BRANDEFENSE COUNTRY REPORT · CHILE 2026

Brandefense Chile Cyber Threat Landscape Report 2026

Identity, extortion claims and essential-service continuity

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

98 of 250
selected organisations had a credential listed for sale when checked

6
detailed claim dossiers, not six confirmed intrusions

41
Chilean ransomware listings in the observation window

25
selected banking, payment and investment domains, not a bank census

CONTENTS

Contents

01	Executive summary	05
	Report map	09
02	Chile's digital and security context	10
03	National exposure: a selected domain portfolio	14
04	Underground evidence and claim interpretation	22
05	Incidents, claims and response decisions by sector	37
06	Hacktivism, DDoS and service availability	53
07	Threat actors and supported relationships	57
08	The fraud economy	67
09	Banking and financial services	71
10	Regulation and national response	76
11	Outlook and conditional planning	83
12	Action plan	87
A	Appendix A. Scope and evidence boundaries	94
B	Appendix B. Evidence register	96
C	Appendix C. Sources	98
D	Appendix D. Glossary	102
	About this report	104

Board and executives	01 05 11 12
CISO and delegate	03 04 05 10 12
Intelligence and SOC	04 06 07 B
Fraud and customer support	05 08 09
Legal and privacy	05 10 A

About this edition

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

Chile's visible threat picture connects account misuse, data claims, financial deception and interrupted services; validate the specific exposure while preserving the function people depend on.

27,891

Chile-associated post-volume observations; not an incident count

400

post-volume observations in 8–22 November; not new intrusions

41

Chilean ransomware listing rows; criminal assertions

250

selected organisation domains; not a national census

The post-volume, listing and selected-domain populations are separate. Their counts must not be added. The narrative evidence is bounded by the retained material and source accounts described in each chapter. [S1][S2] [S5]

Contents and reading routes

Chapter	Decision question	First reader
1 Executive summary	Which decisions deserve immediate ownership?	Leadership and CISO
2 Context	Which national conditions change the response?	CISO and legal
3 Selected-domain exposure	Which measurements are available, and what remains unknown?	Security and infrastructure
4 Underground evidence	What do the advertisements actually establish?	Intelligence and response
5 Sector cases	Which consequences require different owners?	Service, privacy and fraud teams
6 DDoS and availability	What separates disruption from established access?	Operations and communications
7 Actors and relationships	Which source supports each actor-related proposition?	Intelligence and leadership
8 Fraud economy	How should teams interrupt credible deception?	Fraud, treasury and support
9 Financial services	Which institutional and customer questions must remain separate?	Financial security and compliance
10 Regulation	Which duty, trigger and reporting clock apply?	Legal and delegate
11 Outlook	Which signals should change the plan?	Leadership and risk
12 Action plan	Who delivers, and what demonstrates completion?	Accountable owners
Appendices A–D	What are the evidence boundaries, cards, sources and terms?	All readers

Leadership can start with Chapters 1, 5, 11 and 12. Responders can follow Chapters 3, 4, 6 and 7. Fraud, legal and customer teams can use Chapters 8–10 alongside the specific sector case.

The evidence labels are **observation**, **claim**, **reported official account** and **analyst inference**. An observed advertisement remains a claim about its contents. A confirmed service limitation can leave data access, actor identity and entry route unresolved.

CHAPTER 01

Executive summary

01

THIS CHAPTER ANSWERS

What does Chile's evidence justify doing first, and how should leaders verify the response?

4

leadership decisions with accountable owners

Four decisions for leaders 07

The year in numbers 07

CHAPTER 01

Executive summary

IN SHORT

Chile's evidence supports identity validation, essential-service recovery, customer protection and reporting readiness. Criminal posts advertise provider files, privileged access, education records and health information. Their assertions are not confirmed intrusions. Official and reported organisational accounts distinguish valid-account access, historical republication, possible extraction and service interruption. Assign an owner to each relevant signal, verify the affected account or function, and exercise the reporting decision before the short statutory clock starts.

This report combines Brandefense's retained underground material and ransomware listings with passive domain observations and public sources. It preserves separate populations, dates and confidence boundaries. No post, listing, selected domain or public notice is converted automatically into a unique national incident. [S1][S2][S3][S5]

The incident window is 1 January–22 November 2026. The closing fortnight, 8–22 November, is highlighted separately. Publication time does not establish intrusion time. Some newly public material is historical, while a new update can concern an interruption that began months earlier.

1. Account evidence requires a narrower response than a broad leak headline. ANCI's May update identified unauthorised access with valid credentials and distinguished it from infrastructure attacks. Its later historical-data notice attributed another alert to older material. Validate account purpose, validity, privileges and current activity before deciding how widely to contain. [S7][S8]

2. Provider and institutional advertisements remain claims about access and files. Six detailed underground dossiers cover provider uploads, consultancy material, a bank-related administration portal, education data, a historical school dataset and health records. The text establishes offers and assertions. It does not establish the claimed quantities, successful sales or a separate incident at every named customer. [S1]

3. Extortion visibility is concentrated, but preparation must work beyond two labels. Ransompedia records 41 Chilean listing rows across 13 labels. Qilin and The Gentlemen account for 26, or 63.4%. The remaining 15 carry other labels. Listings support recovery and disclosure preparation, not a count of confirmed encryption or theft. [S2]

4. Operational consequences differ even within essential services. Hospital reporting separates interrupted booking from maintained clinical care. Electricity records describe a generation facility's continuing unavailability. A retailer's later update adds logistics and sales-channel disruption. Recovery needs the relevant service owner's acceptance, not a general statement that systems are back. [S34][S53][S86][S52]

5. Existing reporting duties and proposed changes need different treatment. Law 21.663's relevant early-warning maximum is three hours. ANCI's November MFA document remains a consultation. Parliamentary approval of a data-law postponement does not establish completed enactment and publication. Preserve the legal instrument, applicable entity and awareness time supporting each decision. [S13][S15][S31][S50]

Four decisions for leaders

1. **Ensure relevant evidence reaches an owner.** Test alert delivery and escalation, then validate current identity and service signals against the organisation's own evidence. Record current, historical, unrelated and unresolved dispositions.
1. **Demonstrate minimum service and safe recovery.** Ask the business owner to complete the essential task during degradation. Restore records and reconcile interrupted work before accepting the service as recovered.
1. **Join supplier, customer and fraud response.** Obtain a scoped supplier account and provide an independent verification route for suspicious contact. Do not close customer protection solely because technical service has returned.
1. **Exercise the applicable reporting decision.** Confirm legal scope, OIV status, contacts and the awareness chronology. Test an out-of-hours event with legal, the cybersecurity delegate and the relevant operational owner.

The year in numbers

27,891

Chile-associated post-volume observations in the requested window

WHAT IT DOES NOT MEASURE

Confirmed attacks or unique victims

400

Recent post-volume observations for 8–22 November

WHAT IT DOES NOT MEASURE

Intrusions beginning in that fortnight

41

Chilean ransomware listing rows

WHAT IT DOES NOT MEASURE

Independently confirmed intrusions

39

Distinct organisation-name strings in those listing rows

WHAT IT DOES NOT MEASURE

Validated independent legal organisations

19 / 7 / 15

Qilin / The Gentlemen / other listing rows

WHAT IT DOES NOT MEASURE

Operators, paid ransoms or loss totals

250

Selected organisation domains in ten sector groups

WHAT IT DOES NOT MEASURE

National prevalence or a revenue ranking

98 / 250

Selected organisations with a credential listed for sale when checked

WHAT IT DOES NOT MEASURE

Confirmed intrusions or completed sales

58/100 (B)

National Atlas headline for the selected portfolio

WHAT IT DOES NOT MEASURE

A breach percentage or sector rating

324

Significant-incident reports received by ANCI in January–June

WHAT IT DOES NOT MEASURE

A count through November or unique affected organisations

Sources: retained Brandefense observations, listing aggregates and exposure snapshot [S1][S2][S5][S210], and ANCI's first-semester reporting [S9][S10].

Of 250 selected organisations, 98 had a credential listed for sale when checked. The national Atlas headline is 58/100 (B). 795,641 device associations and 2,999,478 credential-record associations require separate account and endpoint validation. These overlapping observations do not establish national prevalence or confirmed intrusions. [S210]

The closing-fortnight evidence deserves attention without overstating novelty. A school-data offer explicitly spans older years. A separate education/photos claim and an electoral-data assertion have unresolved provenance. The latter does not establish a current election-system intrusion or an effect on any election. [S1]

For a reader handling a current event, start with the case that matches the evidence rather than the sector name alone. The same sector can face account misuse, unavailable services, supplier-held information and impersonation. Each requires a different validation and completion test.

KEY TAKEAWAYS

01

Validate the specific identity, data or service proposition behind a claim.

02

Keep posts, listings, public cases and selected-domain observations separate.

03

Demand owned decisions and demonstrated service, customer and reporting readiness.

Report map

Start with the decision you own, then follow the evidence, its boundary and the completion test.

Board and executives	Can the organisation protect its essential function and make timely decisions?	01 05 11 12
CISO and delegate	Which observations justify validation or containment?	03 04 05 10 12
Intelligence and SOC	Which statements are observed, asserted or corroborated?	04 06 07 B
Fraud and customer support	How can credible information be used to induce a harmful action?	05 08 09
Legal and privacy	Which entity, source, date and trigger support the decision?	05 10 A

Evidence track	Supports	Does not establish
Held underground text	An offer, release claim or request exists	Possession, freshness, sale or impact
Criminal listing	A claimant publication exists	Encryption, theft or a unique organisation
Public account	The cited source's reported event and position	Unstated technical or attribution details
Passive observation	A dated configuration result for an assessed domain	Application security or national control effectiveness
Analyst inference	A bounded interpretation with alternatives	A verified relationship or future attack probability

CHAPTER 02

Chile's digital and security context

THIS CHAPTER ANSWERS

Which national conditions change the decisions a Chilean defender must make?

324

significant-incident reports received by ANCI in the first semester

2.1 Connectivity makes identity and service decisions broadly relevant 11
2.2 National reporting describes a different population 11
2.3 Valid accounts change the containment question 12
2.4 Essential services create an operating obligation 12
2.5 Financial fraud crosses institutional boundaries 13
2.6 Attribution and publication dates need separate evidence 13
2.7 Regulatory dates need a current status check 13

CHAPTER 02

Chile's digital and security context

IN SHORT

Chile's public evidence puts identity security, essential-service continuity and financial fraud in the same operational picture. ANCI's incident reports, public disclosures and criminal advertisements describe different populations. They cannot be combined into a national attack total. Regulatory designation also creates obligations without implying that an organisation suffered an incident. Identify the accounts, services, suppliers and reporting duties your organisation owns, then test their response together.

2.1 Connectivity makes identity and service decisions broadly relevant

DataReportal's Digital 2027 Chile edition was published on 5 November 2026. Its October 2026 observation estimates 19.1 million internet users and 95.6% population penetration. The edition title does not make those figures a forecast for 2027. [S85]

These estimates describe connectivity, not cyberattack prevalence or control effectiveness. They support attention to accessible customer, citizen and employee services without supplying a denominator for the criminal posts or organisational incidents in this report.

2.2 National reporting describes a different population

ANCI reported 324 significant-incident reports for January–June 2026. Its October threat assessment and cybersecurity-month announcement give the same first-semester figure. This is neither a count through November nor a total of unique affected organisations. [S9][S10]

A later press account quotes an ANCI transparency response recording 566 significant-effect incident reports from 1 January through 15 October. That is a different period and a reported official response, not a count through this report's cut-off. [S71]

The same account notes that reporting began in March 2025 and that reporting uptake can affect comparisons. It does not support reading the change as an equivalent increase in underlying attacks. Preserve the reporting universe and period when presenting the figure. [S71]

The following populations support different decisions.

Population	Unit	Appropriate use	Boundary
ANCI reporting	Significant-incident reports in a stated period	Understand the authority's reported caseload	Not a complete national incident census
Public disclosures	Statements and reported incidents	Compare response choices and supported consequences	Publication and intrusion dates can differ
Underground posts	Messages, offers and claims	Validate leads relevant to owned assets	Not verified possession or successful access
Ransomware listings	Criminal publications	Prepare extortion and continuity response	Not confirmed theft or encryption
Selected domains	Organisation-associated observations	Investigate specific exposure signals	Not national prevalence or independent legal entities

2.3 Valid accounts change the containment question

ANCI's May statements show why credential access requires a specific assessment. Its initial notice described an investigation into reported data publications. A later update identified unauthorised access using valid user credentials, probably obtained from earlier leaks or information-stealing malware. [S6][S7]

The agency distinguished those findings from an attack against the underlying infrastructure. It did not support a general claim that the state had been accessed as one environment. The response should therefore begin with the affected identity and the service it could reach. [S7]

For an organisation receiving an account-related alert, ownership, validity and privileges come before a conclusion about the wider network. A password found in historical material needs a different response from evidence that a current privileged account was used. A single label such as data leak hides that distinction.

2.4 Essential services create an operating obligation

ANCI's July designation notice reported a combined first-process total of 1,154 operators of vital importance, or OIV. The notice describes reinforced responsibilities, including a cybersecurity delegate, training, security management and continuity planning. Designation is regulatory status, not incident evidence. [S11]

The practical unit is the designated legal entity and its relevant services. A corporate group should not assume that one entity's status applies identically to every affiliate. Equally, an organisation should not infer its status from this report's sector label or selected-domain list.

The security delegate needs access to the people who can make operational decisions. A technical team can assess an affected account. A service owner must judge the minimum acceptable function and the consequences of restricting access. Legal and compliance teams determine which reporting duties apply.

2.5 Financial fraud crosses institutional boundaries

In August, Fiscalía described a national coordination table involving the prosecution service and nine public and private financial bodies. The notice identifies business-email fraud, phishing, malware, payment fraud, investment scams and false job offers among relevant variants. [S29]

ANCI's September bank-account warning illustrates this problem. It describes fraudsters provoking an account block and then pretending to be the bank to seek a verification code or authorisation. The apparent match between an account problem and a subsequent call is part of the deception. [S21]

2.6 Attribution and publication dates need separate evidence

Telecommunications reporting in August described an investigation informed by US authorities, with some observed activity dating from 2024. The publication date does not establish that the activity began in 2026. Actor and state-association descriptions remain the cited sources' assessments. [S45]

The November public-service case contains competing accounts of the technical mechanism. The evidence does not support resolving that disagreement through speculation about an operator. Keep service impact, access, chronology and attribution as separate propositions. [S36]

2.7 Regulatory dates need a current status check

Two recent developments require different treatment. CMF says its reinforced-authentication rule entered full force on 1 August 2026. ANCI's November MFA document was still a public consultation at the cut-off. A draft standard is not an already effective obligation. [S27][S15][S16]

The personal-data timetable also needs care. The original law scheduled commencement for 1 December 2026. A 20 November parliamentary notice says a postponement bill moved to promulgation. Legislative approval alone does not establish that a new commencement date has been enacted and published. [S30][S31][S32]

KEY TAKEAWAYS

01

Preserve the period and unit when comparing national reporting with criminal publications.

02

Map identities and essential services to accountable operational and legal owners.

03

Treat political attribution and legal commencement as source-specific questions requiring their own evidence.

CHAPTER 03

National exposure: a selected domain portfolio

THIS CHAPTER ANSWERS

Which exposure observations require validation in the selected portfolio?

98 of 250

selected organisations had a credential listed for sale when checked

3.1 Universe card 15

3.2 Current listings and the national headline 16

3.3 Device and credential associations need context 17

3.4 Passive results and their boundaries 20

3.5 Ownership and completion evidence 21

CHAPTER 03

National exposure: a selected domain portfolio

IN SHORT

Of 250 selected organisations, 98 had a credential listed for sale when checked. The national Atlas headline is 58/100 (B). The portfolio contains 795,641 device associations and 2,999,478 credential-record associations. These observations can overlap and do not establish current account validity or national prevalence. Validate current listings, establish employee or customer context, and assign the appropriate identity, endpoint or fraud owner.

3.1 Universe card

Item	Definition
Selected population	250 primary-domain records across ten merged sector groups
Sector selection	25 records in each group, based on institutional and service relevance
Unit	Selected organisation-domain association; a domain alone does not establish independent legal identity or ownership
Resolving population	225 selected domains in the dated passive observation
Non-resolving population	25 selected domains; non-resolution is not a security verdict
Exposure date	22 November 2026; device, credential, document and listing observations describe the dated holdings, not only events beginning in 2026
Passive measurements	Dated DNS, mail-policy and HTTPS observations with their assessed denominators
Exposure measurements	Device, employee-device, credential-record, document and current credential-market observations
National rating	Atlas headline for the selected portfolio: 58/100 (B)

The sample describes selected services rather than national prevalence. Related companies can share control, and one organisation can operate several domains. Validate an association before attributing a finding to a legal entity. [S5]

The exposure snapshot and the incident window have different time bases. Historical credentials and repeated advertising can remain visible after remediation. The observation date does not establish when the underlying activity occurred. [S210]

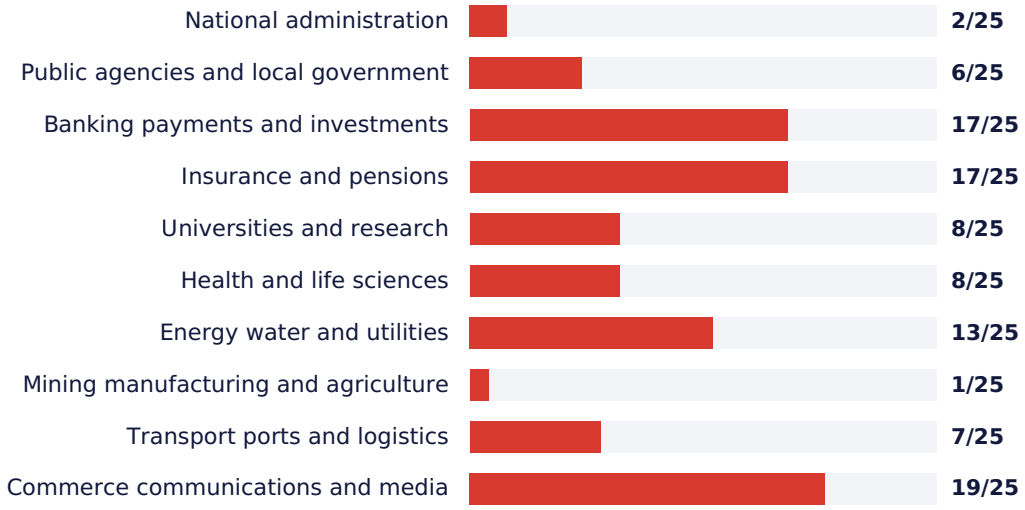
3.2 Current listings and the national headline

In the selected portfolio, 98 of 250 organisations had a credential listed for sale when checked. Credential-record associations concern 238 selected domains, device associations concern 238, and employee-device associations concern 200. These populations can overlap. [S210]

The national Atlas headline is 58/100 (B). Higher values indicate greater observed exposure within this selected portfolio. The rating is not a breach percentage, an intrusion probability or a certification of control effectiveness. [S210]

Only the national rating is published. Sector rows show signal counts and their denominators. They do not provide sector or organisation security ratings.

Current credential listings concern selected domains across sector groups



Current credential listings by sector (coral); selected-domain denominators. No sector risk ratings. Source: Brandefense exposure snapshot, 22 November 2026 [S5][S210]. 250 selected domains; cumulative overlapping associations, not unique people or confirmed intrusions.

Sector	Domains	Currently listed	Documents
National administration	25	2	5,285
Public agencies and local government	25	6	1,426
Banking payments and investments	25	17	2,359
Insurance and pensions	25	17	185
Universities and research	25	8	4,601
Health and life sciences	25	8	133
Energy water and utilities	25	13	359

Sector	Domains	Currently listed	Documents
Mining manufacturing and agriculture	25	1	135
Transport ports and logistics	25	7	450
Commerce communications and media	25	19	2,212

The document column totals 17,145 associations across 149 selected domains. A document association does not establish confidentiality, unlawful access or adversary possession. Public documents and repeated material remain possible explanations. [S210]

98 / 250

Selected organisations with a credential listed for sale when checked

58/100 (B)

National Atlas headline for the selected portfolio

149 / 250

Selected domains with document associations

3.3 Device and credential associations need context

The portfolio contains 795,641 device associations, including 23,676 employee-device associations. It also contains 2,999,478 credential-record associations. The following table preserves separate units. [S210]

Sector	Domains	Devices	Employee devices	Credential records
National administration	25	49,507	430	61,050
Public agencies and local government	25	55,505	748	127,556
Banking payments and investments	25	151,575	1,151	249,271
Insurance and pensions	25	124,175	431	67,612
Universities and research	25	51,929	15,703	2,022,142
Health and life sciences	25	13,420	278	22,281

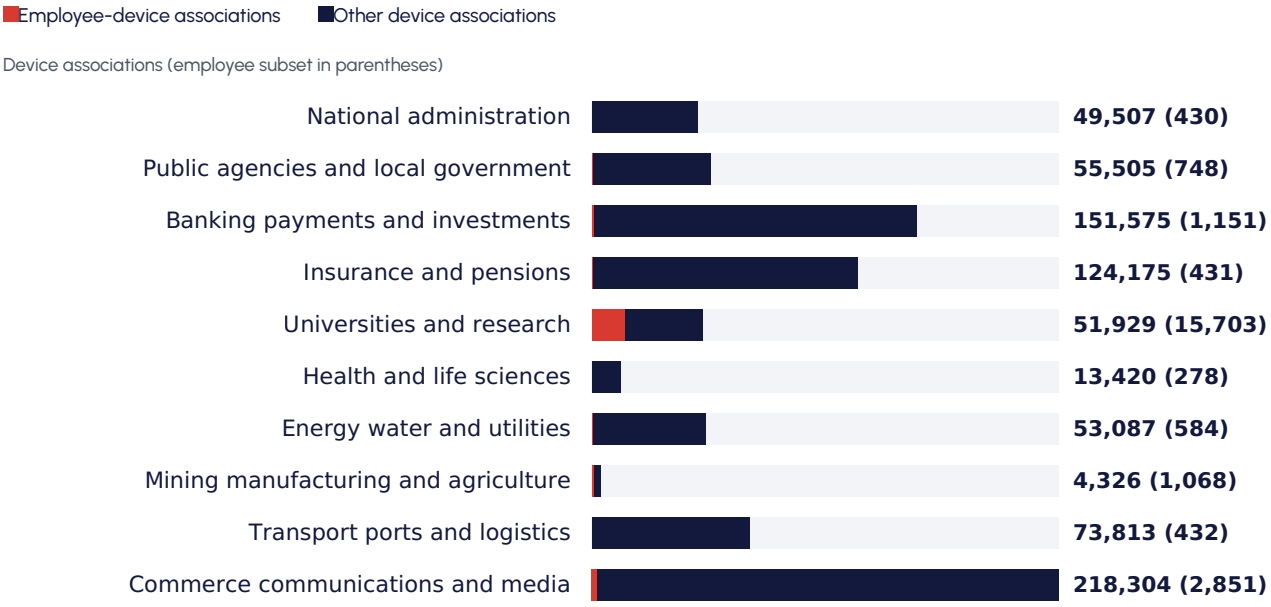
Sector	Domains	Devices	Employee devices	Credential records
Energy water and utilities	25	53,087	584	63,078
Mining manufacturing and agriculture	25	4,326	1,068	88,617
Transport ports and logistics	25	73,813	432	36,538
Commerce communications and media	25	218,304	2,851	261,333
Total	250	795,641	23,676	2,999,478

Device totals are observed associations. Associations can overlap across domains. Employee-device associations appear within the device view and must not be added to it. Neither population is a distinct national endpoint count.

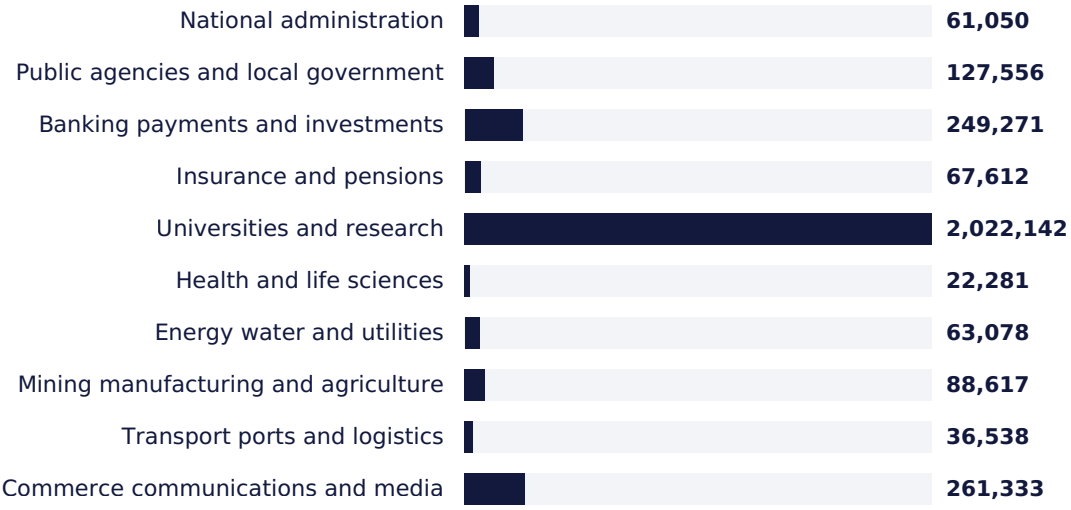
Universities and research account for 2,022,142 credential-record associations. Historical visibility and service populations can influence concentration. This does not establish the sector's current compromise rate or the number of affected people. [S210]

A customer-facing domain can appear on a customer's device. That association does not establish that the service operator owns the endpoint. Credential records likewise do not establish the source system, current validity or an internal intrusion.

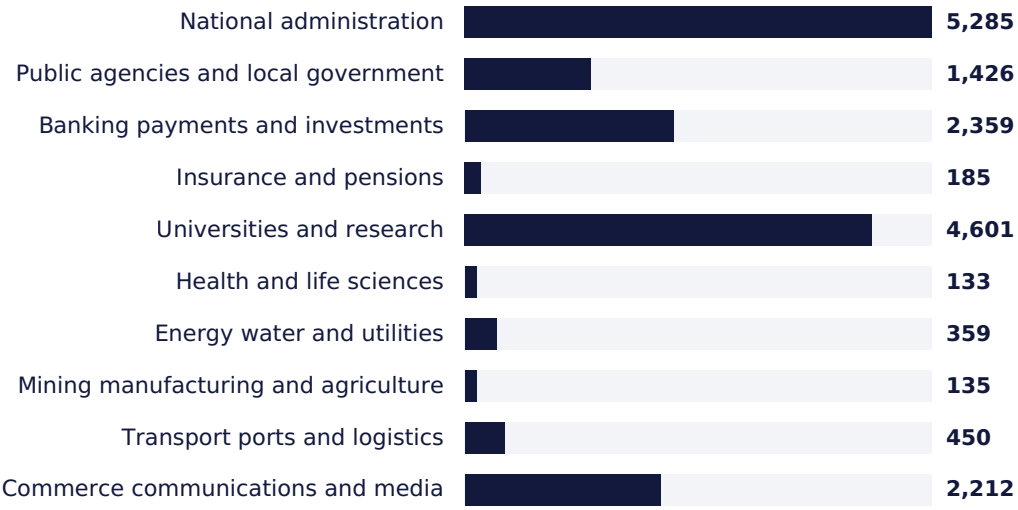
Sector device and credential populations differ in scale and meaning



Credential-record associations (separate scale)



Document associations (separate scale)



Source: Brandefense exposure snapshot, 22 November 2026 [S5][S210]. 250 selected domains; cumulative overlapping associations, not unique people or confirmed intrusions.

3.4 Passive results and their boundaries

Passive-control observations retain a separate denominator for each result

	DMARC	SPF	DKIM	DNSSEC DS	Valid TLS	HSTS
National administration	17/24	21/24	19/24	1/24	15/19	8/12
Public agencies and local government	19/21	21/21	18/21	1/21	16/17	6/15
Banking payments and investments	16/21	20/21	16/21	2/21	18/19	7/8
Insurance and pensions	21/23	20/23	18/23	0/23	19/21	18/19
Universities and research	10/24	24/24	22/24	0/24	19/20	12/23
Health and life sciences	6/23	16/23	15/23	0/23	15/17	7/13
Energy water and utilities	15/18	17/18	16/18	2/18	14/15	8/9
Mining manufacturing and agriculture	16/23	21/23	20/23	1/23	18/22	7/16
Transport ports and logistics	16/23	22/23	20/23	0/23	19/22	11/17
Commerce communications and media	15/25	24/25	20/25	4/25	24/24	10/17

Source: dated passive observations [S5]. Each result retains its assessed denominator. Observed policy does not establish enforcement or control effectiveness.

Control observation	Observed	Assessed population
DMARC quarantine or reject	151	225
SPF record observed	206	225
DKIM record observed	184	225
DNSSEC DS record observed	11	225
TLS certificate validation positive	177	196
HSTS header observed	94	149

A mail-policy observation supports a configuration review. It does not establish authentication or receiver enforcement for every legitimate message. Validate authorised senders and delivery requirements before changing production policy. [S3]

An unobserved DKIM record does not establish that mail is never signed. A DNSSEC-related record does not establish a validated chain for every service. A valid TLS result does not establish application security.

The passive pass covered 225 resolving domains. TLS results were conclusive for 196, and HTTP-header observations were available for 149. Inconclusive results remain unknown, and non-resolution is not evidence of a missing control. [S3]

3.5 Ownership and completion evidence

Function	Responsibility	Completion evidence
Domain owner	Confirm the organisation, service and administrative responsibility	Approved ownership and service record
Messaging	Validate authorised senders and intended authentication	Controlled delivery and policy review
Infrastructure	Assess relevant DNS and HTTPS observations	Dated local result and remediation decision
Identity and endpoint	Validate account freshness, privileges, employee context and sessions	Current, historical, unrelated or unresolved disposition
Fraud and customer protection	Validate customer-device and card relevance separately	Owned fraud assessment without an institutional-intrusion assumption

KEY TAKEAWAYS

01

Validate the 98 current-listing associations against owned accounts and services.

02

Keep devices, employee devices, credential records and documents as separate overlapping populations.

03

Assign identity, endpoint, fraud and configuration owners with dated completion evidence.

CHAPTER 04

Underground evidence and claim interpretation

THIS CHAPTER ANSWERS

What do Chile-associated advertisements establish, and which claims deserve an owned validation?

6

detailed claim dossiers, not six confirmed intrusions

4.1 Universe card 23

4.2 Monthly volume and the closing fortnight 23

4.3 The principal claim types require different checks 26

4.4 Detailed claim dossiers 27

4.5 Other specific offers and recent assertions 33

4.6 What changes a defender's decision 36

CHAPTER 04

Underground evidence and claim interpretation

IN SHORT

The held material advertises provider files, consultancy code, privileged access, education information and health records. Six dossiers preserve the claims, chronology, alternatives and limits. Recent posts include a historical school offer, another education claim and electoral-data material with unresolved provenance. None establishes a verified affected-person total or completed sale. Validate the assertion relevant to your accounts or records before choosing containment, notification or customer support.

4.1 Universe card

The post-volume population and the narrative evidence have different scope. The volume figures describe Chile-associated observations in the requested period. Narrative cards include relevant held material beyond that volume population. They are not presented as a strict subset of its count. [S1]

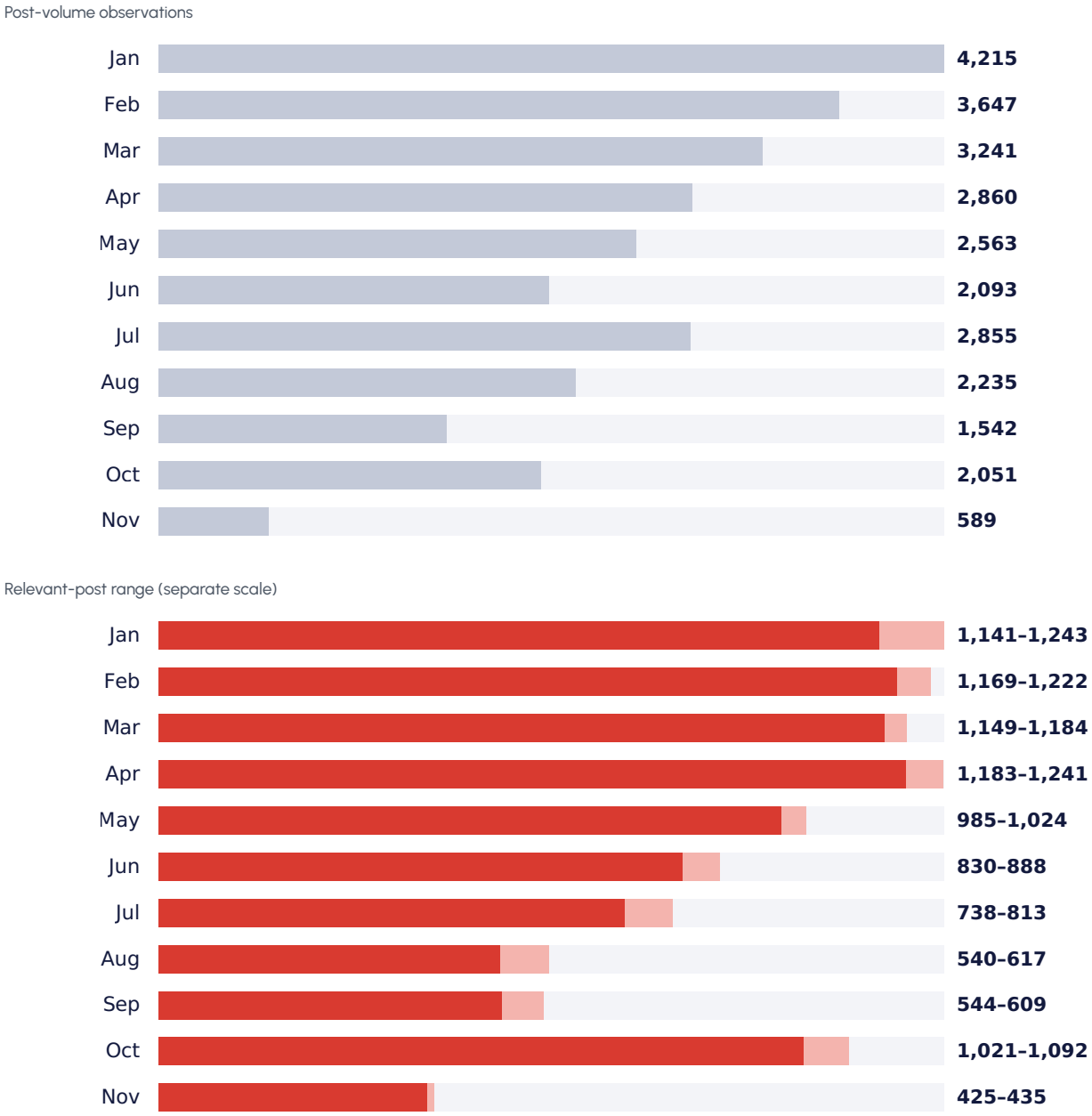
Item	Meaning
Window	Posts dated 1 January–22 November 2026
Volume observations	27,891 in the associated monthly totals
Recent volume	400 observations dated 8–22 November
Relevant content	Analytical range of 9,725–10,368 posts within the 27,890 held volume-population posts
Narrative evidence	Held offers and claims with specific source context
Counting boundary	Posts are not incidents, people, datasets or completed sales
Date boundary	Post dates do not establish extraction or intrusion dates
Relationship boundary	Similar wording or quantities do not independently establish common possession or operation

Country association is also narrower than targeting. A message can mention Chile within a broader offer or request. Its presence does not establish that the author operated in Chile or directed an intrusion at a Chilean institution.

4.2 Monthly volume and the closing fortnight

The monthly series shows observed publication volume. Changes can reflect the source population as well as activity. The final month is partial, and the series does not establish a comparable trend in successful intrusions. [S1]

Observed post volume falls from January while November remains partial



Source: Brandefense observations, 1 January–22 November 2026; November partial [S1]. Post-volume observations and overlapping themes are not confirmed incidents.

Month	Volume observations	Month	Volume observations
January	4,215	July	2,855
February	3,647	August	2,235
March	3,241	September	1,542
April	2,860	October	2,051
May	2,563	November to cut-off	589
June	2,093	Total	27,891

The closing fortnight has 400 volume observations. The number describes posts, not activity beginning in that period. A newly published school dataset can span many earlier years, and an electoral-data assertion can have unresolved public or historical provenance.

Platform observations describe messages, not actor nationality



Source: Brandefense observations, 1 January–22 November 2026; November partial [S1]. Post-volume observations and overlapping themes are not confirmed incidents.

Population	Observed count	Meaning
Telegram	27,578	Posts in the retained country-associated population
Forum	284	Posts in the retained country-associated population
Paste	24	Posts in the retained country-associated population
Discord	4	Posts in the retained country-associated population

Telegram accounts for 27,578 of 27,890 held posts in the corresponding volume population, or 98.9%. The narrative forum cases do not represent that platform distribution. Language counts are omitted because the available categories do not support an unambiguous comparison. [S1]

4.3 The principal claim types require different checks

The analytical range is 9,725–10,368 relevant posts within the 27,890 held volume-population posts. It is an analytical range, not a statistical confidence interval or a national activity estimate. [S1]

The narrative cases cover different alleged products: provider uploads, source code, privileged access and institutional records. They cannot be added as if they measured one kind of loss. A database row, an individual, a file volume and an access right are different units.

The retained claim themes overlap and require different validation owners



Source: Brandefense observations, 1 January–22 November 2026; November partial [S1]. Post-volume observations and overlapping themes are not confirmed incidents.

Theme	Post range	Boundary
Ransomware-related content	93–93	Overlapping content themes, not incidents
Data and database claims	2,909–2,975	Overlapping content themes, not incidents
Identity-document offers	2,002–2,125	Overlapping content themes, not incidents
Access offers	105–106	Overlapping content themes, not incidents
Information-stealer material	119–124	Overlapping content themes, not incidents
Credential packages	410–426	Overlapping content themes, not incidents

Theme	Post range	Boundary
Payment-card material	3,912–4,046	Overlapping content themes, not incidents
Financial-account offers	2,001–2,101	Overlapping content themes, not incidents
Phishing and fraud	1,058–1,112	Overlapping content themes, not incidents
Disruption-related content	8–8	Overlapping content themes, not incidents
Malware and vulnerability material	197–199	Overlapping content themes, not incidents

The chart's themes are descriptions of messages, not mutually exclusive incident categories. One advertisement can combine source code, credentials and customer records. Its presence in several themes does not create several intrusions or prove that every advertised component exists.

Payment-card theme counts describe posts discussing card-related material. They are separate from the distinct card-record population in Section 8.5. A message can discuss cards without establishing a usable card, a completed transaction or the source of exposure.

4.4 Detailed claim dossiers

A

CASE A

Provider uploads and a later sale announcement (B01, B02)

Technology services

Criminal claim; unverified

CLAIM	A quoted offer asserted 6.1 TB of customer uploads and application source code associated with a business software and hosting provider. A later post advertised sale availability. [S1]
CHRONOLOGY	A forum reply dated 4 April contains the quoted offer. A 15 April follow-up in the same thread says the material is for sale. The earlier text's date does not establish extraction time.
ESTABLISHED	The retained reply and follow-up contain related advertising. Customer names appearing in an offer are not independent confirmation that each customer suffered an incident.

ALTERNATIVE	The offer could exaggerate volume, combine older uploads or use a customer list to increase pressure. Related advertising does not establish that the offered files are authentic or complete.
LIMIT	The material's possession, extraction, customer-specific scope, completed sale, deletion and recovery are not established. The two posts do not justify a wider actor network.
RESPONSE	Request a provider account tied to your own service and records. Review relevant administrator access, tenant activity and shared credentials where internal evidence supports the concern.

Bottom line

Request a provider account tied to your own service and records. Review relevant administrator access, tenant activity and shared credentials where internal evidence supports the concern.

Evidence card B01 — 4 Apr 2026

Withheld | darkforums.su | Forum | ['EN']

ORIGINAL
we obtained 6.1TB of customer uploads

TRANSLATION
we obtained 6.1TB of customer uploads

Held
The retained post contains the quoted advertisement or release claim.

Not established
The advertised data or access was genuine, current, complete or usable. The post date is the intrusion or collection date.

Evidence card B02 — 15 Apr 2026

Withheld | darkforums.su | Forum | ['EN']

ORIGINAL
Data is now for sale

TRANSLATION
Data is now for sale

Held
A retained follow-up in the same forum thread says the data is for sale.

Not established
A sale occurred. The full offered material existed.

June reporting describes a mining client's account of an external platform-supplier event. The company said its corporate systems and production continuity were unaffected. Its preliminary associated-data estimate differed from larger allegations and a broader platform claim. [S44]

The provider also appears in Case A's source context. That overlap does not establish that the posts and company response concern the same event or files. The public response supplies context; it is not counted as another independent intrusion.

For a customer, the correct request is a scoped supplier assessment. Identify which service, information and access were involved. Do not substitute a platform-wide claimed quantity for a measured loss at one customer.

CASE B

B

Consultancy files advertised with ransom language

Evidence card B04 | 5 Apr 2026 | spear.cx | Technology services

Criminal claim; unverified

CLAIM	A seller alleged website disruption and advertised application source and a database described as 40,081 rows. The offer included a payment deadline and ransom language. [S1]
CHRONOLOGY	The post is dated 5 April. That publication date does not establish when access or extraction allegedly occurred.
ESTABLISHED	The held text combines a consultancy-related file offer with extortion language. The row quantity is not a verified employee, customer or affected-person total.
ALTERNATIVE	Older site backups or a smaller website dataset could be described as a broader corporate event. The text alone cannot resolve that possibility.
LIMIT	Website disruption, current code, usable secrets and customer consequences are unestablished. No ransomware family is attributed from the post's wording.
RESPONSE	Review relevant website integrity, backup access and application changes. Assess exposed secrets against owned evidence before rotating them or attributing an incident to a customer.

Bottom line

Review relevant website integrity, backup access and application changes. Assess exposed secrets against owned evidence before rotating them or attributing an incident to a customer.

CASE C

C

A bank-related administration-portal offer

Evidence card B03 | 6 Mar 2026 | breachforums.as | Banking

Criminal claim; unverified

CLAIM	A forum author offered administration-portal users, endpoints and API keys to a bidder. The asserted role concerns a Chilean bank. [S1]
CHRONOLOGY	The offer is dated 6 March. A separate reply calls it a scam. Neither the offer nor the accusation establishes access validity.
ESTABLISHED	

The retained conversation contains an access advertisement and a credibility dispute. It does not establish current account control or a completed transaction.

ALTERNATIVE	The author could be recycling identifiers, bluffing about privileges or making a fraudulent offer. The dispute remains a forum participant's assessment.
LIMIT	Valid credentials, usable keys, a successful institutional intrusion and customer consequences are not established. A bank-related label is not proof that the underlying banking infrastructure was accessed.
RESPONSE	Validate relevant privileged accounts, API activity and session changes through the bank's controlled incident process. Revoke access when the owned evidence warrants it.

Bottom line

Validate relevant privileged accounts, API activity and session changes through the bank's controlled incident process. Revoke access when the owned evidence warrants it.

Cards B04 and B03 support Cases B and C, respectively. Their distinct claims and limits remain separate.

Evidence card B04 — 5 Apr 2026

Withheld | spear.cx | Forum | ['EN']

ORIGINAL
The ransom price will double in 48 hours.

TRANSLATION
The ransom price will double in 48 hours.

Held
The retained post contains the quoted advertisement or release claim.

Not established
The advertised data or access was genuine, current, complete or usable. The post date is the intrusion or collection date.

Evidence card B03 — 6 Mar 2026

Withheld | breachforums.as | Forum | ['EN']

ORIGINAL
I have endpoints and API keys.

TRANSLATION
I have endpoints and API keys.

Held
The retained post contains the quoted advertisement or release claim.

Not established
The advertised data or access was genuine, current, complete or usable. The post date is the intrusion or collection date.

D

CASE D

An education-administration release claim (B06, B07)

Education

Criminal claim; unverified

CLAIM	Spanish posts asserted information on 3,046,248 students and guardians. A later version said the material was not for sale and no ransom was being charged. [S1]

CHRONOLOGY	Closely related posts are dated 4 and 5 October. They use the same claimed population and similar descriptions, which supports one claimed dataset dossier rather than two confirmed incidents.
ESTABLISHED	The text describes students or guardians and asserts extraction. This report establishes that the authors made that assertion, not that the claimed extraction occurred.
ALTERNATIVE	The posts could repackage older information, repeat copied advertising or present publicly obtainable material as intrusion-derived information. The source wording does not decide among those possibilities.
LIMIT	Authenticity, completeness, extraction date, unique-person count and successful access to the service are not established. A claimed record total is not an independently counted affected population.
RESPONSE	Review relevant education-account activity and bulk exports. If exposure is internally validated, prepare a support route that addresses guardian and student impersonation concerns.

Bottom line

Review relevant education-account activity and bulk exports. If exposure is internally validated, prepare a support route that addresses guardian and student impersonation concerns.

Evidence card B06 — 5 Oct 2026

Withheld | updap.com | Forum | ['ES']

ORIGINAL

extraído información de 3,046,248 estudiantes y tutores.

TRANSLATION

extracted information on 3,046,248 students and guardians.

Held
The retained post contains the quoted advertisement or release claim.

Not established
The advertised data or access was genuine, current, complete or usable. The post date is the intrusion or collection date.

Evidence card B07 — 4 Oct 2026

Withheld | updap.com | Forum | ['ES']

ORIGINAL

extraido informacion de 3,046,248 estudiantes y tutores.

TRANSLATION

extracted information on 3,046,248 students and guardians.

Held
The retained post contains the quoted advertisement or release claim.

Not established
The advertised data or access was genuine, current, complete or usable. The post date is the intrusion or collection date.

CASE E

E

A school-network offer spanning earlier years

Evidence card B08 | 12 Nov 2026 | bf.st | Education

Criminal claim; unverified

CLAIM	A 12 November post advertises a dataset associated with five schools and dated 2010–2026. It claims 107,781 rows and 23,240 unique individuals. [S1]
CHRONOLOGY	The post belongs to the closing fortnight. Its stated historical span prevents treating every advertised record as a new 2026 acquisition.
ESTABLISHED	The author distinguishes yearly rows from a claimed unique-person quantity. Both numbers remain seller assertions and are not added together.
ALTERNATIVE	A historical directory or reused dataset could have been repackaged as a new extraction. The asserted self-extraction is not independently established.
LIMIT	Authenticity, uniqueness, extraction mechanism and a fresh intrusion remain unverified. The offer does not prove a separate incident at every school it references.
RESPONSE	Review archival-data access and bulk-export activity. Verify provenance before treating the advertisement as a current security incident or identifying affected people.

Bottom line

Review archival-data access and bulk-export activity. Verify provenance before treating the advertisement as a current security incident or identifying affected people.

CASE F

F

A multi-provider healthcare release claim

Evidence card B05 | 29 Oct 2026 | darkforums.su | Healthcare

Criminal claim; unverified

CLAIM	A 29 October forum post asserts a free release of records attributed to several healthcare organisations. It refers to 2026 material. [S1]
ESTABLISHED	The held text contains medical target roles and release language. The naming list is not a set of confirmed institutional incidents.
ALTERNATIVE	The post could combine older health information or publicly available material. Its narrative does not independently establish the information's origin or the author's identity.

LIMIT	Authenticity, completeness, current access and separate incidents at the referenced providers remain unestablished. The poster's date label does not independently date the records.
RESPONSE	Validate matching records through controlled internal channels. Review relevant patient-data exports and prepare targeted support if the organisation's evidence establishes an exposure.

Bottom line

Validate matching records through controlled internal channels. Review relevant patient-data exports and prepare targeted support if the organisation's evidence establishes an exposure.

No connection is established between this claim and the hospital incidents discussed in Chapter 5. A shared health-sector role is not enough to join events. Each claim needs its own provenance, chronology and consequence assessment.

Cards B08 and B05 support Cases E and F, respectively. The paired display does not establish a shared event.

Evidence card B08 — 12 Nov 2026

Withheld | bf.st | Forum | ['EN']

ORIGINAL

I am selling a database from a network of 5 schools in Chile

TRANSLATION

I am selling a database from a network of 5 schools in Chile

Held
The retained post contains the quoted advertisement or release claim.

Not established
The advertised data or access was genuine, current, complete or usable. The post date is the intrusion or collection date.

Evidence card B05 — 29 Oct 2026

Withheld | darkforums.su | Forum | ['EN']

ORIGINAL

full data free

TRANSLATION

full data free

Held
The retained post contains the quoted advertisement or release claim.

Not established
The advertised data or access was genuine, current, complete or usable. The post date is the intrusion or collection date.

4.5 Other specific offers and recent assertions

The additional cards preserve claims that deserve attention without overstating their evidentiary status. They are not counted as further confirmed intrusions.

Card	Posted	Role	Held assertion and boundary
B11	2 February	Property-management platform	Advertises 724,000 user records; provenance, freshness and scope unverified
B12	14 January	Public-records service	Advertises 9,200,000 lines; collection date and a new 2026 intrusion unestablished
B09	20 November	Education organisation	Claims data and photographs involving minors; authenticity and a connection to other education claims unestablished
B10	22 November	Electoral records	Claims material concerning six million voters; public availability, age and a new system intrusion unresolved

Source: held post material [S1]. The quantities belong to the authors' claims. A record, line, voter reference and unique affected person are not interchangeable units.

Evidence card B11 — 2 Feb 2026

Withheld | breachforums.bf | Forum | ['EN']

ORIGINAL
724,000 Chilean user records

TRANSLATION
724,000 Chilean user records

Held
The retained post contains the quoted advertisement or release claim.

Not established
The advertised data or access was genuine, current, complete or usable. The post date is the intrusion or collection date.

Evidence card B12 — 14 Jan 2026

Withheld | breachforums.bf | Forum | ['EN']

ORIGINAL
total lines 9 200 000

TRANSLATION
total lines 9 200 000

Held
The retained post contains the quoted advertisement or release claim.

Not established
The advertised data or access was genuine, current, complete or usable. The post date is the intrusion or collection date.

Evidence card B09 20 Nov 2026

Withheld darkforums.su Forum ['EN']

ORIGINAL

faces and names of minors

TRANSLATION

faces and names of minors

Held
The retained post contains the quoted advertisement or release claim.

Not established
The advertised data or access was genuine, current, complete or usable. The post date is the intrusion or collection date.

Evidence card B10 22 Nov 2026

Withheld darkforums.su Forum ['EN']

ORIGINAL

have electoral data for 6 million voters

TRANSLATION

have electoral data for 6 million voters

Held
The retained post contains the quoted advertisement or release claim.

Not established
The advertised data or access was genuine, current, complete or usable. The post date is the intrusion or collection date. A current-election breach. Whether the underlying electoral data was already public.

The 20 November education claim is separate from the school-network offer and the education-administration dossier. The report establishes no shared dataset or operator. Sensitive subject matter justifies careful validation and support, not an inference that related institutions suffered one campaign.

The 22 November electoral-data assertion requires particular restraint. The source does not establish whether the information was already public, when it was obtained or how complete it is. It establishes no current election-system intrusion, political motive or effect on an election.

A 23 March forum claim advertises 10,000 website records attributed to a university. The description mentions names and user codes. Authenticity, currentness, nonpublic provenance and usable account access remain unestablished. The claimed rows are not a confirmed affected-person count. [S1]

A separate March university claim advertises 70,000 site records. The corresponding relay describes student information and photographs. The original assertion and its relay do not establish independent corroboration or another intrusion. Data authenticity and currentness remain unresolved. [S1]

These university claims retain their separate target and dataset assertions. No shared intrusion, common underlying files or verified common operator is established.

A separate public-sector offer describes a transparency-related dataset. Public availability and collection date remain unresolved. That boundary prevents turning a large advertised volume into proof that nonpublic government information was stolen. [S1]

4.6 What changes a defender's decision

For access offers, check account status, permissions and activity. For files, establish provenance and sensitivity through the organisation's controlled channels. For supplier claims, request an assessment tied to the organisation's own service rather than a global customer list.

The completion evidence is a dated disposition with an owner and rationale. Record which proposition was established, contradicted or left unresolved. A reset or customer warning should follow that assessment and the organisation's incident procedure, not the advertisement's pressure language.

KEY TAKEAWAYS

01

The held posts establish claims and offers, not verified possession, new intrusions or completed sales.

02

Preserve the distinct units, dates and alternatives within each dossier.

03

Validate relevant owned evidence before choosing account, supplier, privacy or customer actions.

CHAPTER 05

Incidents, claims and response decisions by sector

THIS CHAPTER ANSWERS

Which public accounts establish an operational problem, and what should each sector verify first?

Separate

access, data publication and service availability

5.1 Read the case before counting the incident 38
5.2 May public-service and communications claims 39
5.3 Health information and clinical continuity 40
5.4 Energy operations require a distinct impact assessment 42
5.5 A public-service incident with competing technical accounts 43
5.6 Recent activity: 8–22 November 2026 43
5.7 Financial warnings require their own case population 45
5.8 What the sector evidence supports 45
5.9 Retail recovery and the limits of an initial statement 46
5.10 Supplier, network and administrative-access accounts 47
5.11 Legal services and content-publishing accounts 50
5.12 Further source context without an additional incident count 52
5.13 Important exclusions and non-incident notices 52

CHAPTER 05

Incidents, claims and response decisions by sector

IN SHORT

Chile's public accounts distinguish unauthorised use of valid accounts, historical data presented as new, hospital information exposure and interrupted services. Recent notices add a hospital outage, continued energy disruption and disputed accounts of a public-service incident. These are different evidence states. A regulator's warning is not another confirmed intrusion. Begin with the affected function and the source's actual finding, then assign the appropriate identity, privacy, fraud or continuity response.

5.1 Read the case before counting the incident

The cases below preserve the distinction between a primary authority statement and press reporting of an organisation's account. Names remain role-based where the public naming conditions are not established. A generic role does not mean that the underlying notice lacks a specific subject.

A case is a dossier explaining a decision. It is not automatically one confirmed intrusion. The May access notices concern several reported claims. The historical-data correction concerns an alert's interpretation. The hospital notices describe different reported episodes. None should be added mechanically to criminal listings.

The table sets out the evidence state and the first responsible function.

Evidence state	Supported conclusion	First owner	Initial question
Authority identifies valid-account access	Affected accounts require investigation	Identity and response	Which accounts and permissions were used?
Authority identifies historical material	New publication need not mean new intrusion	Intelligence and privacy	Does the evidence match a known event?
Press reports a criminal complaint	The reported complaint describes an incident	Response and legal	What does the official account actually establish?
Organisation account reports disruption	The named service function was affected	Service owner	Which essential tasks still work?
Regulator warns of suspected fraud	Customers need a trusted verification route	Fraud and customer support	What request or payment needs validation?
Actor publishes an extortion listing	A criminal assertion exists	Response and communications	Is there independent evidence of access or impact?

5.2 May public-service and communications claims

CASE G

G

Valid-account access within a broader leak narrative

Public administration

Source account; limits retained

INITIAL REPORT	On 1 May, ANCI said it was investigating reported data publications concerning communications operators and public services. Authenticity and scope had not yet been corroborated. [S6]
UPDATED FINDING	On 8 May, ANCI identified unauthorised access using valid user credentials. It considered earlier leaks or information-stealing malware probable sources and reported no evidence of infrastructure attacks. [S7]
BOUNDARY	The update does not establish access to every organisation mentioned in the earlier claims. It also does not support treating the state as one affected network.
ALTERNATIVE	A criminal advertisement can combine an actual account event with historical or unrelated material. Each asserted source and access path requires its own evidence.
RESPONSE	Validate matching accounts, review current privileges and sessions, and scope accessible records. Use targeted containment when the evidence warrants it, rather than treating every advertised credential as a current institutional intrusion.

Bottom line

Validate matching accounts, review current privileges and sessions, and scope accessible records. Use targeted containment when the evidence warrants it, rather than treating every advertised credential as a current institutional intrusion.

CASE H

H

A new alert about material attributed to an older leak

Identity data

Historical-data assessment

REPORTED CLAIM	A May alert described more than six million Chilean records. That quantity belongs to the alert, not to a verified new-incident population in this report. [S8]

AUTHORITY ASSESSMENT	ANCI's 20 May notice attributed the material to a 2019 social-platform leak rather than a recent intrusion into national infrastructure. [S8]
BOUNDARY	Historical origin does not establish that the data are harmless, current or accurate. It also does not establish a new access event when the material is advertised again.
RESPONSE	Check whether affected accounts were already remediated and whether the information still supports impersonation. Correct the incident chronology while preserving proportionate support for people facing renewed contact.

Bottom line

Check whether affected accounts were already remediated and whether the information still supports impersonation. Correct the incident chronology while preserving proportionate support for people facing renewed contact.

5.3 Health information and clinical continuity

CASE I

September reporting of imaging-record access and publication

Reported complaint; scope uncertain

Healthcare

REPORTED OFFICIAL ACCOUNT	T13 reported that a hospital filed a criminal complaint describing unauthorised access to imaging records and online publication. The account followed an ANCI notification on 20 September. [S33]
SCOPE	The report did not establish the total affected population. The complaint account does not validate a quantity claimed in an earlier extortion publication.
EVIDENCE BOUNDARY	This case rests on press reporting of the complaint. No actor attribution, entry route or final patient total is adopted here.
RESPONSE	Assign clinical data owners to identify the records concerned and assess consequences for patients. Preserve the distinction between the privacy investigation and the availability of clinical systems.

Bottom line

Assign clinical data owners to identify the records concerned and assess consequences for patients. Preserve the distinction between the privacy investigation and the availability of clinical systems.

Imaging information can have a different sensitivity from a contact list. Response teams should establish what the records reveal and who needs support. They should not infer that every patient, every department or every system was affected from a broad hospital reference.

A patient-facing response also needs a trusted contact route. Staff should be able to explain what is known, what remains under review and how a person can report suspicious follow-up contact. Do not use knowledge of a medical detail as sufficient caller authentication.

CASE J

J

November hospital-server disruption with clinical care maintained

Reported service incident

Healthcare

REPORTED EVENT	T13 reported the hospital's statement on 16 November, followed by BioBioChile coverage. The account describes an incident beginning on 14 November, interrupted booking and support channels, maintained clinical care and technical coordination with ANCI. [S56][S34]
BOUNDARY	Patient-data exposure remained unresolved in the cited account. The event is not assigned a ransomware family or linked to the September episode through timing or institutional type.
OPERATIONAL DISTINCTION	Maintained clinical care does not establish that every administrative or patient journey worked normally. Interrupted booking also does not establish that treatment systems were accessed.
RESPONSE	Test scheduling alternatives, prioritise clinically urgent requests and reconcile work accumulated during the outage. Run the data-access assessment separately from the service-restoration decision.

Bottom line

Test scheduling alternatives, prioritise clinically urgent requests and reconcile work accumulated during the outage. Run the data-access assessment separately from the service-restoration decision.

For clinical leaders, a functioning ward is one milestone rather than the whole recovery. Patients may still struggle to arrange appointments, obtain information or confirm a scheduled visit. The service owner should identify those tasks and provide a reliable alternative.

ANCI and CENS announced health-information-system guidance in August. That publication supplies a relevant sector resource. This report does not attribute detailed controls to the guide without relying on its substantive text. [S38]

5.4 Energy operations require a distinct impact assessment

CASE K

K

Prolonged disconnection of a generation facility

Energy

Operator-reported cause

OPERATIONAL RECORD	The electricity coordinator's 27 August record lists a solar facility and battery system disconnected with a cyberattack as the operator-reported cause. Its 9 and 15 November records still list 0% availability. Later press reporting describes continued disconnection. [S53][S54][S86][S35]
BOUNDARY	The report does not establish an actor, entry route or common cause with remote-control problems at other facilities. Continued disconnection does not establish a wider power-supply outage.
OPERATIONAL QUESTION	A facility can be unavailable for dispatch while other generation serves demand. The consequences for that facility and the consequences for the national system require different evidence.
RESPONSE	Verify the affected operating function with the responsible engineer. Document safe recovery, remote-access controls and acceptance by the operating owner before reconnecting a service.

Bottom line

Verify the affected operating function with the responsible engineer. Document safe recovery, remote-access controls and acceptance by the operating owner before reconnecting a service.

The same caution applies to simultaneous reports. Proximity in date can justify investigating a relationship. It does not establish a shared operator, vulnerability or campaign without a concrete connection.

A November parliamentary request asks about knowledge, reporting and response to the electricity incidents. The request does not establish its own answers. It expressly preserves uncertainty about origins, affected systems and links between the events. [S60]

5.5 A public-service incident with competing technical accounts

CASE L

L

An investigation without a settled entry mechanism

Public services

Accounts differ

PRESS ALLEGATIONS	November reporting cited anonymous accounts alleging phishing and persistent malware at a public-service agency. These are attributed allegations, not findings adopted by this report. [S36]
REPORTED OFFICIAL RESPONSES	The organisation said forensic analysis was underway. ANCI told the outlet it was investigating and suspected DDoS. It had not been informed of the alleged malware mechanism and had not imposed fines. [S36]
BOUNDARY	The evidence does not settle the entry mechanism, persistence, data sales or actor identity. A suspected availability event does not establish access to the underlying records.
RESPONSE	Separate availability monitoring from the access investigation. Preserve competing accounts, obtain service-owner evidence and issue updates that identify which proposition has changed.

Bottom line

Separate availability monitoring from the access investigation. Preserve competing accounts, obtain service-owner evidence and issue updates that identify which proposition has changed.

5.6 Recent activity: 8–22 November 2026

The closing fortnight includes new reported events, updates to earlier disruption, fraud warnings and policy developments. The table preserves those types. It is not a count of new intrusions.

Published	Type	Supported development	Defender implication
9 November	Ongoing operational record	The electricity coordinator still lists 0% availability for the affected facility units [S54]	Preserve facility-level consequences and operating acceptance
10 November	Awareness warning	ANCI describes fake error or verification prompts that induce unsafe user actions [S18]	Give staff a trusted support route for unexpected instructions

Published	Type	Supported development	Defender implication
11 November	Incident reporting	Public-service accounts differ on the technical mechanism [S36]	Preserve uncertainty and verify service and access separately
12 November	Response guidance	ANCI distinguishes receiving a message from entering credentials or banking information [S19]	Triage what the person actually did
15 November	Continuing operational observation	The electricity coordinator again records 0% availability for the same facility units [S86]	This extends the existing event, not a new incident
17 November	Reported new event	Hospital authorities describe the 14 November server incident and interrupted booking [S34]	Maintain clinical and administrative fallback routes
17 November	Consultation	CMF proposes changes to bank cyberincident reporting definitions and information [S87]	Retain the proposal's status and track the final instrument
18 November	Ongoing disruption	Reporting says an August energy disconnection continued [S35]	Require an operationally accepted recovery state
18 November	Parliamentary inquiry	An official request asks about hospital continuity and preparedness [S57]	Questions do not establish forensic findings
18 November	Fraud warning	CMF warns about credit-app collection practices and suspected usury [S25]	Route coercive collection reports to trained support and investigations
18 November	Fraud warning	CMF describes advance-fee loan offers and a complaint [S26]	Verify the provider and never treat claimed approval as authentication
18 November	Awareness warning	ANCI addresses unsolicited job offers seeking information, money or recovery codes [S20]	Brief recruitment and customer-facing staff
19 November	Consultation	ANCI opens consultation on proposed MFA requirements [S15][S16]	Review the proposal while preserving its draft status

Published	Type	Supported development	Defender implication
19 November	Security guidance	ANCI addresses AI-assisted attacks without announcing a confirmed national campaign [S17]	Assess behaviour and owned exposure, not an AI label alone
20 November	Legislative development	Cámara reports the data-law postponement bill at promulgation stage [S31][S32]	Confirm enactment and publication before changing the legal deadline

The continuing energy event should not be recounted as a November intrusion. The hospital article's publication date should not replace its reported event date. The CMF complaints describe alleged misconduct and regulatory action, not convictions.

5.7 Financial warnings require their own case population

CMF's June notice concerned thirteen unregulated credit applications. Its November notice concerned three applications. Both describe extortionate collection and suspected usury. Those counts concern applications in notices, not ransomware incidents, borrowers or separate criminal groups. [S28][S25]

Separate advance-fee loan warnings describe requests for payment before loans that were not delivered. The March notice concerns eight entities; the April notice concerns four. The November warning describes another reported offer. These are not added into a unique-victim or financial-loss total. [S42][S43][S26]

5.8 What the sector evidence supports

The strongest common lesson is to keep consequences distinct. Identity misuse calls for account and session validation. Possible record exposure calls for a scoped privacy assessment. Service interruption calls for a usable fallback and business acceptance. Suspected customer fraud calls for a trusted verification route.

These lessons transfer across sectors without establishing a national sector ranking. Public disclosure practices differ, and some incidents do not become public. The number of cases described here is not the frequency of all incidents in health, energy, government or finance.

5.9 Retail recovery and the limits of an initial statement

CASE M

M

A retailer's later update changes the operating picture

Retail

Official disclosure

INITIAL DISCLOSURE	A retailer's 16 September essential disclosure says it learned of an incident on 15 September. Some systems were affected, response and forensic work were activated, and the financial effects remained unresolved. [S51]
LATER UPDATE	Its 6 October statement describes logistics, distribution and store-replenishment delays, as well as digital and wholesale disruption. Stores remained open. The company still had not established the financial impact. [S52]
BOUNDARY	The company statements do not establish a ransomware group or confirmed data theft. The September position should remain dated rather than becoming a permanent assurance about every possible consequence.
RESPONSE	Assess physical stores, digital sales, wholesale orders and replenishment as separate service journeys. Reconcile accumulated orders and stock movements before treating open stores as complete recovery.

Bottom line

Assess physical stores, digital sales, wholesale orders and replenishment as separate service journeys. Reconcile accumulated orders and stock movements before treating open stores as complete recovery.

5.10 Supplier, network and administrative-access accounts

Source context: a mining client's supplier incident

- **Reported company account.** A June report reproduces the mining client's response that the event concerned an external platform supplier rather than its corporate systems. The company said production continuity was unaffected. [S44]
- **Quantity boundary.** The client's preliminary associated-data estimate differed from a larger allegation and a broader attacker claim about the platform. The quantities describe different assertions and scopes.
- **Limit.** The cited response does not establish a separate corporate-network intrusion at the client. A supplier incident can affect client information without becoming an independent intrusion at each client.
- **Response.** Obtain a client-specific supplier assessment, identify the information and access involved, and record production and privacy consequences separately. Do not use the supplier's global claim as the client's measured loss.

This supplier also appears in Case A's source context. The records do not establish the same event or files, so this account is not counted as a separate independent intrusion.

A company's statement that its own systems were unaffected narrows one proposition. It does not automatically resolve the information held elsewhere. The response record should preserve the distinction rather than forcing a single all-clear or all-affected label.

CASE O

A telecommunications investigation with historical activity

Telecommunications

Investigation reported

REPORTED INVESTIGATION	August reporting says PDI and Fiscalía investigated telecommunications-network activity after information from US authorities. The reporting referred to malware and an actor label, with some observed activity dating from 2024. [S45]
ATTRIBUTION BOUNDARY	The actor and state-association descriptions belong to the cited sources. This report does not infer a government connection, a new 2026 entry date or a relationship with infrastructure policy.
SCOPE BOUNDARY	The report establishes no confirmed end-user data population. An investigation into network activity is not a count of every subscriber or device using the service.

RESPONSE	Preserve the source's observed period, validate relevant network and administrator evidence, and assess supplier or customer consequences separately. Keep historical activity distinct from the date the investigation became public.

Bottom line

Preserve the source's observed period, validate relevant network and administrator evidence, and assess supplier or customer consequences separately. Keep historical activity distinct from the date the investigation became public.

P

CASE P

Unauthorised messages and a short public-service interruption

Public services

Source account; limits retained

REPORTED AGENCY ACCOUNT	An August report quotes a public-service agency saying that an unauthorised incident temporarily disrupted services from 05:00 to 09:00. The report also describes mass unsolicited messages. [S46]
BOUNDARY	Those facts do not establish access to every agency record, a named operator or a political motive. Service restoration does not establish the scope of any data access.
RESPONSE	Review the affected messaging authority and relevant account permissions. Confirm that recipients can recognise legitimate follow-up messages and that the restored public-service task works.

Bottom line

Review the affected messaging authority and relevant account permissions. Confirm that recipients can recognise legitimate follow-up messages and that the restored public-service task works.

The message's content is unnecessary to the defensive finding. The issue is unauthorised use of a trusted communication channel and the reported service interruption. The report does not reproduce political imagery or adopt an interpretation of its ideology.

Q

CASE Q

Possible health-information extraction with care maintained

Healthcare

Possible extraction

PRIMARY STATEMENT	A health-service statement describes detection on 4 May of possible unauthorised information extraction following an external alert. It says systems and care were unaffected at that time. [S63]

UNRESOLVED MECHANISM	The origin remained under analysis, and credential misuse had not been excluded. Neither possibility should become a settled access mechanism.
BOUNDARY	The statement concerns possible extraction, not a verified final volume or a conclusion about every record. Its account of unaffected systems and care remains tied to that date.
RESPONSE	Preserve the external alert, identify relevant data owners and assess account use. Maintain care while the information-access question receives its own scoped determination.

Bottom line

Preserve the external alert, identify relevant data owners and assess account use. Maintain care while the information-access question receives its own scoped determination.

R

CASE R

A multinational incident with a reported Chilean consequence

Manufacturing

Reported forensic account

REPORTED EVENT	August reporting describes a March ransomware incident at a multinational manufacturing group. It says storage at the Chilean operation was also encrypted. [S64]
ATTRIBUTION BOUNDARY	The article attributes its actor assessment to a reported forensic investigation. This report does not independently adopt that attribution or a claimed data volume.
GEOGRAPHIC BOUNDARY	The chronology began outside Chile. The reported local consequence does not make the entire multinational incident a wholly domestic event.
RESPONSE	Map shared identity, storage and support dependencies across group entities. Test how the Chilean operation can restore its necessary service when a group-controlled resource is unavailable.

Bottom line

Map shared identity, storage and support dependencies across group entities. Test how the Chilean operation can restore its necessary service when a group-controlled resource is unavailable.

CASE S

S

An administrative-account event at a regional public body

Regional administration

Local reporting

REPORTED ACCOUNT	March reporting describes a 1 March event involving an administrative account, a password change and access to institutional services. It also reports a criminal complaint. [S65]
BOUNDARY	This account relies on the cited regional reporting. A source-address location does not establish the operator's identity.
IMPACT BOUNDARY	A small reported data quantity would not by itself establish low consequence. Permissions, data sensitivity and continuing access require separate assessment.
RESPONSE	Review the account's privileges, sessions and recovery configuration. Confirm which institutional services were reachable and preserve the chronology supporting the complaint.

Bottom line

Review the account's privileges, sessions and recovery configuration. Confirm which institutional services were reachable and preserve the chronology supporting the complaint.

5.11 Legal services and content-publishing accounts

CASE T

T

A legal-services firm's ransomware complaint and recovery account

Legal services

Reported complaint

REPORTED EVENT	A May article dates an extortion message to 22 April. It describes an internal report and criminal complaint concerning encrypted or deleted information and unavailable systems. The firm confirmed a complaint and recovery work with outside specialists. [S70]
OPERATIONAL ACCOUNT	The firm said normal legal operations were continuing. That later statement has a different scope from the earlier reported system effects and should remain tied to its date.

ATTRIBUTION BOUNDARY	The threats used the Akira identity. This report treats that as the reported claimant name, without independently determining operator identity, origin or a link to another case.
RESPONSE	Test the restoration of matter-related records, essential communications and access to working documents. Preserve privileged access and client-information assessments separately from a statement that professional services continue.

Bottom line

Test the restoration of matter-related records, essential communications and access to working documents. Preserve privileged access and client-information assessments separately from a statement that professional services continue.

U

CASE U

Publication-account exposure with core services excluded

Public services

Official account reported

REPORTED STATEMENT	Two May reports carry the same institutional response to an account alert. The statement limits the issue to accounts used to publish news content and says core operational services were unaffected. [S83][S84]
RESPONSE DESCRIBED	The institution reported additional authentication protection and legal action. The alert and subsequent statement belong to one account-related case, not two incidents because two outlets reported it.
BOUNDARY	The quoted statement is not an independent forensic assessment by each outlet. It does not support extending the event to all institutional systems or inferring the operator's identity.
RESPONSE	Review publishing permissions, delegated access, account recovery and session state. Confirm the integrity of public communications while keeping the core-service assessment separate.

Bottom line

Review publishing permissions, delegated access, account recovery and session state. Confirm the integrity of public communications while keeping the core-service assessment separate.

5.12 Further source context without an additional incident count

January energy-distributor reporting describes an acknowledged internal-storage access event, authority notification and reinforced monitoring. The company said customer personal data, access passwords and operations were unaffected. Separate criminal data-theft claims remained unresolved. The January disclosure does not establish a January intrusion date. [S74][S75]

A May response from a health-sector organisation describes a contained institutional-system anomaly and says there was no interruption to healthcare services or extraction of personal information. That is the institution's dated position. It should be read with ANCI's later account and not treated as proof that every broader claim was false. [S77][S7]

Instructure, a global education-platform vendor, also confirms April and May security events and subsequent mitigation. Its account does not identify Chilean customers or establish Chile-specific information access. No local institution or additional Chilean intrusion is inferred from that global statement. [S76]

5.13 Important exclusions and non-incident notices

A September manufacturing case study says the described event occurred on Christmas Eve without establishing the year. Its publication date is not sufficient to classify the event as a new 2026 incident. It remains outside dated 2026 incident counts. [S49]

An August report of ANCI's preventive supply-chain response also requires restraint. The agency described potential exposure and notifications to potentially affected institutions. It explicitly distinguished that position from a confirmed significant-impact incident at the stated time. [S48]

The health-insurer extortion relay describes an actor listing without company or authority confirmation. Its claimed scope is not adopted as a verified health incident. The listing population in Chapter 7 remains separate from the reported organisational cases above. [S37]

An enforcement announcement is another distinct population. September reporting describes prosecutors and PDI pursuing alleged illicit access, credential use, data aggregation and sale. Investigation and device examination continued. An accusation is not a conviction or proof that every earlier public claim belonged to that case. [S47]

KEY TAKEAWAYS

01

Distinguish actual account access, historical republication, possible data exposure and service interruption.

02

Recent activity includes guidance and continuing disruption as well as reported new events.

03

Give identity, privacy, fraud and operational recovery separate owners and completion evidence.

CHAPTER 06

Hacktivism, DDoS and service availability

06

THIS CHAPTER ANSWERS

What distinguishes an availability claim from established access or operational harm?

3

separate questions: service state, data access and attribution

6.1 A claim needs more than a failed page check 54

6.2 Timeline of public accounts and response context 54

6.3 Claim versus official account 55

6.4 Operational consequences require their own evidence 55

6.5 Prepare a bounded public statement 56

6.6 Completion evidence for availability readiness 56

CHAPTER 06

Hacktivism, DDoS and service availability

IN SHORT

An availability claim does not establish access to records, a persistent foothold or a named operator. The recent public-service case illustrates competing technical accounts rather than a settled national campaign. Health and energy reporting also shows that operational consequences differ by service. Verify the essential user task, preserve the access investigation and prepare a statement that describes only the impact currently supported.

6.1 A claim needs more than a failed page check

The November public-service report is a useful example. Anonymous accounts alleged phishing and persistent malware. ANCI told the outlet that it was investigating and suspected DDoS, while the organisation said forensic analysis continued. The source does not settle the technical mechanism. [S36]

6.2 Timeline of public accounts and response context

The timeline distinguishes source statements and reported developments. It does not connect the rows into one campaign.

1 May 2026	**ANCI**	Investigating reported data publications; authenticity and scope unresolved [S6]
8 May 2026	**ANCI**	Identifies valid-account access and distinguishes it from infrastructure attacks [S7]
4 Jul 2026	**Radio reporting**	Relays an unconfirmed claim concerning a public-service body; service impact and mechanism unestablished [S82]
27 Aug 2026	**Electricity coordinator**	Operational record lists facility disconnection with an operator-reported cyberattack cause; no actor established [S53]
9 Nov 2026	**Electricity coordinator**	Dated operational record still lists 0% availability for the affected units [S54]
11 Nov 2026	**Press reporting**	Public-service investigation includes competing accounts of phishing, malware and suspected DDoS [S36]
15 Nov 2026	**Electricity coordinator**	Updated record again lists 0% availability for the same units; existing event [S86]

17 Nov 2026 **Press reporting**
Hospital authorities describe interrupted booking and maintained clinical care [S34]

18 Nov 2026 **Press reporting**
Reports continued disconnection of the energy facility [S35]

The May notices concern access claims rather than proof of a DDoS event. The energy and hospital rows concern different operational functions. Their inclusion shows why the evidence type and consequence must remain visible in a response chronology.

6.3 Claim versus official account

The following panel separates the disputed public-service assertions from the supported reporting. It does not reproduce an actor's direct quotation.

Question	Reported allegation	Reported official account	Assessment
Entry route	Anonymous sources alleged phishing [S36]	Forensic analysis was underway [S36]	No settled entry route is adopted
Persistent access	Anonymous sources alleged malware persistence [S36]	ANCI had not been informed of that alleged mechanism [S36]	Persistence remains unestablished
Availability cause	The account contains competing explanations [S36]	ANCI said it suspected DDoS and was investigating [S36]	Suspicion is not a final technical finding
Data sales	Speculation can accompany a disruption	The cited account establishes no verified sale	Do not infer possession, transfer or commercial delivery
Regulatory action	No verified sanction is established in the cited allegations	ANCI said it had not imposed fines [S36]	Preserve the agency's stated position at that date

6.4 Operational consequences require their own evidence

The hospital report distinguishes interrupted booking from maintained clinical care. That supports separate administrative and clinical continuity tests. It does not establish that all patient-facing processes were unaffected or that data confidentiality was preserved. [S34]

The energy account describes a facility and battery system remaining disconnected. It does not establish a national electricity outage. Its response needs operational acceptance rather than a generic instruction to reconnect equipment when a network problem appears resolved. [S35]

6.5 Prepare a bounded public statement

A useful first statement identifies the affected function, the current alternative and the next update time. It can acknowledge an investigation without selecting an unverified entry mechanism. It should separate a confirmed service limitation from a possible privacy consequence.

6.6 Completion evidence for availability readiness

Owner	Exercise	Evidence of completion
Service owner	Complete the essential customer or citizen task during degradation	Witnessed task result and usable fallback instructions
Infrastructure	Activate the agreed availability-response route	Dated escalation and mitigation exercise record
Identity and response	Assess whether disruption coincides with unauthorised account use	Separate access determination with remaining uncertainty
Operations	Accept the relevant physical or clinical service state	Authorised operational sign-off and exception list
Communications	Issue an evidence-bounded update	Approved statement naming the function and next update
Legal	Review reporting triggers against established facts	Recorded decision and preserved awareness chronology

KEY TAKEAWAYS

01

A published availability claim does not establish persistent access, data sales or actor identity.

02

Test the essential service and the access question separately.

03

Require service-owner evidence and a bounded public update before declaring recovery.

CHAPTER 07

Threat actors and supported relationships

07

THIS CHAPTER ANSWERS

Which actor-related observations are supported, and what do the listing counts actually measure?

41

Chilean ransomware listings in the observation window

7.1 Listing labels describe a publication population 58
7.2 Regional comparators provide context, not a safety ranking 60
7.3 Publication timing is not intrusion timing 61
7.4 Supported relationships, with no inferred common operator 63
7.5 Investigations and enforcement do not complete attribution 65
7.6 Prepare for capabilities while preserving actor uncertainty 65
7.7 A global vulnerability example with no Chile exploitation claim 65

CHAPTER 07

Threat actors and supported relationships

IN SHORT

Ransompedia records 41 Chilean listings across 13 claimant labels. Qilin and The Gentlemen account for 26, or 63.4%. These are criminal publications, not confirmed intrusions or unique legal organisations. Public reporting also describes investigations and enforcement without establishing a common operator across cases. Prepare for extortion and identity misuse, and keep each actor label attached to the specific source that supports it.

7.1 Listing labels describe a publication population

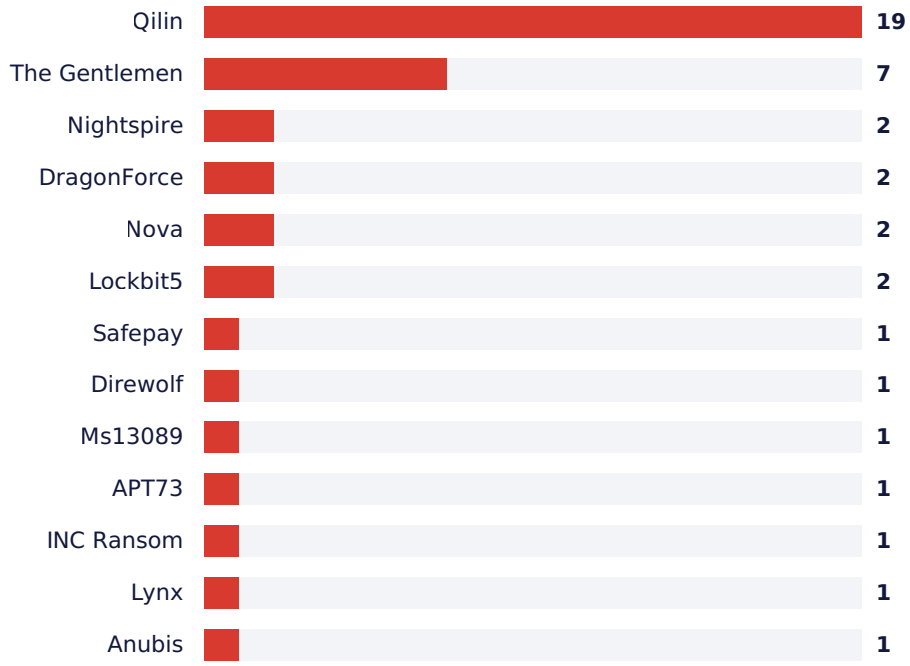
The retained Chilean population contains 41 dated listing rows and 39 distinct organisation-name strings. Neither measure establishes an independently validated count of legal organisations. Repeated names, group structures and the underlying criminal assertions require separate assessment. [S2]

A ransomware label identifies the name used in the listing source. It does not prove that every row used the same affiliate, access route or malware. A listing also does not establish encryption, copied information, payment or the amount of harm.

The leading labels are Qilin and The Gentlemen. Their combined share shows concentration within this retained population. It does not measure their share of every incident in Chile or the probability that a reader will face either group. [S2]

The following chart and table preserve the distinction between leading labels and the remaining listing population.

Qilin and The Gentlemen account for 26 of 41 Chilean listings



Source: Brandefense Ransompedia, 1 January–22 November 2026; November partial [S2]. Listing rows remain criminal assertions, not confirmed intrusions or a national risk ranking.

Label	Listings	Share	Meaning
Qilin	19	46.3%	Publications carrying this claimant label
The Gentlemen	7	17.1%	Publications carrying this claimant label
Other 11 labels	15	36.6%	Remaining labels combined
Total	41	100.0%	Chilean listing rows in the observation window

Qilin

Extortion listing label | No state attribution assessed

IN CHILE, 2026

2026
19 Chile-labelled listings in the report window

CLAIMED TARGETS

Only the retained country-labelled listing population; victim names withheld

SEEN IN PUBLIC REPORTING

[S2] Ransompedia records 19 Chile-labelled listings under this label.

OUR ASSESSMENT

A listing is an assertion. It does not establish encryption, data removal, a completed payment or a common operator across all entries.

CONFIDENCE

High for the retained label count; underlying incident assertions remain unverified

The Gentlemen

Extortion listing label | No state attribution assessed

IN CHILE, 2026

2026

7 Chile-labelled listings in the report window

CLAIMED TARGETS

Only the retained country-labelled listing population; victim names withheld

SEEN IN PUBLIC REPORTING

[S2] Ransompedia records 7 Chile-labelled listings under this label.

OUR ASSESSMENT

Use a relevant listing to validate owned data and service continuity. The label does not identify an individual operator or establish a completed incident.

CONFIDENCE

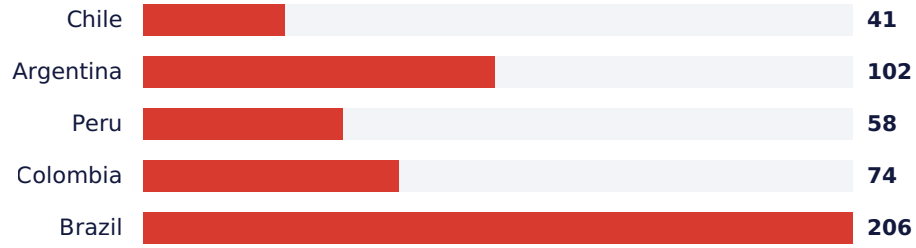
High for the retained label count; underlying incident assertions remain unverified

7.2 Regional comparators provide context, not a safety ranking

Argentina, Peru, Colombia and Brazil provide a regional comparison for the same requested window. Their listing totals are shown beside Chile's, with the same caveat about criminal assertions. Economic scale, organisation populations and disclosure behaviour are not controlled here. [S2]

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

Chile has 41 retained listings against 58–206 across the four selected peers



Source: Brandefense Ransompedia, 1 January–22 November 2026; November partial [S2]. Listing rows remain criminal assertions, not confirmed intrusions or a national risk ranking.

Country	Listing rows	Interpretation
Chile	41	Nationally associated listing population
Argentina	102	Regional comparison, without population adjustment
Peru	58	Regional comparison, without population adjustment
Colombia	74	Regional comparison, without population adjustment
Brazil	206	Regional comparison, without population adjustment

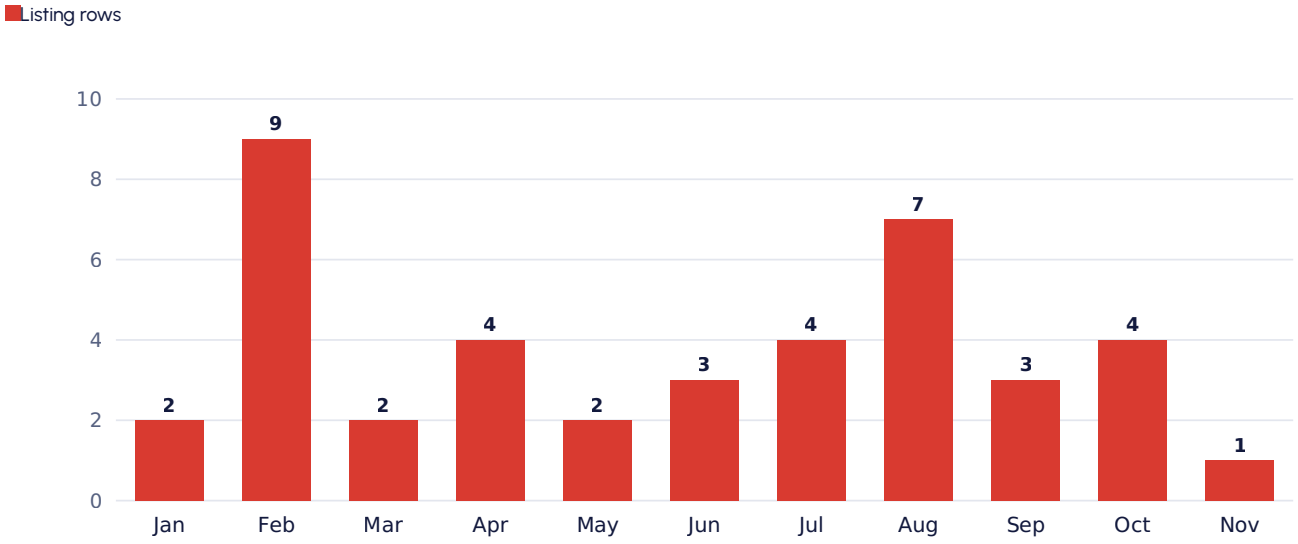
All four peers have more retained listing rows than Chile. That does not establish that Chilean organisations are safer or that their controls are more effective. The table contains no denominator for comparable organisations and no independently verified success rate.

The prior full-year Chilean total is 21 for 2025. The 41 current-window rows exceed that earlier annual total. This compares a partial year with a full year, so it is not a matched-period growth rate. [S2]

7.3 Publication timing is not intrusion timing

The monthly listing series describes when the records were dated. It does not establish when initial access occurred or when the organisation discovered an event. November is a partial month at the report's cut-off. [S2]

Listing publication varies by month, with no retained row in the closing fortnight



Source: Brandefense Ransompedia, 1 January–22 November 2026; November partial [S2]. Listing rows remain criminal assertions, not confirmed intrusions or a national risk ranking.

Month	Chilean listings	Month	Chilean listings
January	2	July	4
February	9	August	7
March	2	September	3
April	4	October	4
May	2	November to cut-off	1
June	3	Total	41

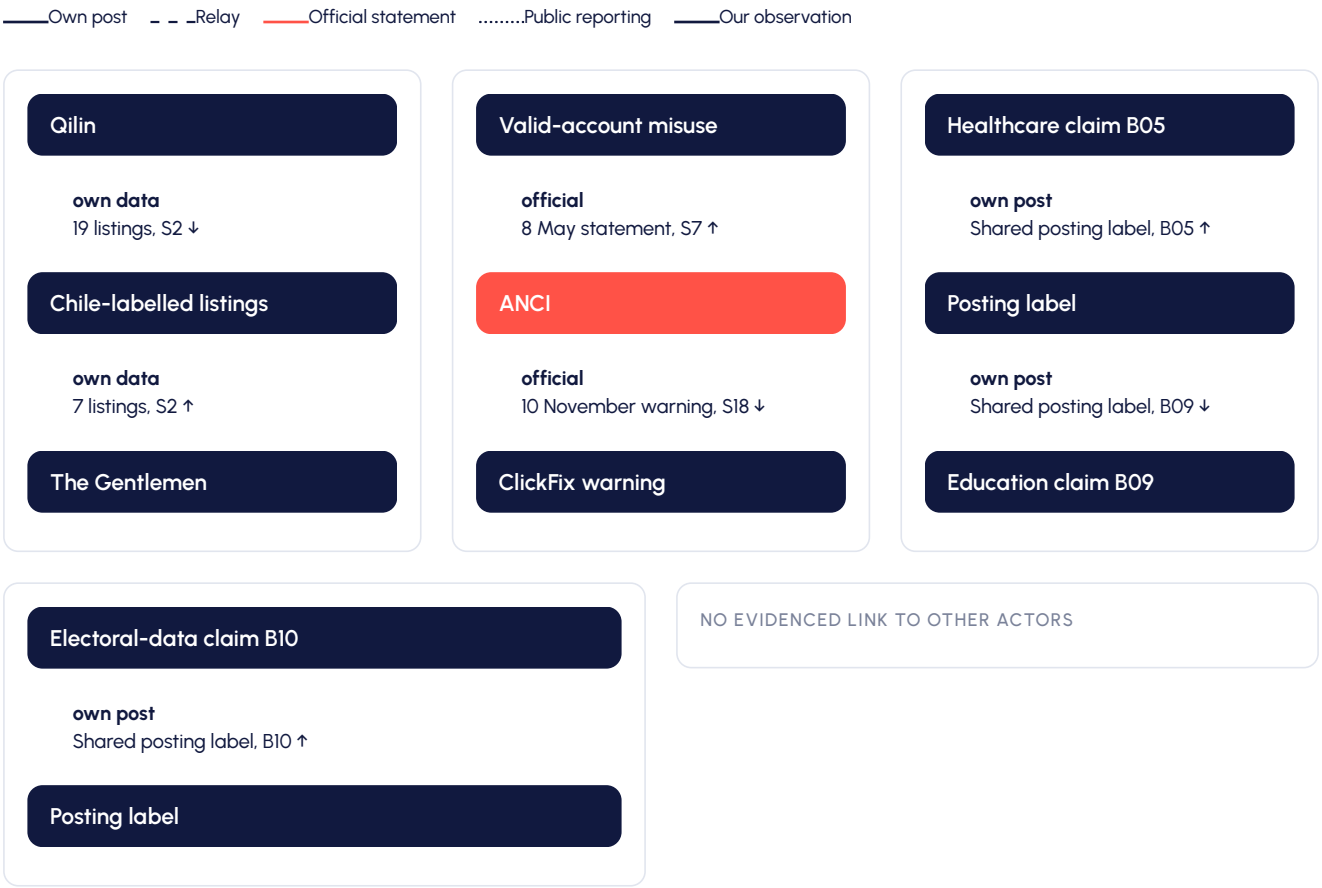
The only November row is dated 2 November and carries the Qilin label. No retained listing row falls in 8–22 November. That is a statement about this source population, not evidence that Chile experienced no ransomware activity during the closing fortnight. [S2]

A public relay also describes an unverified Qilin claim concerning a health insurer. Company or authority confirmation and technical scope were absent from that account. A relay does not become independent confirmation of the underlying criminal assertion. [S37]

Public relays also describe a September finance-company listing and an April maritime-company claim. Those publications do not establish company-confirmed incidents or verified operational consequences. Their dates describe listing or claim visibility, not independently established intrusion dates. [S72][S73]

7.4 Supported relationships, with no inferred common operator

The relationship map connects a source to the proposition it supports. It does not connect separate actors through a shared national label, a similar technique or a common political theme.



The source relationships can also be read as a table.

Source	Supported relationship	What it does not establish
Ransompedia	Qilin and The Gentlemen labels occur in the Chilean listing population [S2]	Common operator across every listing or confirmed intrusion
ANCI May update	Valid-account access was identified in the investigated claims [S7]	A named actor or access to the whole state
Telecom investigation reporting	Authorities investigated network activity with information from US authorities [S45]	This report's own state attribution or end-user data total
September enforcement reporting	Prosecutors and PDI pursued alleged illicit access and data trading [S47]	A conviction or linkage to every earlier advertisement
Public-service reporting	Technical accounts differed while investigation continued [S36]	A settled entry route, persistent access or verified sale

Ransompedia relationships are own-data relationships in this report. Official statements and press accounts remain distinct source types. Their proximity in the diagram does not imply that they agree on an actor or describe the same event.

The health-release post B05, education/photos post B09 and electoral-data post B10 share the same displayed posting label in the held material. This supports a publication association, not a finding that one verified person operated the label. [S1]

Cross-sector posting label

Alias withheld

Source-level association | No political or state attribution assessed

IN CHILE, 2026

2026-10-29
B05 retained claim

2026-11-20
B09 retained claim

2026-11-22
B10 retained claim

CLAIMED TARGETS

Healthcare, education and electoral-data roles in separate unverified advertisements

SEEN IN PUBLIC REPORTING

[S1] The same posting label appears on B05, B09 and B10.

OUR ASSESSMENT

This supports an association between retained advertisements. It does not establish one human operator, a shared intrusion, identical files or common affected infrastructure.

CONFIDENCE
High for the observed posting-label association; underlying data and access claims remain unverified

The association does not establish common data, a shared intrusion, common infrastructure or a political motive. Each post's authenticity, provenance and asserted consequences remain separate. The label is withheld, and no contact route is reproduced.

7.5 Investigations and enforcement do not complete attribution

August telecommunications reporting refers to malware and an actor label while describing a PDI and Fiscalía investigation. Some observed activity dates from 2024. The public reporting date should not become a new-entry date, and the investigation's attribution remains source-specific. [S45]

September reporting describes an arrest and formal investigation concerning illicit access, credential use, data aggregation and sale. Device examination and correlation continued. No individual defendant is named here, and an accusation is not treated as a conviction. [S47]

7.6 Prepare for capabilities while preserving actor uncertainty

A relevant claimant message should reach an accountable responder. The responder should assess the specific assertion against owned evidence and the service owner's account. Record whether the claim is corroborated, contradicted, historical or unresolved.

7.7 A global vulnerability example with no Chile exploitation claim

The following control example is separate from the Chilean actor and access claims. The NVD record and vendor advisory concern a remote-support vulnerability. They do not establish that a selected Chilean organisation installed the affected product or experienced exploitation. [S68][S69]

Reference	Affected scope	Verified remediation	Boundary
CVE-2026-1731	Vendor: Remote Support 25.3.1 and earlier; Privileged Remote Access 24.3.4 and earlier	Vendor branch patches BT26-02-RS / BT26-02-PRA; Remote Support 25.3.2 or later; PRA mitigation guidance specifies 25.1.1 or later	Follow the installed branch's supported vendor instructions

NVD describes a PRA configuration boundary before 25.1, while the vendor's mitigation text specifies 25.1.1 or later. Preserve that distinction rather than inventing an intermediate fixed release. Updating a product also does not independently establish whether earlier unauthorised access occurred. [S68][S69]

The vendor patch branches cover Remote Support 21.3–25.3.1 and PRA 22.1–24.X. Older unsupported releases require a supported upgrade path rather than an assumed patch. Follow the vendor's installed-version instructions. [S68]

The bank-related advertisement in Case C has no established connection to this vulnerability. A global record supplies control context, not its missing entry route or actor attribution.

KEY TAKEAWAYS

01

Qilin and The Gentlemen lead the retained listing population, not a verified national incident census.

02

Regional counts and monthly publication dates do not establish comparative safety or intrusion timing.

03

Keep source-to-proposition relationships separate from common-operator attribution.

CHAPTER 08

The fraud economy

08

THIS CHAPTER ANSWERS

How can credible information support deception, and which response can interrupt it?

Verify

a plausible detail does not authenticate a request

8.1 Information and monetisation are separate propositions 68
8.2 Loan offers and coercive collection 68
8.3 Real context is not authentication 69
8.4 Official impersonation and unsafe prompts 69
8.5 Payment-card material: a narrow observation 69
8.6 Enforcement is a separate evidence population 70
8.7 Completion evidence for fraud protection 70

CHAPTER 08

The fraud economy

IN SHORT

The public warnings describe loan offers, coercive collection, bank impersonation, booking messages and false jobs. The underground cases advertise information and access without proving a completed transaction. Their common defensive question is whether a person can verify a plausible request through a trusted route. Keep offers, customer reports, criminal allegations and validated payments separate, then train the relevant support and approval teams.

8.1 Information and monetisation are separate propositions

Provider files, school records, health information and access advertisements can create different concerns. A post's commercial wording does not establish possession or a completed sale. A free-release assertion does not establish authenticity or make the potential privacy consequence disappear. [S1]

The following is an **analytical model** for planning. It connects information, credible contact, a requested action and a possible payment. It does not establish that the same operator controlled those stages in the Chilean cases.

Stage	Possible abuse	Defender's interruption
Information is available	Personal context makes a message convincing	Establish affected categories and appropriate support
Contact is initiated	A caller or message imitates a trusted service	Provide an independently verified contact route
Action is requested	A person is asked for a code, payment or recovery approval	Explain the legitimate process and escalation
Payment is attempted	A changed destination or advance fee diverts money	Apply the organisation's payment and fraud checks
Contact continues	Earlier context supports another approach	Link supported reports and update the warning

8.2 Loan offers and coercive collection

CMF's March and April notices describe complaints concerning eight and four entities, respectively, that offered loans after advance payments without delivering the loans. The November notice describes another reported online loan offer and a complaint. These are attributed regulatory accounts, not convictions. [S42][S43][S26]

CMF also warned about thirteen credit applications in June and three in November, describing extortionate collection and suspected usury. Application counts are not borrower counts, criminal-group counts or ransomware incidents. The notices do not supply a national financial-loss denominator. [S28][S25]

8.3 Real context is not authentication

ANCI's bank-block warning describes a fraudster provoking a block and then impersonating the bank to seek a code or authorisation. A matching account problem can therefore be part of the deception. [S21]

Its booking warning explains that real reservation details can make a malicious payment request credible. Those details do not establish that the sender controls the legitimate service or that its underlying infrastructure was accessed. [S22]

In November, ANCI warned about false jobs seeking personal information, payments or messaging-app recovery codes. Human resources and customer support should know how to redirect a person to a genuine application or support process. Do not authenticate the approach through the suspicious sender. [S20]

8.4 Official impersonation and unsafe prompts

ANCI's tax-season warning describes fraudulent messages imitating tax-related public services. Its February email example imitates a state enterprise. Impersonation of an institution does not establish access to that institution's systems. [S23][S24]

The ClickFix warning describes fake error or human-verification prompts that persuade a person to follow unsafe instructions. The relevant defensive message is to stop and use a trusted support route. This report reproduces no commands or offensive workflow. [S18]

ANCI's post-click guidance distinguishes receiving a message from entering credentials or banking information. An enterprise response should likewise establish what the person actually did and which service was involved. Do not prescribe the same disruptive action for every report. [S19]

8.5 Payment-card material: a narrow observation

SCOPE OF THE CARD FIGURES

These figures describe a limited observed population of payment-card material. They do not establish national prevalence, current usability, completed transactions or fraud losses.

The held post material contains 288 distinct Chile-associated payment-card records. This is a narrow observation of published card material, not a Chilean issuer census or a measure of current card usability. No completed fraudulent transaction or loss total is inferred. [S4]

Source: narrow post-based payment-card observations [S4]. Published card material does not independently establish current usability, a completed fraudulent payment or the origin of exposure. No personal or payment-card identifier is reproduced.

8.6 Enforcement is a separate evidence population

September reporting describes prosecutors and PDI pursuing alleged illicit access, credentials, aggregation and sale. Device examination and correlation remained underway. The account does not prove every advertised dataset existed or that every earlier claim belonged to that investigation. [S47]

Fiscalía's August coordination notice identifies several financial-fraud variants and a national cooperation table. It supports attention to coordination across institutions. Historical totals in that notice are not adopted as 2026 national incidence. [S29]

CMF's January and February investment-platform warnings concern registration and legal authorisation to provide regulated services. Lack of authorisation is not by itself a conviction for fraud. A reader should verify a provider's status through the competent official route. [S40][S41]

An August judicial measure concerns an employee accused of selling information from an investigation. It is an allegation under investigation, not a conviction or evidence of external hacking. The context supports reviewing privileged access and information handling without connecting it to separate account-publication incidents. [S78]

8.7 Completion evidence for fraud protection

Owner	Capability	Completion evidence
Customer support	Recognise plausible impersonation and coercion	Staff exercise and an escalation record
Treasury	Verify changed instructions through a trusted route	Approved payment-verification record
Fraud	Assess relevant authorisations and transactions	Scoped decision with supporting evidence
Privacy	Identify information that supports follow-up contact	Data-category assessment and appropriate warning
Security	Distinguish a message from an account or device event	Dated response disposition

KEY TAKEAWAYS

01

Accurate personal context and claimed regulatory approval do not authenticate a request.

02

Keep advertised products, regulatory complaints and validated financial consequences separate.

03

Give staff and customers a trusted verification route that has been tested.

CHAPTER 09

Banking and financial services

09

THIS CHAPTER ANSWERS

Which financial-service observations require account, customer or continuity action?

25

selected banking, payment and investment domains, not a bank census

9.1 Preserve the financial denominators 72

9.2 An administration offer is not a bank-wide access finding 73

9.3 A continuity statement has a dated scope 73

9.4 Institutional access and customer fraud need parallel owners 74

9.5 Authentication obligations require a journey-specific assessment 74

9.6 Supplier dependencies and completion evidence 74

CHAPTER 09

Banking and financial services

IN SHORT

Financial services face separate questions about institutional access, customer deception, supplier dependencies and authentication. The selected banking, payment and investment portfolio has 25 domains; another 25 cover insurance and pensions. Passive observations do not establish bank intrusions or current customer exposure. A privileged-access advertisement remains unverified. Validate the specific account, maintain trusted customer verification and test the applicable authentication and reporting decisions in parallel.

9.1 Preserve the financial denominators

The selected financial group includes banks, payment services and investment organisations. Its 25 domains are not 25 independently validated banks. The insurance and pension group is a separate set of 25 selected domains, with different services and account populations. [S5]

Selected sector	Assessed domains	DMARC policy	HSTS header
Banking payments and investments	21	16 / 21	7 / 8 responses
Insurance and pensions	23	21 / 23	18 / 19 responses

The DMARC column counts observed policies requesting quarantine or rejection. It does not demonstrate effective enforcement for every legitimate message. HSTS counts retain the smaller denominator of available HTTPS responses. [S3]

The 25-domain banking, payment and investment group contains 151,575 device associations, including 1,151 employee-device associations. It has 249,271 credential-record associations, 17 current-listing domains and 2,359 document associations. These are overlapping observations, not confirmed bank intrusions. [S210]

The insurance and pension group contains 124,175 device associations, including 431 employee-device associations. It has 67,612 credential-record associations, 17 current-listing domains and 185 document associations. No institutional, sector or group rating is published. [S210]

The bank-issuer view covers 10 issuer domains within the selected banking portfolio. It contains 112,293 non-employee device associations, 940 employee associations and 10 current-listing domains. Non-employee associations do not establish customer identity or bank ownership of an endpoint. [S210]

SCOPE OF THE CARD FIGURES

These figures describe a limited observed population of payment-card material. They do not establish national prevalence, current usability, completed transactions or fraud losses.

The same bank-issuer view has 136 card associations across 6 issuers. This selected view is separate from the 288 distinct Chile-associated card records in Chapter 8. It does not establish a common exposure event or a bank-security ranking. [S4][S210]

10

Issuer domains within the selected banking portfolio

112,293

Non-employee device associations in the bank-issuer view

940

Employee-device associations in the bank-issuer view

The card scope above also governs the bank-issuer view interpretation. Card material, credential records and an access advertisement do not establish a common origin, current usability or a completed fraudulent payment.

9.2 An administration offer is not a bank-wide access finding

Case C contains an advertisement for a bank-related administration portal. The author claimed users, endpoints and API keys. Another participant disputed the offer's credibility. Neither post establishes usable access, current privileges or a completed transaction. [S1]

The relevant validation belongs inside the institution's controlled response process. Confirm whether the asserted service is owned, whether the account or key remains valid, and what permissions it could exercise. Review relevant activity before deciding the scope of containment.

9.3 A continuity statement has a dated scope

An official 2 May financial-institution statement says its platforms and services were operating normally amid reports concerning public-sector personal data. That is an attributed service-continuity statement, not confirmation of a bank intrusion. [S55]

9.4 Institutional access and customer fraud need parallel owners

ANCI's bank-block warning describes a deception that uses a real account problem to support a fraudulent contact. The customer can therefore face a convincing request without a demonstrated intrusion into the bank's infrastructure. [S21]

9.5 Authentication obligations require a journey-specific assessment

CMF says reinforced customer authentication under NCG 538 entered full force on 1 August. Its notice focuses chiefly on transfers and digital enrolment, with defined exceptions involving printed-data mechanisms. Do not convert that description into a universal ban on every such mechanism. [S27]

Compliance should identify the transaction and relevant rule. Product and architecture teams should show how the customer authorises the intended action. Fraud teams should assess deception around that journey rather than treating successful authentication as proof of legitimate intent.

ANCI's proposed MFA standard concerns essential services and OIV and remains a consultation at the cut-off. Institutions should assess readiness while retaining that legal status. A draft proposal and an existing CMF obligation must not share an undifferentiated effective date. [S15][S16]

9.6 Supplier dependencies and completion evidence

Test whether the supplier can explain the affected service, period and data categories while uncertainty remains. Preserve awareness times and the receiving institution's decision. Notification, fraud handling and service restoration can require separate owners even when they rely on shared facts.

Owner	Question	Completion evidence
Financial security	Is a relevant institutional account or service affected?	Scoped identity and activity determination
Fraud and support	Can a customer verify a suspicious request independently?	Tested contact route and staff response
Product and compliance	Does the relevant journey meet its applicable authentication duty?	Journey assessment, evidence and exceptions
Supplier owner	Can the provider support the institution's own incident decision?	Joint notification exercise and scoped account
Business continuity	Can customers complete the essential financial task?	Witnessed service and fallback test

KEY TAKEAWAYS

01

Financial-domain observations, privileged-access claims and payment-card material have separate populations.

02

Validate institutional access and customer deception through their appropriate owners in parallel.

03

Test authentication, supplier notification and essential customer journeys against their actual duties.

CHAPTER 10

Regulation and national response

10

THIS CHAPTER ANSWERS

Which duties are already operational, and which November proposals still need a status check?

3 hours

statutory early-warning maximum under the relevant Article 9 duty

10.1 Separate the instrument from its current status 77
10.2 Article 9 requires a usable awareness chronology 78
10.3 OIV containment is more specific than a generic reset instruction 79
10.4 Sanction limits are not incident-loss estimates 80
10.5 Financial authentication is an existing requirement 81
10.6 ANCI's November MFA document is still a proposal 81
10.7 The personal-data commencement question remains consequential 81
10.8 Make the national response routes operational 82

CHAPTER 10

Regulation and national response

IN SHORT

Law 21.663 gives relevant incident teams a short early-warning clock and separate update and final-report duties. OIV status adds responsibilities and can shorten the update period when essential-service provision is affected. CMF's reinforced-authentication requirements are already in effect, while ANCI's November MFA standard remains a consultation. The data-law postponement requires an enactment check. Assign legal scope, awareness times, decision owners and reporting channels before an incident starts.

This chapter supports operational planning. It does not replace legal advice on an entity's obligations, amendments, applicable sector rules or the facts of a particular incident.

10.1 Separate the instrument from its current status

The following table separates the principal instruments in the cited evidence.

Instrument	Status at cut-off	Relevant obligation or development	Responsible function
Law 21.663	Published statutory framework	Article 9 incident reporting; reinforced OIV responsibilities and statutory sanction bands [S13]	Legal, cybersecurity delegate and response
OIV designation	ANCI reported completion of its first process	1,154 designated entities in the combined process; designation itself is not an incident [S11]	Legal entity owner and compliance
General Instruction 4	Published December 2025; ANCI explained duties in June 2026	OIV containment, affected administrative credentials and remote-administration controls [S12][S14]	Delegate, identity and operations
CMF NCG 538	CMF says full effect from 1 August 2026	Reinforced customer authentication, chiefly for transfers and digital enrolment, with defined exceptions [S27]	Financial compliance, fraud and product owners
CMF bank-reporting proposal	Consultation opened 17 November	Proposed cyberincident and alert definitions and reporting information; comments until 15 December [S87]	Financial compliance and response

Instrument	Status at cut-off	Relevant obligation or development	Responsible function
ANCI MFA standard	Public consultation opened 19 November	Proposed essential-service and OIV requirements, not a final standard [S15][S16]	Security architecture and legal
Law 21.719 timetable	Original commencement and a later bill must be distinguished	Original date 1 December 2026; postponement bill at promulgation stage on 20 November [S30][S31][S32]	Privacy lead and legal

Article 53 identifies bodies operating under special regimes outside ANCI's regulation, inspection and supervision. They must agree incident-reporting and response-coordination mechanisms. Legal owners should establish the applicable regime before treating the ordinary ANCI sequence as uniform across public bodies. [S209]

10.2 Article 9 requires a usable awareness chronology

For institutions covered by Article 4, Article 9 requires reporting cyberattacks or cybersecurity incidents that may have significant effects under Article 27. Applicable special regimes must be considered. [S209]

The original law requires reporting as soon as possible, with an early-warning maximum of three hours from knowledge. It then requires an update within 72 hours. For an OIV where essential-service provision is affected, the stated update period is 24 hours. The final-report period is measured from the early warning. [S13]

The relevant clocks therefore need separate entries in the incident record.

Stage	Statutory maximum in cited text	Clock reference	Accountable operational owner	Operational evidence
Early warning	3 hours	Knowledge of the relevant incident	Response lead	Recorded awareness time, duty decision and submission receipt
Incident update	72 hours	Knowledge, under the relevant Article 9 sequence	Response lead	Updated scope, impact and response account
OIV affected-service update	24 hours	Knowledge, where essential-service provision is affected	Cybersecurity delegate	OIV status and documented service-impact determination
OIV action plan	Adopt within 7 calendar days; notify CSIRT Nacional as soon as adopted	Knowledge of the incident	Cybersecurity delegate, with response lead	Recorded awareness and adoption times, adopted plan and submission receipt

Stage	Statutory maximum in cited text	Clock reference	Accountable operational owner	Operational evidence
Final or situation report	15 calendar days	Early-warning submission	Response lead, with legal review	Final report; situation report replaces it if the incident remains ongoing
Final report after an ongoing incident	15 calendar days	Incident has been managed	Response lead, with legal review	Recorded management date, final report and submission receipt

For an ongoing incident, submit a situation report in place of the initial final report. Submit the final report within fifteen calendar days after the incident has been managed. Do not assume that unresolved investigation permits silence until every fact is known. The legal and response owners should prepare a bounded account of established facts and remaining uncertainty. [S13]

10.3 OIV containment is more specific than a generic reset instruction

General Instruction 4 sets the following OIV incident duties. Suggested owners and completion records make them operational; these job titles are recommendations. [S14]

Duty	Trigger and scope	Required action	Suggested owner	Completion evidence
Administrative passwords, Article 2	Incident affecting information confidentiality, integrity or legitimate resource use; affected or suspected systems	Change all passwords for accounts with full or partial administration permissions immediately, within three hours of awareness. Report changed accounts to ANCI in the early warning.	Identity and infrastructure leads	Awareness and reset times; account list and submission receipt
Administrative-account removal, Article 2	Same Article 2 trigger and systems	Immediately remove generic accounts and those not linked to active staff or suppliers, within three hours of awareness. First create a personal administrative account if none exists. Report removed accounts in the early warning.	Identity and infrastructure leads	Account review, personal-account creation where needed, removal times and submission receipt

Duty	Trigger and scope	Required action	Suggested owner	Completion evidence
Publicly exposed access, Article 3(a)	Any detected cybersecurity incident; remote or administrative access publicly exposed to the internet	Check for exposed access. Report any found to ANCI in the early warning and block or disable it within three hours of awareness.	Infrastructure lead, with response lead	Exposure review, restriction times and submission receipt
Incident remote access, Article 3(b–d)	Internet-exposed remote-access systems and remote access used during incident management	Permit access only through the institutional VPN. If unavailable, restrict access to indispensable segments or specific IP addresses; block and log other connection attempts. Use random credentials and MFA if immediately feasible. Disable remote access when its incident task ends.	Infrastructure and identity leads	Access rules, connection logs, authentication settings and shutdown record

Article 2 separately requires the account review and removal measures in its second paragraph preventively at least every six months. The incident duties above apply when their triggers occur; Chapter 12's scheduled readiness exercises do not defer them. [S14]

That credential requirement is not a universal three-hour password-reset instruction for every organisation and every rumour. The legal scope, affected identity and applicable incident facts matter. A team should know which administrative credentials and systems it can act on under the relevant duty.

10.4 Sanction limits are not incident-loss estimates

The original law sets different maximum fines by seriousness and OIV status. These are statutory ceilings in UTM, not predictions of the penalty for a case or a measure of cyber loss. [S13]

Classification	General maximum	OIV maximum
Minor	5,000 UTM	10,000 UTM
Serious	10,000 UTM	20,000 UTM
Very serious	20,000 UTM	40,000 UTM

The legal assessment determines the applicable classification and procedure. The public-service report discussed in Chapter 6 quoted ANCI as saying it had not imposed fines in that case. Do not turn controversy, an investigation or a newspaper headline into a completed sanction. [S36]

10.5 Financial authentication is an existing requirement

CMF's 31 July notice says NCG 538 entered full force on 1 August 2026. Its account emphasises reinforced authentication for transfers and digital enrolment. It also describes defined exceptions involving printed-data mechanisms. The notice does not support a universal claim that every such mechanism was banned. [S27]

ANCI's bank-account warning reinforces the distinction. A caller can exploit a real account block to seek a code or authorisation. The customer's actual problem does not authenticate the caller. Provide a trusted route for verification that does not depend on the suspicious contact. [S21]

A separate CMF consultation opened on 17 November concerns bank-reporting files, including cyberincident and alert definitions and the information used to describe incidents. Comments are accepted until 15 December. This is a proposal, not a final change to existing reporting obligations. [S87]

10.6 ANCI's November MFA document is still a proposal

On 19 November, ANCI opened a 30-day consultation on a proposed MFA and incident-prevention standard for essential services and OIV. The draft addresses human accounts, remote administration and operational-technology access. Its publication does not make every proposed provision effective. [S15][S16]

The draft's recitals discuss valid-credential access in significant incidents reported from March 2025 to the document date. That observation window differs from this report's window. The recital must not become a January–November 2026 national incident share or a Brandefense post statistic. [S16]

10.7 The personal-data commencement question remains consequential

BCN's legislative history records Law 21.719's publication on 13 December 2024 and its original commencement date of 1 December 2026. The 20 November Cámara notice says the postponement bill passed to promulgation. Its intended replacement date is 15 October 2027. [S30][S31]

The committee report identifies bulletin 18.623-07 and describes the proposed date change. The official tracker records presidential-approval stage and dispatch to the Executive. Neither record is an enacted amendment. The cited parliamentary progress does not establish promulgation and publication in Diario Oficial by this report's cut-off. [S32][S50]

The organisation's legal owner should check that final step immediately and again before 1 December 2026. Retain the original deadline unless a verified published amendment changes it. Record the checked instrument, publication and effective date. A project schedule should not be revised solely because a postponement was approved by legislators.

The same distinction applies to the future data-protection authority. A parliamentary proposal concerning its composition is not evidence that the authority is already operating under the amended framework. Do not infer an active regulator, reporting route or sanction from that proposal alone. [S31]

10.8 Make the national response routes operational

ANCI's October announcement describes citizen reporting and a first national cybersecurity exercise. Fiscalía's August notice describes national financial-fraud coordination. These are different response functions. An organisation should identify its appropriate incident and fraud contacts before deciding that one notification satisfies every need. [S10][S29]

KEY TAKEAWAYS

01

Preserve the three-hour warning clock and the separate update and final-report requirements.

02

Apply OIV and financial duties to the relevant entity, service and transaction.

03

Confirm the MFA and data-law instruments' final legal status before presenting proposals as existing law.

CHAPTER 11

Outlook and conditional planning

11

THIS CHAPTER ANSWERS

Which preparations follow from the evidence, and what would change those priorities?

6

bounded planning judgements with explicit revision signals

11.1 Six judgements and their limits 84

11.2 Conditional scenarios for the next planning cycle 85

11.3 What this report cannot predict 85

CHAPTER 11

Outlook and conditional planning

IN SHORT

Prepare for identity misuse, convincing impersonation, extortion claims and service interruption. Chile's official notices support those response questions without establishing future attack probabilities. Historical data can remain useful to fraudsters, and restored services can leave privacy questions unresolved. The regulatory timetable also needs continuing verification. Give each planning judgement an owner, a revision signal and a completion test, then reassess when the evidence changes.

11.1 Six judgements and their limits

Confidence concerns the stated proposition, not a prediction that an individual organisation will suffer an incident. A documented mechanism can justify preparation even when its national frequency is unknown. The table keeps the supporting evidence and the limitation together.

Judgement	Confidence	Basis	Boundary	Revision signal
Current account misuse deserves early validation	High for the documented response need	ANCI's May update identifies valid-credential access [S7]	No national probability or affected-account census	Evidence that a relevant account is active, privileged or recently used
Historical data can create renewed impersonation work	Medium for the planning implication	ANCI distinguishes historical material from a new infrastructure event [S8]	Continued usefulness is not established for every record	Verified follow-up contact using the information
Service continuity needs business acceptance	High for the distinction	Hospital and energy accounts describe different operating consequences [S34][S35]	The cases do not establish a common cause or sector frequency	A failed critical task or an unresolved operating restriction
Financial fraud requires a trusted independent contact route	High for the documented mechanism	Bank-block, advance-fee and credit-app warnings [S21][S25] [S26]	Warnings are not national loss estimates	Customer evidence of a suspicious authorisation or payment request
An AI label alone is a weak response trigger	High for the authority's guidance	ANCI emphasises malicious behaviour and unnecessary exposure [S17]	No confirmed Chilean AI campaign is inferred	Evidence of a specific affected asset, identity or harmful action
Legal readiness must track final instrument status	High for the need to verify	MFA consultation and data-law parliamentary progress [S15] [S31][S32]	Proposed dates are not enacted dates	Publication of a final standard or amendment

These judgements do not rank sectors by safety. They identify response capabilities supported by the retained public evidence. An organisation should prioritise them according to its actual services, validated exposures and obligations.

11.2 Conditional scenarios for the next planning cycle

The following scenarios are exercises, not forecasts or findings of a shared criminal operation.

Scenario	Trigger	First decision	Evidence of readiness
An advertised credential matches an active privileged account	Owned-account validation and relevant current evidence	Decide containment with identity and service owners	Tested session revocation, access review and business fallback
Customers receive plausible payment requests after a data incident	Preserved reports contain matching incident context	Coordinate fraud support and a trusted warning	Staff exercise, verified contact route and case linkage
A critical service is unavailable while the cause remains disputed	Service owner confirms a failed essential task	Activate fallback while investigating access separately	Witnessed task test and bounded communication template
A final regulatory instrument changes the applicable duty	Official enactment or publication is verified	Update the obligation register and implementation owner	Dated legal assessment and revised control plan

No scenario assumes that the same actor obtains information, contacts the customer and receives the proceeds. Any such chain would be an analytical model until evidence establishes its links. The exercise tests interruption points without claiming a complete criminal supply chain.

11.3 What this report cannot predict

Post volumes cannot establish the probability of an attack on a Chilean organisation. Criminal listings cannot establish future loss, control effectiveness or the national frequency of successful encryption. Public disclosure patterns do not provide a complete denominator for sector comparison.

The report also does not forecast political outcomes or attribute a future campaign to a government decision. A new actor announcement should be assessed against owned assets and corroborated consequences. It does not by itself change the country's technical risk profile.

Review the planning judgements when a material incident, validated exposure or final legal instrument changes the evidence. Keep a short record of what changed and why the owner altered the response. That creates an accountable planning cycle rather than a static threat ranking.

KEY TAKEAWAYS

01

Prepare for documented mechanisms without turning them into future attack probabilities.

02

Revise priorities when account, customer, service or legal evidence changes.

03

Give each scenario a decision owner and a demonstrated completion test.

CHAPTER 12

Action plan

12

THIS CHAPTER ANSWERS

What should teams deliver in 30, 60 and 90 days, and how will leadership verify it?

21

planning actions with accountable owners and completion evidence

12.1 The 30/60/90-day plan 88
12.2 Identity and endpoint teams 91
12.3 Business and operational owners 91
12.4 Fraud, treasury and customer operations 91
12.5 Legal, privacy and communications 91
12.6 A board scorecard based on evidence 91
12.7 Use the report as an evidence-to-decision record 92

CHAPTER 12

Action plan

IN SHORT

Start by ensuring that relevant alerts reach an owner. Validate current accounts, preserve reporting clocks and establish the minimum service that must continue. Then test supplier notification, authentication, customer verification and operational fallback. By day 90, demonstrate recovery and a joint incident exercise to leadership. These are planning targets, not permission to delay an urgent response. Assign each action and retain evidence that the intended function works.

12.1 The 30/60/90-day plan

The plan translates the report's evidence into a programme. Apply each row to the organisation's actual services and validated exposure. A current material incident belongs in the response process immediately, regardless of the planning period.

1Immediate; repeat before 1 December 2026

Check the personal-data-law status; retain the original deadline unless a verified published amendment changes it [S30][S50]

OWNER

Legal and privacy lead

COMPLETION EVIDENCE

Two dated publication checks, checked instrument and operative compliance deadline

2Days 1–30

Confirm relevant identity, data and service alerts reach an accountable person

OWNER

CISO and service desk

COMPLETION EVIDENCE

Tested delivery, backup owner and escalation record

Validate matching current credential offers against owned accounts

OWNER

Identity and incident response

COMPLETION EVIDENCE

Dated account, privilege, freshness and session assessment

Investigate relevant employee-device evidence without assuming other devices are customers

OWNER

Endpoint and identity teams

COMPLETION EVIDENCE

Account-purpose determination and documented response decision

Map the essential task, responsible owner and fallback for each critical service

OWNER

Business and operations

COMPLETION EVIDENCE

Approved service map and demonstrated alternative route

Confirm legal entity scope, OIV status and applicable reporting sequence

OWNER

Legal and cybersecurity delegate

COMPLETION EVIDENCE

Obligation register, checked sources and named reporting approver

Test the early-warning decision outside normal working hours

OWNER

Response, legal and delegate

COMPLETION EVIDENCE

Awareness chronology, practice submission and gap log

Establish a trusted route for suspicious payment and contact reports

OWNER

Fraud, treasury and customer support

COMPLETION EVIDENCE

Published verification process and staff briefing

3Days 31–60

Test notification with a supplier holding sensitive records or critical access

OWNER

Supplier owner and legal

COMPLETION EVIDENCE

Exercise notice with scoped facts, timestamps and contacts

Review active privileged sessions, recovery methods and delegated access

OWNER

Identity and security architecture

COMPLETION EVIDENCE

Witnessed revocation and recovery tests with exceptions

Assess authentication for relevant customer and remote-administration journeys

OWNER

Product, architecture and compliance

COMPLETION EVIDENCE

Journey-specific assessment, applicable rule and remediation owner

Validate legitimate email senders and authentication for important communications

OWNER

Messaging and domain owners

COMPLETION EVIDENCE

Approved sender inventory and controlled delivery test

Rehearse booking, citizen-service or operational fallback as applicable

OWNER

Service owner and operations

COMPLETION EVIDENCE

Completed essential-task test and business acceptance

Exercise customer support against accurate-context impersonation

OWNER

Fraud and customer operations

COMPLETION EVIDENCE

Staff exercise and independent-contact verification result

Review the status of the proposed MFA standard

OWNER

Legal and security architecture

COMPLETION EVIDENCE

Dated consultation and publication check, with the applicable obligation decision

4Days 61–90

Restore a critical service and validate its records and essential tasks

OWNER

Infrastructure and business owner

COMPLETION EVIDENCE

Isolated restoration, integrity checks and accepted operating result

Rehearse simultaneous service disruption and possible data exposure

OWNER

Response, operations, privacy and communications

COMPLETION EVIDENCE

Separate service, access, notification and communication decisions

Test operational remote-access restriction where relevant

OWNER

OT owner and authorised engineer

COMPLETION EVIDENCE

Safe procedure, approved change and independent operating check

Review incident-related customer contact after technical recovery

OWNER

Customer support and fraud

COMPLETION EVIDENCE

Scoped follow-up review and disposition of validated reports

Reassess historical exposure and repeated advertisements

OWNER

Intelligence, identity and privacy

COMPLETION EVIDENCE

Current, historical, unrelated or unresolved disposition for each relevant lead

Report outcomes, exceptions and unresolved dependencies to leadership

OWNER

CISO and accountable business executives

COMPLETION EVIDENCE

Board record with owners, due dates and witnessed completion evidence

12.2 Identity and endpoint teams

Begin with the account's actual purpose. Confirm the domain and service belong to the organisation, establish whether the account remains active, and check the privileges at risk. Historical credentials and current unauthorised use require different decisions.

Where containment is warranted, consider sessions, added authentication methods, delegated access and recovery routes alongside the password. The completion test is a controlled account state with an accountable owner. It should not rely solely on a user acknowledging a reset email.

12.3 Business and operational owners

Define the essential task in terms a user can perform. For a hospital, that can include urgent appointment handling. For a public service, it can include an alternative route to a necessary request. For an operating facility, use its approved engineering acceptance criteria.

12.4 Fraud, treasury and customer operations

Corporate treasury should verify changed payment instructions through a known route. The person approving a payment should not authenticate a change solely through the same message that requested it. Record the verification and the decision under the organisation's payment procedure.

12.5 Legal, privacy and communications

Maintain one shared chronology of established facts, but record each reporting and communication decision separately. The technical response, an authority notification, a criminal complaint and a message to affected people can have different triggers and owners.

Track legal changes through the final official instrument. ANCI's MFA consultation and parliamentary progress on the data-law postponement have different legal status. Retain the source and date supporting any change to the operative compliance timetable. [S15][S31][S32]

12.6 A board scorecard based on evidence

The board needs a small set of outcomes rather than a national threat score. The following questions make the programme reviewable without asserting a numerical target unsupported by the report.

Decision area	Leadership question	Evidence to request
Identity	Can the team distinguish an active account event from historical material?	Validated case with account and session decisions

Decision area	Leadership question	Evidence to request
Service continuity	Can users complete the essential task during degradation?	Witnessed fallback test and business acceptance
Supplier dependency	Can a critical supplier notify and support a timely response?	Joint exercise with scoped facts and timestamps
Customer protection	Can a person independently verify a plausible request?	Tested contact route and trained support response
Reporting	Can the organisation reach an authorised decision within its applicable clock?	Awareness chronology and practice submission
Recovery	Can the organisation restore the service and reconcile interrupted work?	Restoration result, integrity checks and backlog review
Legal status	Are duties based on current enacted instruments?	Dated source check and accountable legal assessment

12.7 Use the report as an evidence-to-decision record

Brandefense Blackhole observations and Ransompedia listings provide distinct evidence populations in this report. The value for a defender lies in reviewing a relevant signal with its limits, assigning an owner and recording a proportionate disposition. Their counts remain separate from confirmed organisational incidents.

For a demonstration of Brandefense, visit Request a demo. Use the discussion to connect the organisation's evidence priorities, accountable owners and completion tests.

KEY TAKEAWAYS

01

Establish alert ownership, account validation, service fallback and reporting readiness by day 30.

02

Test suppliers, authentication, customer verification and relevant service alternatives by day 60.

03

Demonstrate recovery and joint decisions, then report owned exceptions to leadership by day 90.

APPENDICES

Appendices

A–D

THIS CHAPTER ANSWERS

Which populations, dates and limitations govern the report's findings?

Separate

posts, listings, organisations, people and transactions

Appendix A. Scope and evidence boundaries 94

Appendix B. Evidence register 96

Appendix C. Sources 98

Appendix D. Glossary 102

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 Window and dates

The main observation window covers posts dated 1 January–22 November 2026. The recent-activity view covers 8–22 November. Public incident accounts retain the event, discovery, disclosure and update dates supported by their sources.

The report describes the evidence available at the cut-off. It is not a completed census of every Chilean incident or every event on the cut-off date. Subsequent investigations can change the scope, mechanism or attribution of a reported event.

A.2 Source populations

The report uses held underground posts, public ransomware listings, selected-domain observations and public reporting. Each population has its own unit and coverage. A country-associated post, a criminal listing, a domain and an organisation's notice are not interchangeable incident records. [S1][S2][S3][S5]

The monthly series totals 27,891 observations; one July observation is not among the 27,890 held posts used for percentages. [S1]

A.3 Selected domains and passive observations

The portfolio has 250 selected primary-domain records across ten merged sectors. Selection reflects institutional and service relevance. It is not a revenue ranking, a census or a statistically representative estimate of Chilean organisations. [S5]

Passive results describe the assessed configuration at a stated date. Each result retains its available denominator. Inconclusive observations remain unknown. A missing result is not a missing control, and a visible control does not establish its effectiveness for every service. [S3]

Atlas supplies the national headline of 58/100 (B) for the selected portfolio. Only that national rating is published. Device, employee-device, credential-record, listing and document observations describe separate overlapping populations. Passive results retain their own assessed denominators. [S210][S3]

A.4 Ransomware listings

Ransompedia records 41 Chilean listing rows in the requested window, with 39 distinct organisation-name strings and 13 claimant labels. The strings are not independently validated legal entities. A listing remains a criminal assertion about the referenced organisation. [S2]

The four regional peers use the same requested current window. Their raw totals do not control for economic scale, organisation populations or disclosure behaviour. The 2025 Chilean comparison is a full prior year and is not a matched-period growth rate.

A.5 Payment-card scope

These figures describe a limited observed population of payment-card material. They do not establish national prevalence, current usability, completed transactions or fraud losses. [S4]

A.6 Case and relationship boundaries

The detailed case set contains six underground claim dossiers and the bounded public accounts in Chapter 5. A dossier can concern several related posts or updates. It is not automatically one independently confirmed intrusion.

Case A and the mining-client supplier context share a provider reference. That does not establish the same event or files. The supplier context is not counted as an additional independent intrusion. A named customer in an advertisement is not a separately confirmed victim.

Source-to-proposition relationships are distinct from common-operator findings. A shared sector, quantity, language or technique does not establish a campaign. The fraud-chain model is explicitly analytical rather than a verified mapping of the same operator through every stage.

A.7 Confidence and alternatives

Confidence attaches to a proposition. Confidence that a held message exists can be high while confidence in the asserted access remains low. An official statement can establish the source's position without independently resolving every technical question.

A.8 Names, sources and neutrality

Victim roles remain broad where the naming conditions are not established. Public-source addresses that would identify a withheld subject are shortened to the publisher's root and marked as withheld. Supporting source status is retained separately from the public citation address.

The report takes no position on the 2025 presidential and parliamentary elections, the subsequent government, political parties or government decisions. It takes no position on Mapuche or Araucanía issues or relations with Bolivia and Peru.

An actor's political framing does not establish motive, nationality or state direction. Source-attributed state associations remain that source's assessment. The electoral-data claim establishes no current system intrusion or effect on an election.

Appendix B. Evidence register

The twelve post cards present bounded excerpts and accompanying limits. They support the existence and wording of assertions, not the authenticity or completeness of advertised material. Card IDs remain the same across editions.

Card	Posted	Venue	Alias	Shown in
B01	2026-04-04	Forum	Withheld	Case A
B02	2026-04-15	Forum	Withheld	Case A
B03	2026-03-06	Forum	Withheld	Case C
B04	2026-04-05	Forum	Withheld	Case B
B05	2026-10-29	Forum	Withheld	Case F
B06	2026-10-05	Forum	Withheld	Case D
B07	2026-10-04	Forum	Withheld	Case D
B08	2026-11-12	Forum	Withheld	Case E
B09	2026-11-20	Forum	Withheld	Section 4.5
B10	2026-11-22	Forum	Withheld	Section 4.5
B11	2026-02-02	Forum	Withheld	Section 4.5
B12	2026-01-14	Forum	Withheld	Section 4.5

The case index distinguishes dossiers from confirmed-incident counts. Case letter N is not used.

Case	Subject role	Principal evidence
A	Business software and hosting provider	Related advertisements; supplier source context remains bounded
B	Enterprise software consultancy	Source/database offer and ransom language
C	Banking-related administration portal	Access advertisement and credibility dispute
D	Education administration	Related dataset release claims
E	School network	Historical-span sale offer
F	Healthcare providers	Multi-target release claim
G	Public services and communications	ANCI's initial and updated account-access notices

Case	Subject role	Principal evidence
H	Historical data alert	ANCI's earlier-leak assessment
I	Hospital imaging information	Press reporting of a criminal complaint
J	Hospital support services	Reported organisational statement and continuity account
K	Energy facility	Dated operational records and subsequent reporting
L	Public-service agency	Competing technical accounts during investigation
M	Retailer	Official disclosure and later operational update
O	Telecommunications	Reported investigation with historical activity
P	Public-service agency	Reported unauthorised messages and interruption
Q	Health service	Qualified statement of possible information extraction
R	Manufacturing group	Reported multinational incident with a Chilean consequence
S	Regional public body	Regional reporting of an administrative-account event
T	Legal-services firm	Reported ransomware complaint and recovery account
U	Public-sector publishing service	One account-related statement reported by two outlets

Cases A and the mining-client supplier source context are not treated as independent intrusions. Case H is an alert correction, and several other dossiers preserve investigation or data-scope uncertainty. The index is a reading aid, not a national victim count.

Appendix C. Sources

Each entry records the supporting-source review date. Some addresses are shortened to protect withheld subjects. A public citation address is distinct from the substantive source passage supporting the finding.

S1: Odin by Brandefense. Retained Chile-associated underground post observations. Own retained research; no public URL. Verified on 2026-11-22.

S2: Ransompedia. Chile and regional-peer ransomware listing aggregates. Own retained research; no public URL. Verified on 2026-11-22.

S3: Odin by Brandefense. Passive DNS and TLS observations for selected Chilean domains. Own retained research; no public URL. Verified on 2026-11-22.

S4: Brandefense Blackhole. Narrow payment-card aggregates from collected post material. Own retained research; no public URL. Verified on 2026-11-22.

S5: Odin by Brandefense. Selected Chilean organisation-domain portfolio and sector denominators. Own retained research; no public URL. Verified on 2026-11-22.

S6: ANCI. ANCI initial response to reported data publications. https://anci.gob.cl/noticias/anci-informa-sobre-reportes-de-las-ultimas-horas/ Verified on 2026-11-22.

S7: ANCI. ANCI update: unauthorized access with valid credentials. https://anci.gob.cl/noticias/actualizacion-anci-filtraciones-por-robo-de-credenciales/ Verified on 2026-11-22.

S8: ANCI. ANCI identifies historical material in new leak alert. https://anci.gob.cl/noticias/sobre-reciente-informacion-de-supuestas-filtraciones/ Verified on 2026-11-22.

S9: ANCI. Panorama Actual de Amenazas: first semester 2026. https://anci.gob.cl/documents/5140/Panorama_Actual_de_Amenazas_2026_Octubre.pdf Verified on 2026-11-22.

S10: ANCI. ANCI month of cybersecurity launch and reporting total. https://anci.gob.cl/noticias/anci-mes-de-la-ciberseguridad-2026/ Verified on 2026-11-22.

S11: ANCI. ANCI closes first OIV designation process. https://anci.gob.cl/noticias/anci-finaliza-el-primer-proceso-de-calificacion-de-operadores-de-importancia-vital/ Verified on 2026-11-22.

S12: ANCI. OIV mitigation measures under General Instruction 4. https://anci.gob.cl/noticias/obligaciones-instruccion-general-n4/ Verified on 2026-11-22.

S13: Diario Oficial. Law 21.663 official publication. https://www.diariooficial.interior.gob.cl/publicaciones/2024/04/08/43820/01/2475674.pdf Verified on 2026-11-22.

S14: Diario Oficial. General Instruction 4 original publication. https://www.diariooficial.interior.gob.cl/publicaciones/2025/12/26/44333-B/01/2747332.pdf Verified on 2026-11-23.

S15: ANCI. MFA standard opens for public consultation. https://anci.gob.cl/noticias/consulta-publica-normativa-mfa/ Verified on 2026-11-22.

S16: ANCI. MFA draft under public consultation. https://anci.gob.cl/documents/5200/Estandar_1_20261105.pdf Verified on 2026-11-22.

S17: ANCI. ANCI advice on AI-assisted attacks. https://anci.gob.cl/noticias/recomendaciones-anci-ante-el-uso-de-herramientas-de-ia-en-ciberataques/ Verified on 2026-11-22.

S18: ANCI. ClickFix citizen warning. https://anci.gob.cl/ciberconsejos/ciberconsejos-clickfix/ Verified on 2026-11-22.

S19: ANCI. Post-click response guidance. https://anci.gob.cl/ciberconsejos/ciberconsejos-y-si-ya-hice-clic/ Verified on 2026-11-22.

S20: ANCI. Fake-job offer warning. https://anci.gob.cl/ciberconsejos/ciberconsejos-estafas-en-falsas-ofertas-laborales/ Verified on 2026-11-22.

S21: ANCI. Bank-account blocking social engineering warning. https://anci.gob.cl/ciberconsejos/ciberconsejos-el-fraude-de-la-cuenta-bancaria-bloqueada/ Verified on 2026-11-22.

S22: ANCI. Hotel-reservation phishing warning. https://anci.gob.cl/ (article URL withheld) Verified on 2026-11-22.

S23: ANCI. Tax-season impersonation warning. https://anci.gob.cl/ciberconsejos/ciberconsejos-operacion-renta-2026/ Verified on 2026-11-22.

S24: ANCI. State-company impersonation email warning. https://anci.gob.cl/ciberconsejos/ciberconsejos-claves-para-identificar-un-email-falso/ Verified on 2026-11-22.

S25: CMF. CMF warns on credit-app extortion and possible usury. https://www.cmfchile.cl/portal/prensa/625/w4-article-115042.html Verified on 2026-11-22.

S26: CMF. CMF warns on advance-fee loan fraud. https://www.cmfchile.cl/portal/prensa/625/w4-article-115043.html Verified on 2026-11-22.

S27: CMF. CMF reinforced authentication comes into full effect. https://www.cmfchile.cl/portal/prensa/625/w4-article-112253.html Verified on 2026-11-22.

S28: CMF. CMF thirteen credit-app warning. https://www.cmfchile.cl/portal/prensa/625/w4-article-111149.html Verified on 2026-11-22.

S29: Fiscalía de Chile. National financial fraud coordination body. https://www.fiscaliadechile.cl/actualidad/noticias/organismos-publicos-y-del-sector-privado-financiero-crean-mesa-nacional-contra Verified on 2026-11-22.

S30: Biblioteca del Congreso Nacional. Personal-data law legislative history. https://www.bcn.cl/balance-legislativo/detalle/ficha_LEY_21719_2024-12-13 Verified on 2026-11-23.

S31: Cámara de Diputadas y Diputados. Cámara reports postponement bill sent to promulgation. https://www.camara.cl/cms/2026/11/20/datos-personales-combustibles-y-sala-cuna-en-los-temas-despachados-por-la-camara/ Verified on 2026-11-22.

S32: Cámara de Diputadas y Diputados. Data-law postponement committee report. https://www.camara.cl/verDoc.aspx?prmID=79766&prmTipo=DOCUMENTO_COMISIONINFORME Verified on 2026-11-22.

S33: T13. Hospital imaging-data incident reported from criminal complaint. https://www.t13.cl/ (article URL withheld) Verified on 2026-11-22.

S34: BioBioChile. Hospital November service disruption and maintained clinical care. https://www.biobiochile.cl/ (article URL withheld) Verified on 2026-11-22.

S35: 24 Horas. Energy-service interruption after an operator-reported cyberattack. https://www.24horas.cl/ (article URL withheld) Verified on 2026-11-22.

S36: El Mostrador. Public-service incident: allegations and official responses differ. https://www.elmostrador.cl/ (article URL withheld) Verified on 2026-11-22.

S37: NIVEL4 Labs. Health-insurer Qilin listing is unverified. https://blog.nivel4.com/ (article URL withheld) Verified on 2026-11-23.

S38: ANCI. ANCI health-sector guidance. https://anci.gob.cl/noticias/anci-y-cens-lanzan-recomendaciones-de-ciberseguridad-para-sistemas-de-informacion-en-salud/ Verified on 2026-11-22.

S40: CMF. CMF investment-platform warning January. https://www.cmfchile.cl/portal/prensa/625/w4-article-102694.html Verified on 2026-11-22.

S41: CMF. CMF investment-platform warning February. https://www.cmfchile.cl/portal/prensa/625/w4-article-103951.html Verified on 2026-11-22.

S42: CMF. CMF advance-fee loan warning March. https://www.cmfchile.cl/portal/prensa/625/w4-article-108614.html Verified on 2026-11-22.

S43: CMF. CMF advance-fee loan warning April. https://www.cmfchile.cl/portal/prensa/625/w4-article-109384.html Verified on 2026-11-22.

S44: BioBioChile. Mining client response to supplier incident. https://www.biobiochile.cl/ (article URL withheld) Verified on 2026-11-22.

S45: BioBioChile. Telecom network-activity investigation reporting. https://www.biobiochile.cl/ (article URL withheld) Verified on 2026-11-22.

S46: BioBioChile. Public-service unauthorized messages and short outage. https://www.biobiochile.cl/ (article URL withheld) Verified on 2026-11-22.

S47: BioBioChile. September data-trading enforcement action. https://www.biobiochile.cl/ (article URL withheld) Verified on 2026-11-22.

S48: BioBioChile. ANCI preventive response to AI-integration supply-chain concern. https://www.biobiochile.cl/ (article URL withheld) Verified on 2026-11-22.

S49: trendTIC. Manufacturing ransomware case with unresolved event year. https://www.trendtic.cl/ (article URL withheld) Verified on 2026-11-22.

S50: Cámara de Diputadas y Diputados. Data-law postponement legislative tracker. https://www.camara.cl/legislacion/proyectosdeley/tramitacion.aspx?prmBOLETIN=18623-07&prmID=19307 Verified on 2026-11-23.

S51: Retail operator. Retail incident official essential disclosure. Publisher address withheld to protect the subject. Verified on 2026-11-22.

S52: Retail operator. Retail incident official October update. Publisher address withheld to protect the subject. Verified on 2026-11-22.

S53: Coordinador Eléctrico Nacional. Electricity-coordinator operation record, 27 August. https://www.coordinador.cl/ (article URL withheld) Verified on 2026-11-22.

S54: Coordinador Eléctrico Nacional. Electricity-coordinator operation record, 9 November. https://www.coordinador.cl/ (article URL withheld) Verified on 2026-11-22.

S55: Financial institution. Bank official service-continuity statement. Publisher address withheld to protect the subject. Verified on 2026-11-22.

S56: T13. Hospital statement reported on 16 November. https://www.t13.cl/ (article URL withheld) Verified on 2026-11-22.

S57: Cámara de Diputadas y Diputados. Parliamentary hospital continuity inquiry. https://camara.cl/ (article URL withheld) Verified on 2026-11-22.

S60: Cámara de Diputadas y Diputados. Parliamentary request concerning electricity incidents. https://www.camara.cl/ (article URL withheld) Verified on 2026-11-22.

S63: BioBioChile. Health-service statement on possible information extraction. https://www.biobiochile.cl/ (article URL withheld) Verified on 2026-11-22.

S64: BioBioChile. Manufacturing-group ransomware reporting with Chile effect. https://www.biobiochile.cl/ (article URL withheld) Verified on 2026-11-22.

S65: Araucanía Noticias. Regional public-body account-access reporting. https://araucanianoticias.cl/ (article URL withheld) Verified on 2026-11-23.

S68: BeyondTrust. BeyondTrust BT26-02 original advisory. https://www.beyondtrust.com/trust-center/security-advisories/bt26-02 Verified on 2026-11-22.

S69: NVD. NVD CVE-2026-1731 page. https://nvd.nist.gov/vuln/detail/CVE-2026-1731 Verified on 2026-11-23.

S70: 24Horas. Legal-services firm confirms ransomware complaint and recovery. https://www.24horas.cl/ (article URL withheld) Verified on 2026-11-22.

S71: BioBioChile. ANCI transparency-response significant incident reports through 15 October. https://www.biobiochile.cl/especial/bbcl-investiga/noticias/de-pasillo/2026/11/07/ciberataques-a-servicios-esenciales-organismos-han-reportado-566-incidentes-significativos-en-2026.shtml Verified on 2026-11-22.

S72: BlackDoor. September finance-company extortion listing remains unconfirmed. https://www.blackdoor.cl/ (article URL withheld) Verified on 2026-11-22.

S73: DeXpose. Maritime company Qilin public claim relay. https://www.dexpose.io/ (article URL withheld) Verified on 2026-11-22.

S74: Diario Financiero. Energy distributor statement on internal-storage unauthorized access. https://www.df.cl/ (article URL withheld) Verified on 2026-11-23.

S75: El Mostrador. Energy distributor public response and conflicting extortion claim. https://www.elmostrador.cl/ (article URL withheld) Verified on 2026-11-23.

S76: Instructure. Canvas incident vendor update. https://www.instructure.com/incident_update Verified on 2026-11-23.

S77: T13. Health-sector organisation dated response to May alert. https://www.t13.cl/ (article URL withheld) Verified on 2026-11-22.

S78: T13. Judicial employee alleged insider information sale investigation. https://www.t13.cl/ (article URL withheld) Verified on 2026-11-22.

S82: ADN Radio. July unverified public-service claim. https://www.adnradio.cl/ (article URL withheld) Verified on 2026-11-22.

S83: Emol/ATON. Institutional publication-account statement. https://www.emol.com/ (article URL withheld) Verified on 2026-11-22.

S84: ADN Radio. Institutional publication-account scope corroboration. https://www.adnradio.cl/ (article URL withheld) Verified on 2026-11-22.

S85: DataReportal/Simon Kemp. Digital 2027 Chile: October 2026 internet adoption context. https://datareportal.com/reports/digital-2027-chile Verified on 2026-11-22.

S86: Coordinador Eléctrico Nacional. Electricity operator daily report extends solar and battery unavailability observation. https://www.coordinador.cl/ (article URL withheld) Verified on 2026-11-22.

S87: CMF. CMF consults on bank reporting files including cyberincident file I12. https://www.cmfchile.cl/portal/prensa/625/w4-article-115004.html Verified on 2026-11-22.

S200: NIST. Multi-factor authentication definition. https://csrc.nist.gov/glossary/term/multi_factor_authentication Verified on 2026-11-22.

S201: NIST. Distributed denial-of-service definition. https://csrc.nist.gov/glossary/term/distributed_denial_of_service Verified on 2026-11-22.

S202: Servicio de Impuestos Internos. Monthly tax-unit definition. https://www.sii.cl/ayudas/ayudas_por_servicios/4669-u.html Verified on 2026-11-22.

S203: RFC Editor. DMARC specification. https://www.rfc-editor.org/rfc/rfc9989 Verified on 2026-11-22.

S204: RFC Editor. SPF specification. https://www.rfc-editor.org/rfc/rfc7208 Verified on 2026-11-22.

S205: RFC Editor. DKIM specification. https://www.rfc-editor.org/rfc/rfc6376 Verified on 2026-11-22.

S206: RFC Editor. DNSSEC specification. https://www.rfc-editor.org/rfc/rfc4033 Verified on 2026-11-22.

S207: RFC Editor. TLS specification. https://www.rfc-editor.org/rfc/rfc9846 Verified on 2026-11-22.

S208: RFC Editor. HSTS specification. https://www.rfc-editor.org/rfc/rfc6797 Verified on 2026-11-22.

S209: Biblioteca del Congreso Nacional. Law 21.663: current statutory text and Article 53 special regimes. https://www.bcn.cl/leychile/navegar?i=1202434 Verified on 2026-11-23.

S210: Brandefense Atlas exposure ratings and Blackhole device, employee-device, credential-record, document and current credential-market observations for 250 selected domains; bank-issuer exposure and card aggregates. Read 22 November 2026. Verified on 2026-11-22.

Appendix D. Glossary

Term	Plain meaning
ANCI	Agencia Nacional de Ciberseguridad, Chile's national cybersecurity agency [S11]
API key	A credential used by software to access a service
Awareness time	The recorded time when an organisation knows the facts relevant to an incident assessment
Claimant label	The name used in a criminal publication, without proving common operation
ClickFix	Deception through a fake error or verification prompt that induces an unsafe action [S18]
Credential	Information used to authenticate, such as a password or access token
DDoS	A denial-of-service attack using many hosts [S201]
DKIM	A method for signing email so receivers can check its association with a domain [S205]
DMARC	A domain's policy for handling email authentication and sender alignment [S203]
DNSSEC	Extensions that support validation of DNS data authenticity [S206]
HSTS	A web policy directing compatible browsers to use HTTPS for a service [S208]
MFA	Authentication requiring more than one distinct type of evidence [S200]
OIV	An operator designated as vital under Chile's cybersecurity framework, with reinforced duties [S11]
Privileged session	Authenticated access with permissions that can affect sensitive functions
Ransompedia	Brandefense's ransomware-listing source; its listings remain criminal assertions
SPF	A domain's statement of which services may send email on its behalf [S204]
Supplier dependency	A service, information store or access path controlled by another organisation

Term	Plain meaning
TLS	A protocol used to protect network communications [S207]
UTM	Chile's monthly tax unit, expressed in pesos and updated for consumer-price changes [S202]

About this report

Prepared by Odin by Brandefense for security leadership, responders, infrastructure and operational teams, fraud specialists, customer support, legal and privacy owners. Version 1.0 covers the requested 1 January–22 November 2026 window, with a separate 8–22 November recent-activity view.

The Spanish edition is translated from the English master and carries a visible AI-translation notice. The English edition prevails where the editions differ. The report does not claim that unavailable evidence, an unresolved investigation or a restored service answers every remaining security question.

© 2026 Brandefense. All rights reserved.

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