnregStealer: Human-operated browser credential theft targeting Brazilian banking, 16 June 2026. Verified on 2026-11-22.

S21: Câmara dos Deputados. Decree 12.573 of 4 August 2025, original national cybersecurity strategy. Verified on 2026-11-22.

S22: Brandefense. Request a Demo. Verified on 2026-11-22.

S23: Kaspersky GReAT. BeatBanker: um trojan de dupla função para Android, 10 March 2026. Verified on 2026-11-22.

S24: Kaspersky GReAT. A VBScript campaign distributed through WhatsApp deploying RMM software, 22 June 2026. Verified on 2026-11-22.

S25: Check Point Research. Gaming the system: Brazilian government sites and SEO fraud, 2 September 2026. Verified on 2026-11-22.

S26: MITRE ATT&CK. Spearphishing Attachment. Verified on 2026-11-22.

S27: MITRE ATT&CK. PowerShell. Verified on 2026-11-22.

S28: MITRE ATT&CK. System Information Discovery. Verified on 2026-11-22.

S29: MITRE ATT&CK. Screen Capture. Verified on 2026-11-22.

S30: Receita Federal. Inscrever Entidade no Cadastro Nacional de Pessoas Jurídicas. Verified on 2026-11-22.

S101: Banco do Nordeste. Banco do Nordeste market notice, 26 January 2026. Verified on 2026-11-22. Indexed primary passage reviewed; full text not reviewed.

S102: Polícia Federal. A health-data service provider; 2026-02-04. Verified on 2026-11-22.

S103: Official source. An interstate electronic-fraud investigation; 2026-02-24. Verified on 2026-11-22. Indexed primary passage reviewed; full text not reviewed.

S104: Polícia Federal. A payment-service-provider fraud investigation; 2026-03-16. Verified on 2026-11-22. Indexed primary passage reviewed; full text not reviewed.

S105: Kaspersky GReAT. Gopix banking malware; 2026-03-16. Verified on 2026-11-22.

S106: Kaspersky GReAT. Janelarat banking malware; 2026-04-13. Verified on 2026-11-22.

S107: Official source. An sms impersonation fraud campaign; 2026-05-14. Verified on 2026-11-22. Indexed primary passage reviewed; full text not reviewed.

S108: Official source. A false bank-manager fraud campaign; 2026-05-18. Verified on 2026-11-22. Indexed primary passage reviewed; full text not reviewed.

S110: Official source. A bank-insider fraud investigation; 2026-05-22. Verified on 2026-11-22. Indexed primary passage reviewed; full text not reviewed.

S112: El País. A bank communication error; 2026-06-12 (article URL withheld). Verified on 2026-11-22.

S113: Official source (address withheld; held in the private evidence record). A public warning platform; 2026-06-20. Verified on 2026-11-23.

S114: ANPD. A multi-state healthcare operator; 2026-07-08 (article URL withheld). Verified on 2026-11-22.

S115: Polícia Federal. A bank-insider investigation; 2026-07-16. Verified on 2026-11-22. Indexed primary passage reviewed; full text not reviewed.

S116: Polícia Federal. A social-account insider investigation; 2026-07-31 (article URL withheld). Verified on 2026-11-22. Indexed primary passage reviewed; full text not reviewed.

S117: Polícia Federal. A cross-border laundering investigation; 2026-08-13. Verified on 2026-11-22. Indexed primary passage reviewed; full text not reviewed.

S119: Official source. A federal regulatory agency; 2026-09-03 (article URL withheld). Verified on 2026-11-22.

S120: CTIR Gov / GSI. Government website search poisoning; 2026-09-08. Verified on 2026-11-22.

S122: Polícia Federal. An institutional extortion investigation; 2026-10-07. Verified on 2026-11-22.

S124: Official source. A federal agency preventive service suspension; 2026-10-21 (article URL withheld). Verified on 2026-11-22.

S125: ANPD. A municipal health-data publication case; 2026-10-26 (article URL withheld). Verified on 2026-11-22.

S126: Caixa Seguridade. Caixa Seguridade: CVP market notice, 12 November 2026. Verified on 2026-11-22.

S127: Ministério da Fazenda / Tesouro Nacional. Tesouro Nacional incident notice, 13 November 2026. Verified on 2026-11-23.

S128: Autoridade Portuária de Santos. Santos partial administrative recovery, 16 November 2026. Verified on 2026-11-22.

S129: Polícia Federal. An international digital-fraud operation; 2026-11-17. Verified on 2026-11-22.

S130: Polícia Federal. A social-benefit digital-account fraud investigation; 2026-11-17. Verified on 2026-11-22.

S131: CNN Brasil. A large bank; 2026-11-18 (article URL withheld). Verified on 2026-11-22.

S132: Viva. A delivery platform; 2026-11-19 (article URL withheld). Verified on 2026-11-22.

S133: Official source. A telephone-message fraud facility; 2026-11-19. Verified on 2026-11-22. Indexed primary passage reviewed; full text not reviewed.

S134: Banco Central do Brasil. A financial institution; not resolved; indexed current registry (article URL withheld). Verified on 2026-11-22. Indexed primary passage reviewed; full text not reviewed.

S135: Banco Central do Brasil. A financial institution; not resolved; PDF indexed around April 2026 (article URL withheld). Verified on 2026-11-22. Indexed primary passage reviewed; full text not reviewed.

S136: Banco Central do Brasil. A public-sector institution; not resolved; current registry (article URL withheld). Verified on 2026-11-22. Indexed primary passage reviewed; full text not reviewed.

S137: Banco Central do Brasil. A public-sector institution; not resolved; current registry (article URL withheld). Verified on 2026-11-22. Indexed primary passage reviewed; full text not reviewed.

S138: Banco Central do Brasil. A financial institution; not resolved; current registry (article URL withheld). Verified on 2026-11-22. Indexed primary passage reviewed; full text not reviewed.

S139: Banco Central do Brasil. A public-sector access incident; 2025; registry updated in 2026 (article URL withheld). Verified on 2026-11-22. Indexed primary passage reviewed; full text not reviewed.

S147: CTIR Gov / GSI. An official campaign warning; 2026-05-21. Verified on 2026-11-22.

S148: CTIR Gov / GSI. An official campaign warning; 2026-05-21. Verified on 2026-11-22.

S149: CTIR Gov / GSI. An official campaign warning; 2026-05-21; recommendation03 updated 2026-06-17. Verified on 2026-11-22.

S150: CTIR Gov / GSI. An official campaign warning; 2026-05-21. Verified on 2026-11-22.

S151: CTIR Gov / GSI. An official campaign warning; 2026-05-21. Verified on 2026-11-22.

S152: CTIR Gov / GSI. An official campaign warning; 2026-05-21. Verified on 2026-11-22.

S153: CTIR Gov / GSI. An official campaign warning; 2026-06-24. Verified on 2026-11-22.

S154: Polícia Federal. An infostealer distribution investigation; 2026-08-04 12:23. Verified on 2026-11-22.

S155: Polícia Federal. A bank-fraud proceeds investigation; 2026-11-09 14:54. Verified on 2026-11-22.

S156: Polícia Federal. An electronic bank-fraud investigation; 2026-11-11 07:59. Verified on 2026-11-22.

S161: Kaspersky GReAT. An attributed information-theft and espionage campaign; 2026-07-03. Verified on 2026-11-23.

S165: Official source (address withheld; held in the private evidence record). A public-sector health-program portal; 2026-11-19 notice. Verified on 2026-11-23. Indexed primary passage reviewed; full text not reviewed.

S166: Unimed Natal. A regional healthcare cooperative; 2026-11-14 primary notice; 2026-11-18 FAQ index. Verified on 2026-11-22.

S167: Prefeitura de Cuiabá. A shared state sanitary-surveillance platform; 2026-11-02 16:27 state primary; 2026-11-09 09:52 municipal follow-up. Verified on 2026-11-22.

S169: Investor-authored financial statement. Subsequent-event note 16, financial statements authorised 12 November 2026; third-party-hosted copy (article URL withheld). Verified on 2026-11-22.

S170: Agência Brasil. Public-benefits query-service reporting, 26 May 2026 (article URL withheld). Verified on 2026-11-22.

S171: Convergência Digital. Operator statement on attack attempts, 5 November 2026 (article URL withheld). Verified on 2026-11-22.

S172: Official source (address withheld; held in the private evidence record). Project-portal incident notice; incident identified 4 October 2026. Verified on 2026-11-22.

S173: Diário do Comércio. Digital-commerce platform notification reporting, 13 November 2026 (article URL withheld). Verified on 2026-11-22.

S174: Official source (address withheld; held in the private evidence record). Cooperative security notice; incident identified 1 June 2026. Verified on 2026-11-22.

S175: Official source (address withheld; held in the private evidence record). Judicial-deposit platform continuity notices, September 2026. Verified on 2026-11-22.

S177: Official financial-sector source (address withheld; held in the private evidence record). Incident statement, updated 5 November 2026. Verified on 2026-11-23.

S178: Official source (address withheld; held in the private evidence record). Shared publication and messaging systems notice, 21 September 2026. Verified on 2026-11-22. Indexed primary passage reviewed; full text not reviewed.

S179: CNN Brasil. Court file-exposure reporting, 16 November 2026 (article URL withheld). Verified on 2026-11-22.

S180: Diário de Pernambuco. Operator-authored portal statement, 27 October 2026; reproduced by original recipient (article URL withheld). Verified on 2026-11-22.

S181: Mobile Time. Hospital-authored patient-data statement, 8 October 2026; reproduced by original recipient (article URL withheld). Verified on 2026-11-22.

S182: Official source (address withheld; held in the private evidence record). An examination-services provider; chronology and scope review. Verified on 2026-11-22.

S183: Attributed public reporting. A financial-services provider; chronology and scope review (article URL withheld). Verified on 2026-11-22.

S184: Attributed public reporting. A university; chronology and scope review (article URL withheld). Verified on 2026-11-22. Indexed primary passage reviewed; full text not reviewed.

S185: Official source (address withheld; held in the private evidence record). A state-court electronic case-service platform; chronology and scope review. Verified on 2026-11-22.

S186: Official source (address withheld; held in the private evidence record). State public-sector systems investigated for unauthorized access; chronology and scope review. Verified on 2026-11-22. Indexed primary passage reviewed; full text not reviewed.

S187: Attributed public reporting. A public warning platform; chronology and scope review (article URL withheld). Verified on 2026-11-22. Indexed primary passage reviewed; full text not reviewed.

S188: Official source (address withheld; held in the private evidence record). A bank-workers union virtual voting platform; chronology and scope review. Verified on 2026-11-22.

S189: Attributed public reporting. A fictitious banking-dispute example; chronology and scope review (article URL withheld). Verified on 2026-11-22.

S190: Attributed public reporting. A utility; chronology and scope review (article URL withheld). Verified on 2026-11-22.

S191: Attributed public reporting. A diagnostics group; chronology and scope review (article URL withheld). Verified on 2026-11-22.

S192: Attributed public reporting. A healthcare operator; chronology and scope review (article URL withheld). Verified on 2026-11-22.

S193: Official source (address withheld; held in the private evidence record). A logistics operator; chronology and scope review. Verified on 2026-11-22.

S194: CNN Brasil / Estadão. Bank customer-notice excerpts, 18–19 November 2026 (article URL withheld). Verified on 2026-11-22.

S195: Viva. Delivery-platform company-notice account, 19 November 2026 (article URL withheld). Verified on 2026-11-22.

S196: Official source (address withheld; held in the private evidence record). Academic-data investigation notice, 17 November 2026. Verified on 2026-11-22.

S197: BNews Alagoas. Public-portal possible-incident press note, 20 November 2026 (article URL withheld). Verified on 2026-11-22.

S201: Estadão / UOL. Banco do Nordeste temporary Pix suspension, 27 January 2026. Verified on 2026-11-22.

S226: Agência Brasil. Caixa Seguridade incident reporting, 12 November 2026. Verified on 2026-11-22.

S227: CNN Brasil. Treasury personal-data disclosure reporting, November 2026. Verified on 2026-11-22.

S228: Folha de S.Paulo. Santos administrative-system recovery reporting, 16 November 2026. Verified on 2026-11-22.

S229: Autoridade Portuária de Santos. Terminal consultation and recovery update, 17 November 2026. Verified on 2026-11-22.

S230: Autoridade Portuária de Santos. Security contingency update, 19 November 2026. Verified on 2026-11-22.

S231: Banco do Nordeste. First-half 2026 management report: January incident loss and recovery. Verified on 2026-11-23. Indexed primary passage reviewed; full text not reviewed.

S232: Cybernews original investigation. Multicountry point-of-sale malware investigation; August 2026 discovery. Verified on 2026-11-23.

S233: Prefeitura de Belo Horizonte. Payment-guide incident statement, updated 19 November 2026. Verified on 2026-11-23.

S234: Diário do Comércio. Belo Horizonte incident reporting, 16 November 2026. Verified on 2026-11-22.

S266: BNews RN. Unimed Natal care continuity and system recovery reporting, 19 November 2026. Verified on 2026-11-22.

S268: SES-MT / Secom Mato Grosso. SES trabalha para restabelecer sistemas após novo ataque hacker, 2 November 2026. Verified on 2026-11-22.

S269: CNN Brasil. Secretaria de Saúde de MT é alvo de ataque; sistemas suspensos, 3 November 2026. Verified on 2026-11-22.

S270: Registro do Dia. Cuiabá extends licensing deadlines after shared SES incident, 10 November 2026. Verified on 2026-11-22.

S300: BTG Pactual. Issuer-authored letter to CVM, 24 March 2026; third-party-hosted copy. Verified on 2026-11-22.

S301: TI Inside. BTG Pactual temporary Pix suspension, 22 March 2026. Verified on 2026-11-22.

S302: Hospital Sírio-Libanês. Official information-security incident questions and answers. Verified on 2026-11-22.

S303: UOL. Sírio-Libanês report-system investigation, 16 October 2026. Verified on 2026-11-22.

S304: Elastic Security Labs. KREMLIN browser-extension and banking-session research, 14 September 2026. Verified on 2026-11-22.

S305: ANY.RUN. PhantomEnigma investigation, 16 July 2026. Verified on 2026-11-22.

S306: Supremo Tribunal Federal. Press note on a tax-record access investigation, 17 February 2026 (article URL withheld). Verified on 2026-11-23.

S307: Official source (address withheld; held in the private evidence record). Court statement on document-borne AI instructions, 20 May 2026. Verified on 2026-11-22.

S308: Official source (address withheld; held in the private evidence record). Preventive service restrictions, 22 October 2026. Verified on 2026-11-22.

S309: CNN Brasil. Education website attack-attempt reporting, 15 November 2026 (article URL withheld). Verified on 2026-11-22.

S310: UOL. Financial-service security incident reporting, 21 April 2026 (article URL withheld). Verified on 2026-11-22.

S311: Baguete. Retail financial-services restrictions, 27 July 2026 (article URL withheld). Verified on 2026-11-22.

S313: Socket. Malicious banking SDK and certificate theft research, 28 May 2026 (article URL withheld). Verified on 2026-11-22.

S314: Cemig. Material fact: personal-data exposure, 14 May 2026. Verified on 2026-11-23.

S315: Diário do Comércio. Cemig personal-data incident reporting, 15 May 2026. Verified on 2026-11-22.

S316: CTIR Gov / GSI. Provider-data and source-code exposure warning, 21 May 2026. Verified on 2026-11-22.

S317: CTIR Gov / GSI. Provider-system technical recommendation, 22 May 2026. Verified on 2026-11-22.

S318: CTIR Gov / GSI. Cloud-resource abuse and cryptojacking warning, 24 June 2026. Verified on 2026-11-22.

S319: CTIR Gov / GSI. Website alteration and framework security warning, 14 August 2026. Verified on 2026-11-22.

S320: CTIR Gov / GSI. Content-management security guidance; updated 10 November 2026. Verified on 2026-11-22.

S321: CTIR Gov / GSI. Mail-client security guidance; updated 16 November 2026. Verified on 2026-11-22.

S322: CTIR Gov / GSI. Web-server security guidance; updated 19 November 2026. Verified on 2026-11-22.

S323: Folha de S.Paulo. Public-safety platform data-disclosure investigation reporting, 13 November 2026 (article URL withheld). Verified on 2026-11-22.

S324: Banco Central do Brasil. Financial Stability Report, October 2026, section2.5, pages79–84. Verified on 2026-11-22.

S325: Folha C-Level. Independent bank customer-notice coverage, 19 November 2026 (article URL withheld). Verified on 2026-11-22.

S326: Canaltech. Delivery-platform population-specific notice coverage, 19 November 2026 (article URL withheld). Verified on 2026-11-22.

S327: Itatiaia. University academic-data inquiry and separate hardware outage, 21 November 2026 (article URL withheld). Verified on 2026-11-22.

S328: Jornal Extra Alagoas. Public-portal official press-note reproduction, 20 November 2026 (article URL withheld). Verified on 2026-11-22.

Appendix D. Glossary

Term	Plain meaning
Account disposition	The recorded decision that an account is active, contained, remediated, historical or not owned
Affected-person notice	Information sent to people about a personal-data incident and relevant protection steps
Analytical model	A reasoned planning relationship that is not a proven operational connection
Authentication	Checking that a person, device or service is the identity it claims
Authorisation	Permission for that identity to perform a particular action
Banking as a service	Financial functions provided through another organisation's service and permissions
Beneficiary validation	Checking that a payment destination is the intended, authorised recipient
Browser extension	Software added to a browser that may receive access to browsing or account activity
Certificate revocation	Ending trust in a digital certificate before its normal expiry
Claim	A source assertion whose underlying access, possession or impact is not independently established here
Controller	The entity responsible for decisions about personal-data processing under the relevant law
CPF	Brazil's individual taxpayer identifier; knowing it does not establish permission to use an account
CNPJ	Brazil's register and identifier for companies, associations and other legal entities [S30]
Credential	Information or material used to authenticate an identity
Data category	A type of information, such as contact details, financial data or authentication information
Device association	An observation connecting a device record with a domain; ownership and current state require validation
Disclosure date	When information about an event became public, which may be later than the event
DLL loading	A Windows program loading a shared software component; the component's provenance matters

Term	Plain meaning
DDoS	Distributed denial of service, intended to prevent legitimate use through traffic or resource exhaustion
DMARC	A mail-domain policy and reporting standard that uses sender-authentication results
Extortion	A demand backed by a threat, such as disclosure of data; encryption is not required
Incident awareness	The relevant point at which the responsible entity knows facts about an incident
KYC	Identity-verification information or checks, commonly called know your customer
Listing	A published entry asserting a victim or offering material; it is not independent incident confirmation
MFA	Multi-factor authentication, using more than one kind of evidence to authenticate an identity
Mutual TLS	Certificate-based authentication in which both sides of a connection authenticate each other
NFSe	A service-invoice record used in municipal fiscal processes
Operator	An entity processing personal data on a controller's behalf under the applicable framework
Pix key	An identifier used to locate a payment recipient; it does not alone authorise a transfer
Privilege	A permission or level of authority held by an account or service
Ransomware	Malware associated with coercive denial of access, commonly through encryption
Reconciliation	Checking that records and transactions agree after interruption or a manual process
Session	An authenticated interaction that can remain valid separately from the password used to begin it
Signing material	Digital identity material used to authorise or validate a signed operation
Social engineering	Deception intended to make a person disclose information or perform an unsafe action
Supplier boundary	The division of systems, data and authority between an organisation and its provider
Token	Digital material representing an authentication or authorisation decision

Term	Plain meaning
Trusted alternate channel	A pre-established route used to verify messages or continue service when the main route is unreliable
Unverified	Not independently established in this report; it does not mean fabricated

The glossary explains terms used in the analysis. Regulatory definitions retain the scope of the cited instruments, especially for controller, operator and notification decisions. [S10][S11][S12]

ABOUT BRANDEFENSE

Attackers See You First. We make sure you do.

Brandefense is an AI-driven platform that sees your organization the way attackers do, continuously monitoring the open, deep, and dark web to detect phishing campaigns, credential leaks, exposed assets, and threat actor activity before they translate into breaches.

Built for security teams that can no longer afford to wait for threats to arrive at the perimeter, it processes millions of external signals in real time and returns only what demands attention.

Unifying Digital Risk Protection, External Attack Surface Management, and Cyber Threat Intelligence under a single interface, Brandefense gives CISOs and SOC teams the external visibility they have always been missing and the intelligence to act on it with confidence.

GARTNER PEER INSIGHTS
4.7 / 5

COVERAGE
3 pillars
CTI, DRPS, EASM

MONITORING
24 / 7
Open, deep and dark web

REQUEST A DEMO

Request A Demo. See what attackers see.

Discuss your domains, brands and security priorities in a 30-45 minute session with Sales and Presales. A Brandefense team member or a partner in your region will follow up.

Request a demo →

AWARDS

Recognised Around The World. Technology and trust.

Selected awards recognising Brandefense technology and innovation.



Top InfoSec Innovator

2026



Deloitte Technology Fast 500 EMEA

2024



Global InfoSec Awards

2025



Cybersecurity Excellence Awards

2025

See Brandefense In Action.

Bring your domains, brands and security priorities to a 30-45 minute conversation with Sales and Presales.

Request a demo →

BRANDEFENSE

See what attackers see. Before they act.

UNITED STATES

300 Delaware Ave. Ste 210 #328
Wilmington, DE 19801

TÜRKIYE

Üniversiteler Mh., 1605 Cd.
Cyberpark Vakıf Binası No: B25
Çankaya, Ankara

BRANDEFENSE.IO