BRANDEFENSE COUNTRY REPORT · PERU 2026

Brandefense Peru Cyber Threat Landscape Report 2026

Identity advertising, supplier access and the decisions that protect public trust

Odin by Brandefense
Research window: 22 November 2026
Version 1.0 · Public Research Edition · TLP:CLEAR · : 23 November 2026

250
selected domain candidates across ten merged sector groups

9
illustrated claim dossiers, supported by ten post cards

5
public case dossiers with different evidence and incident units

58
Peru ransomware listings, each recording a criminal assertion

CONTENTS

Contents

01	Executive summary	05
	Report map	09
02	Peru's digital and threat context	10
03	National exposure: the selected organisation portfolio	14
04	Underground activity and claim interpretation	22
05	Public incidents and sector response	38
06	Unauthorised messages, access claims and service availability	45
07	Threat actors, ransomware and supported relationships	49
08	Fraud economy: identity, persuasion and payment	60
09	Banking and customer protection	64
10	Regulatory response and reporting decisions	69
11	Outlook and conditional planning assumptions	73
12	The 30/60/90-day action plan	77
A	Appendix A. Scope, evidence and confidence	84
B	Appendix B. Post evidence register	87
C	Appendix C. Sources	88
D	Appendix D. Plain-language glossary	91
	About this report	93

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

About this edition

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

Peru's evidence connects identity-data advertising, extortion claims and distinct public security accounts. Validate the specific proposition before choosing account containment, customer protection or service recovery.

99,532

Peru-tagged posts; country association does not establish an incident

58

ransomware listings in the requested window; criminal claims

14

case dossiers: nine underground claims and five public accounts

4

leadership decisions with accountable owners and completion evidence

Contents and reading routes

Chapter	Question
1 Executive summary	Which decisions come first?
2 Context	Which Peruvian operating conditions shape the response?
3 National exposure	What is measured, and what remains unavailable?
4 Underground activity	What do the retained claims establish?
5 Sectors and public cases	Which public accounts change a concrete decision?
6 Availability and message integrity	Which service effect and actor role are actually established?
7 Actors and ransomware	What supports each label and relationship?
8 Fraud economy	How should identity and payment risks be separated?
9 Banking	Which customer and supervisory decisions follow?
10 Regulation	Which duties apply now, and which changes come later?
11 Outlook	What would change the planning assumptions?
12 Action plan	Who acts, and what demonstrates completion?
Appendices A–D	Scope, evidence, sources and definitions

CHAPTER 01

Executive summary

01

THIS CHAPTER ANSWERS

Which findings justify immediate decisions for Peruvian organisations?

4

leadership decisions linked to evidence and completion criteria

Four decisions for leaders 07

The year in numbers 07

CHAPTER 01

Executive summary

IN SHORT

Peru's evidence supports account validation, supplier oversight, customer protection and tested continuity. Ransompedia records 58 listings, while underground posts advertise identity records and access. Public accounts distinguish supplier-account misuse, customer-information access, disputed transfers and impersonation. Recent November publications do not all describe newly acquired data. Establish a reliable alert route, validate owned accounts and records, rehearse a critical service fallback, and assign separate reporting and communication owners.

This report combines Brandefense's own retained post evidence and ransomware listings with source-read public reporting. It separates posts, advertisements, listings, public events, complaints and domain observations. These populations are not added into a national attack total. [S1][S2]

The requested cut-off is 22 November. The cut-off day was still in progress during collection, so the evidence reflects what was available when checked. Publication, acquisition, detection, service restoration and regulatory follow-up can have different dates.

1. **Publication volume does not establish a national incident count.** The country-tagged population contains 99,532 posts. Nine selected claim dossiers examine records, documents and advertised access. A January discussion identifies older material, without independently proving its acquisition date or file identity. Validate relevance and freshness before declaring a new incident. [S1]

2. **Extortion visibility spans several labels and can repeat organisations.** Ransompedia records 58 Peru listings, compared with 26 for all of 2025. This is a partial-year versus full-year comparison, not a growth rate. Qilin, The Gentlemen and Nova account for 28 of the 58 listings. A listing remains a criminal assertion. [S2]

3. **Public accounts support different containment and customer decisions.** The five public dossiers include supplier-account misuse, insurer customer-information access, reported unauthorised transfers, an impersonation warning and an enforcement operation. They are not five confirmed network intrusions. The response should follow the established function and evidence. [S17][S18][S23][S20][S22]

4. **Recent activity includes claims, denials and research about earlier observations.** The closing fortnight includes business-record and education-related advertisements, employment-history offers and three ransomware listings. A vendor's November malware publication covers earlier multi-country attempts. Preserve the date and evidence type for each item. [S1][S2][S27][S32]

5. **Exposure and reporting decisions need their own denominators and clocks.** The selected portfolio contains 250 domain candidates. A credential was listed for sale for 68 candidates when checked; this does not establish usable access. Personal-data, digital-service and financial duties also have separate triggers and recipients. Assign validation and reporting owners before an incident forces the decision. [S3][S5][S6][S7]

Four decisions for leaders

1. **Establish the alert route and validate owned evidence.** Confirm that relevant account and data alerts reach a named team. Validate ownership, account status, privilege and prior remediation before choosing containment (§3–4, §12).
2. **Test supplier privileges and minimum safe service.** Demonstrate who can suspend a supplier account, issue a trusted correction and maintain a critical user task while the normal service is unavailable (§5–6, §12).
3. **Keep customer and payment protection active during technical recovery.** Authenticate beneficiary and account-recovery changes independently. Give customers a legitimate route to verify suspicious requests (§8–9).
4. **Separate the reporting decisions and preserve awareness times.** Map personal-data, digital-service and financial scope. Distinguish rules in force from consultation proposals and later commencement dates (§10).

The year in numbers

99,532

Peru-tagged posts in the requested post-time window

WHAT IT DOES NOT MEASURE

Confirmed targeting, unique offers or national incidents

58

Peru ransomware listings in the requested window

WHAT IT DOES NOT MEASURE

Verified encryption, unique organisations or losses

26

Peru listings for all of 2025

WHAT IT DOES NOT MEASURE

A matched-period baseline

28 of 58

Listings under Qilin, The Gentlemen and Nova labels

WHAT IT DOES NOT MEASURE

Operators, success rates or completed payments

3

Listings dated 8–22 November

WHAT IT DOES NOT MEASURE

Three independently confirmed new intrusions

9 / 10

Illustrated underground dossiers / redacted post cards

WHAT IT DOES NOT MEASURE

Nine confirmed intrusions or ten independent events

5

Public case dossiers, including warnings and an operation

WHAT IT DOES NOT MEASURE

Five confirmed network intrusions

250

Purposively selected domain candidates

WHAT IT DOES NOT MEASURE

Independent legal entities, a revenue ranking or national prevalence

15

Card-record observations in the reviewed post population

WHAT IT DOES NOT MEASURE

Verified validity, ownership or use; national card exposure or fraud losses

Sources: retained post evidence [S1], Ransompedia [S2] and the selected portfolio's observation scope [S3]. The card figure is a narrow retained-post population, not an estimate of national exposure.

KEY TAKEAWAYS

01

Validate the specific account, data or service proposition before declaring impact.

02

Listings, public accounts and post dossiers remain different populations.

03

Assign owners to supplier access, customer protection, continuity and reporting together.

Report map

Twelve chapters, five reader paths. Each chapter opens with a decision question and closes with three takeaways.

Board and executives	Resource validation and service recovery	01 05 11 12
CISO and security leads	Prioritise owned evidence and dependencies	03 04 06 07 12
SOC and identity teams	Test access assertions and endpoint context	04 07 B
Fraud and customer protection	Authenticate requests and reduce secondary harm	05 08 09
Legal and communications	Preserve chronology, scope and reporting decisions	05 06 10 12

The evidence labels are **observation**, **actor claim**, **official account** and **analyst inference**. An observed advertisement remains a claim about its contents. An official account can confirm an event while leaving the actor, entry route or affected population unresolved.

CHAPTER 02

Peru's digital and threat context

02

THIS CHAPTER ANSWERS

Which operating conditions change the response to the evidence in this report?

84.2%

internet penetration in the October 2026 overview

2.1 A connected population creates several identity dependencies 11

2.2 Separate the institution from the service and its supplier 11

2.3 Political context does not supply attribution 12

2.4 Regional peers provide context, not a security league table 12

2.5 Reporting ownership is part of operational readiness 12

CHAPTER 02

Peru's digital and threat context

IN SHORT

Peru combines extensive digital-service use with several distinct security responsibilities. Identity information, public-service access and financial transactions appear in different evidence populations. A website interruption, an illegal data sale and a confirmed account misuse require different response decisions. Regional comparisons describe visibility, while the legal framework separates personal-data incidents from digital-service incidents. Map the service, its identity provider, its data custodian and its reporting owner before choosing containment.

2.1 A connected population creates several identity dependencies

DataReportal's October 2026 overview reports 29.5 million internet users and 84.2% penetration. It also reports 39.6 million mobile connections and 32.7 million social-media user identities. Connections and social identities are not unique people; the publisher cautions about comparability across editions. [S4]

For defenders, these are context figures. They do not measure cybercrime, affected accounts or the reach of a particular advertisement. A country-labelled database offer cannot be divided by internet users to estimate an affected-population percentage.

The practical dependency is between a person, the services that recognise that person and the channels used to recover access. A disclosed identity record may become useful in a later impersonation attempt without giving its holder access to the original institution. This is an analytical risk model, not a finding that the reviewed records caused a particular fraud.

Organisations should therefore map recovery alongside normal authentication. Identify which staff can change a telephone number, approve a new beneficiary, recover a privileged account or issue a replacement credential. Confirm how those actions are independently checked and recorded.

2.2 Separate the institution from the service and its supplier

The incident register distinguishes an institution's internal systems, a supplier account, a public communications channel and the customer-facing service. Evidence about one does not establish access to all the others.

An advertised public-service administrator account requires validation by the service and identity owners. A document mentioning a health provider requires data ownership and provenance checks. A company warning about a false investment video requires customer protection and brand response. Their shared country association does not create a common intrusion chain.

This distinction matters when coordinating suppliers. An organisation may own the public message but depend on another party for identity, hosting or message delivery. The recovery exercise should establish who can suspend a supplier account and who can safely authorise reopening.

2.3 Political context does not supply attribution

This report takes no position on the general elections, presidential successions, Congress, parties, candidates, protests or government decisions. It takes no position on Peru's relations with Chile or Bolivia. Those subjects do not establish an attacker's identity or motive.

A political reference in a post is the author's framing. A language label does not establish nationality. A service outage during a public event does not establish deliberate interference, and a criminal claim does not establish an effect on an election.

The response should use the same evidence standards across political affiliations. Preserve the relevant service record, state what is confirmed, describe what remains unresolved and assign the next verification step. Remove slurs and recruitment appeals when describing actor material.

2.4 Regional peers provide context, not a security league table

The comparison uses Chile, Colombia, Ecuador and Bolivia. Chile and Ecuador provide Pacific regional context; Colombia adds a larger Andean digital-services comparison; Bolivia provides a smaller neighbouring visibility population. The selection does not imply a political grouping or equivalent economies.

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

The listing counts in Chapter 7 are descriptive. Countries differ in population, sector mix, disclosure practice and the sources visible to the reporting service. No observed count establishes a probability of attack or a ranking of national defensive capability.

The same limit applies to posts. An international seller can advertise the same service to many countries. A change in country-associated publication volume does not, without supporting incident evidence, establish a corresponding change in successful intrusions.

2.5 Reporting ownership is part of operational readiness

The Digital Trust Framework regulation became effective during the study window. Personal-data reporting and financial-sector supervision have separate scope and triggers. Chapter 10 distinguishes the duties and their commencement dates. [S5][S6][S7]

Use a shared incident record for the facts, but record each reporting determination separately. Awareness, detection, publication and restoration can happen on different dates. The same incident can require technical assistance, privacy assessment, customer communication and a police complaint without becoming several intrusions.

For a board, the useful question is whether the organisation can make these decisions before the relevant deadline. For a service owner, it is whether a minimum safe service can operate while the investigation continues. For an analyst, it is whether each conclusion still has the same evidence label when it reaches the summary.

KEY TAKEAWAYS

01

Connections, accounts, records and people have different denominators.

02

Supplier access and public messaging need their own response owners.

03

Political context and regional comparison do not establish attribution or national risk rankings.

CHAPTER 03

National exposure: the selected organisation portfolio

03

THIS CHAPTER ANSWERS

Which portfolio observations are available, and which require an owned-asset validation decision?

250

selected domain candidates across ten merged sector groups

3.1 Universe card 15
3.2 Available exposure results 16
3.3 Credential validation should preserve the proposition tested 18
3.4 Email and web controls need observation-specific denominators 18
3.5 A preventive software warning is not an incident count 20
3.6 Integration and interpretation boundaries 21

CHAPTER 03

National exposure: the selected organisation portfolio

IN SHORT

The portfolio contains 250 purposively selected domain candidates. It is not a national prevalence sample or a revenue ranking. Domain ownership, related services and independent legal identity require validation. A credential was advertised for 68 of the 250 candidates; current access requires validation. Treat unavailable observations as unknown, and use validated account alerts and local service records to decide whether containment is warranted.

3.1 Universe card

Item	Definition
Selected population	250 domain candidates across 10 merged sector groups
Selection	Public-service relevance and sector coverage; not a ranking by revenue
Planned cells	25 candidates per sector group; published observations require a usable denominator
Unit	Domain candidate, which may represent a related service or multinational organisation
Independence	Legal ownership and independent-entity status remain unvalidated
Exposure snapshot	Current account offers and cumulative domain associations require their own observation date
Representativeness	Results cannot estimate national prevalence or sector incident probability
Ratings	Only a validated national Atlas headline may be reported

The sectors cover central administration, regional administration, finance and insurance, universities and research, energy and water, mining and materials, transport and logistics, consumer services, health, and communications, agriculture and industry. Smaller operating categories are merged. Candidate allocation is not a measured security result.

3.2 Available exposure results

At the 22 November check, 68 of the 250 selected domain candidates had a credential listed for sale. This is an advertised offer, not verified current access. The selected domains require ownership and independence validation before organisation-level conclusions. [S3]

National Atlas headline for the selected portfolio



49/100 summarises this selected portfolio, not national attack probability or incidence. Source: Odin by Brandefense, 250 selected domain candidates, 22 November 2026 [S3]. Associations can overlap and include older observations.

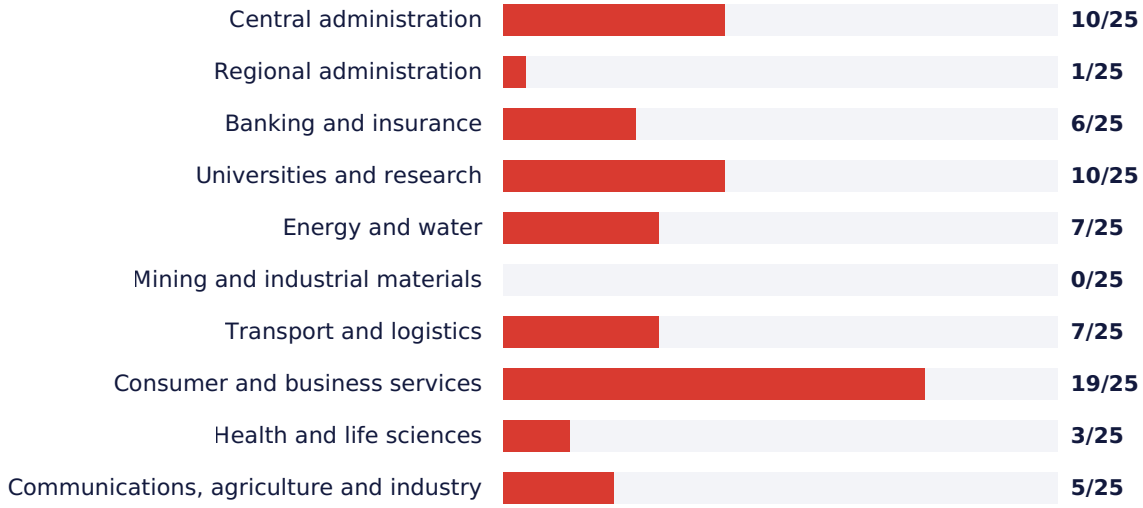
The national Atlas headline for this selected portfolio is 49/100. It is a portfolio exposure summary, not a national attack probability or an incidence rate. No sector or organisation rating is published. [S3]

Portfolio observation	Count	Interpretation
Domains with device associations	231	Not verified organisational device ownership
Device associations	747,185	At least this many cumulative associations; overlap can occur
Domains with employee-labelled device associations	208	Upstream role label, not validated employment
Employee-labelled device associations	83,414	Overlapping associations, not unique staff
Domains with credential-record associations	233	Historical and current relevance require validation
Credential-record associations	4,429,470	Not unique accounts or people
Document associations	887	Not a finding that every document is confidential
Candidate lookalike associations	13,105	Not verified phishing or brand abuse

These figures are domain associations, not unique devices, accounts, documents or people. Counts can overlap across records and related domains. They are not a 2026-only incident population. The snapshot was assembled on 22 November; some association periods end on 18 November. Candidate lookalikes cover 19 October–18 November. [S3]

Sector signal counts require validation and do not constitute sector risk ratings

Current credential listings by sector (coral)



Domain candidates with a credential advertised / selected candidates. Current access is not verified; no sector risk rating is published. Source: Odin by Brandefense, 250 selected domain candidates, 22 November 2026 [S3]. Associations can overlap and include older observations.

Selected sector group	Candidates	Credential listed for sale	Domains with device associations	Credential-record associations
Central administration	25	10	25	143,467
Regional administration	25	1	25	13,489
Banking and insurance	25	6	24	87,730
Universities and research	25	10	25	3,815,424
Energy and water	25	7	22	39,841
Mining and industrial materials	25	0	20	54,536
Transport and logistics	25	7	24	35,352
Consumer and business services	25	19	24	68,087
Health and life sciences	25	3	19	32,363
Communications, agriculture and industry	25	5	23	139,181

Each sector cell contains 25 candidates. Downloadable listing counts describe domain candidates with advertised credentials, not organisations offered for sale or verified current access. Employment labels are upstream labels, not validated employment. The groups partition selected domains, not independently validated legal entities. Their signal counts do not establish sector prevalence or a comparative risk ranking. [S3]

These populations would answer different questions. A current offer says that a login is advertised. A historical credential association may concern an old or remediated account. A device association does not establish employment, ownership or access to the organisation's internal systems.

When a relevant alert is available, validate the asset and account first. Confirm that the service belongs to the organisation, identify whether the account is staff, supplier, student or customer related, and inspect its status. Avoid treating a domain-wide association as a verified employee incident.

3.3 Credential validation should preserve the proposition tested

A useful record separates four questions: whether the material concerns an owned service, whether the account remains active, whether unauthorised use occurred and whether prior remediation already addressed it. A positive answer to one does not answer the others.

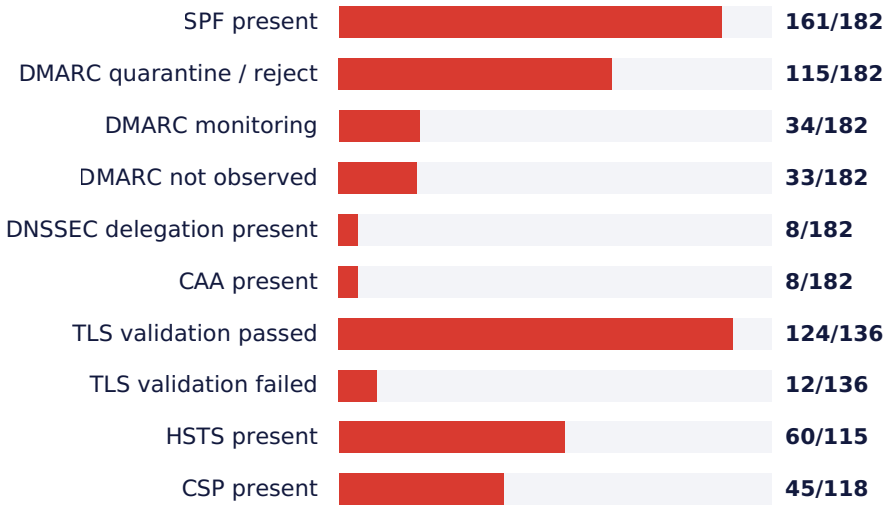
For a current privileged account, the identity team should review sign-ins, session grants, added authentication methods and administrative changes. Containment should follow validated evidence. Reopening should include a check that revoked access is ineffective, rather than relying on a password-change receipt alone.

For historical or unrelated material, record the reason and close the alert at the appropriate scope. A documented historical disposition is more useful than an unbounded breach declaration. Unresolved cases need an owner and a next review time.

3.4 Email and web controls need observation-specific denominators

See Appendix D for definitions of SPF, CAA and TLS.

Passive control observations use separate available denominators



Source: passive observations, 22 November 2026 [S3]. Available denominators differ by observation; policies do not demonstrate effectiveness.

The 250 candidate domains yielded passive observations for 183; 67 have no usable domain result. DNS results are usable for 182, with one incomplete result. These populations describe the selected portfolio on 22 November, not national control prevalence. Domain ownership and independent organisation identity remain unvalidated. [S3]

Observation	Observed count	Available denominator
SPF record present	161	182
DMARC quarantine or reject policy	115	182
DMARC monitoring policy	34	182
No DMARC policy observed	33	182
DNSSEC delegation record present	8	182
CAA record present	8	182
TLS certificate validation passed	124	136
TLS certificate validation failed	12	136
HSTS present on an available HTTPS response	60	115
Content Security Policy present on an available web response	45	118

Source: Odin by Brandefense [S3]. The DMARC categories total 182. TLS has 136 determinate results and 47 unknown results among the 183 observed domains. Web responses are available for 118 domains, including 115 HTTPS responses. Unavailable responses are unknown, not missing controls.

A failed certificate validation is an observation requiring owned verification, not a finding of intrusion. A published mail policy does not establish correct alignment across every sender. A DNS delegation or web header does not establish full implementation quality or application security.

Review authorised senders before tightening mail policy. Validate certificate findings against the intended service and supported trust path. Test web-policy changes against legitimate application workflows. Retain an owner and a reason for every unavailable result rather than counting it as a security failure.

Email authentication, certificate validity and web headers are configuration observations. They do not measure whether phishing succeeded or whether information was stolen. A missing observation does not establish a missing control, and a successful homepage response does not establish complete service availability. [S3]

For email, the owner should inventory legitimate senders and test alignment before changing enforcement. For certificates, confirm the service endpoint, the certificate chain and the deployment process. For web controls, verify the effective behaviour of the application and its dependencies.

A local configuration review remains useful when the external dataset is incomplete. The organisation can test authorised mail paths and service workflows directly. The national report should not replace those results with a sector ranking inferred from selected domains.

3.5 A preventive software warning is not an incident count

The official newspaper reports a CNSD preventive PHP warning issued on 21 October and described on 26 October. Its institutional distribution figures do not establish exploitation or affected organisations. Owners should review actual deployments. [S11]

Both cited PHP vulnerabilities have NVD records. The vendor advisories identify the following affected and fixed versions for their respective supported branches. These are global vulnerability facts, not evidence of exploitation in Peru. [S12][S13][S14][S15]

Vulnerability	Branch	Affected versions	Vendor fixed version
CVE-2026-109618 and CVE-2026-109619	8.2	Before 8.2.35	8.2.35
Same two vulnerabilities	8.3	Before 8.3.36	8.3.36
Same two vulnerabilities	8.4	Before 8.4.27	8.4.27
Same two vulnerabilities	8.5	Before 8.5.12	8.5.12

Verify the version actually running after remediation. For software supplied by a distributor or appliance vendor, follow that provider's applicable advisory and supported update route. A completed package change without a deployment check is not a demonstrated service fix.

3.6 Integration and interpretation boundaries

Any later exposure snapshot must preserve its own date and denominator. Cumulative records should remain separate from the report's post-time window. Related domains and overlapping records must not become unique-person or independent-organisation totals.

Sector signal counts can support triage, while the national Atlas headline provides a separate portfolio summary. This report does not publish sector or organisation ratings. A passive hygiene index, if supported, would be labelled an analytical index rather than an Atlas result.

The response queues should remain distinct: account validation, endpoint investigation, customer protection, document review and configuration remediation. Each requires a responsible team, supporting evidence and a closure condition. An aggregate count cannot decide which individual system should be disconnected.

KEY TAKEAWAYS

01

The selected portfolio is a domain-based descriptive population.

02

Unavailable exposure observations remain unknown rather than zero.

03

Validate ownership, account status and actual use before choosing disruptive containment.

CHAPTER 04

Underground activity and claim interpretation

04

THIS CHAPTER ANSWERS

What do the retained posts establish, and which propositions still require validation?

9

illustrated claim dossiers, supported by ten post cards

4.1 Universe card 23

4.2 A visible recycling dispute 27

4.3 Advertised access and organisational documents 28

4.4 Recent activity: 8–22 November 32

4.5 Additional themes and exclusions 35

4.6 Validation questions that change a response 37

CHAPTER 04

Underground activity and claim interpretation

IN SHORT

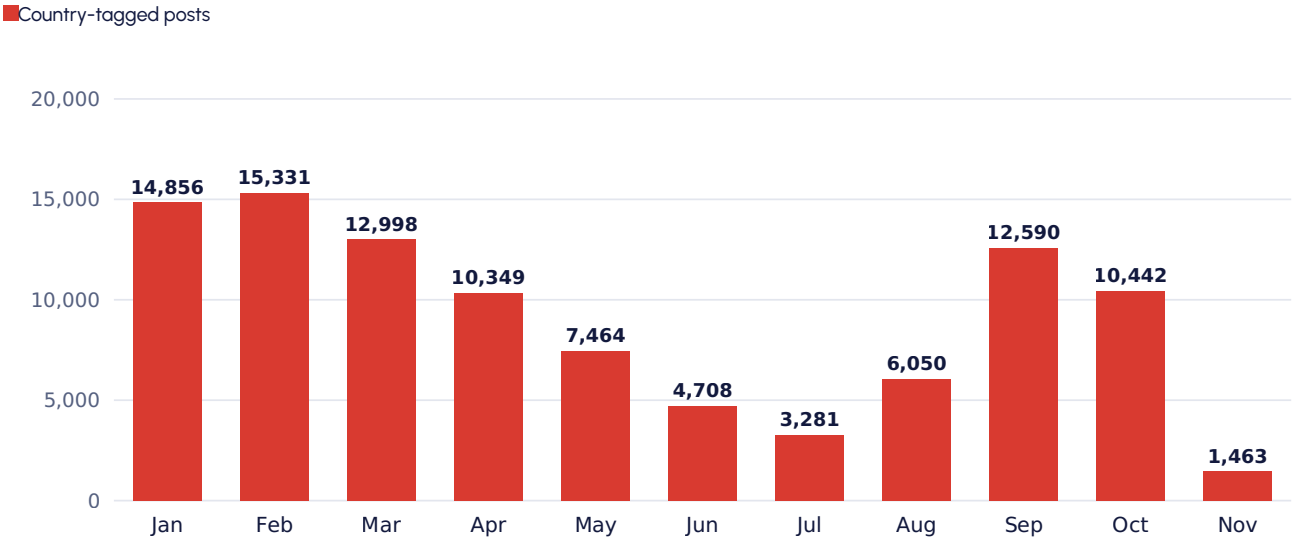
The retained posts advertise identity records, public-service access, health documents, retail access and education data. Nine dossiers separate those assertions from verified outcomes. A January discussion identifies older material; November offers describe distinct public-record and education themes. Repeated messages and matching field lists do not establish new intrusions or identical files. Route each relevant alert to the owner who can validate its origin, account status, data categories and actual service effect.

4.1 Universe card

Item	Meaning
Window	1 January–22 November 2026, by post time
Country association	Peru can be a claimed origin, sales market, customer group or incidental reference
Evidence population	Retained messages, including forum advertisements and discussion
Illustrated dossiers	9, with 10 redacted post cards
Claim status	Publication establishes the assertion, not its accuracy
Completeness	The retained content does not form a national incident census
Ransomware	A separate population of 58 listings in Chapter 7

The report keeps observed publication, claimed possession, usable access, completed sale and independently confirmed incident separate. A field list can be plausible while its claimed origin, age and quantity remain unresolved. A buyer's request does not establish that anyone supplied the requested material. [S1]

Monthly country-tagged publication volumes do not measure successful intrusions



Source: Odin by Brandefense, Peru-tagged posts, 1 January–22 November 2026; November partial [S1]. Tagged posts are not incidents.

Month	Tagged posts
2026-01	14,856
2026-02	15,331
2026-03	12,998
2026-04	10,349
2026-05	7,464
2026-06	4,708
2026-07	3,281
2026-08	6,050
2026-09	12,590
2026-10	10,442
2026-11	1,463
Total	99,532

Source: Odin by Brandefense [S1].

Telegram carries most observed country-tagged posts



Source: Odin by Brandefense, Peru-tagged posts, 1 January–22 November 2026; November partial [S1]. Tagged posts are not incidents.

Platform	Tagged posts
Telegram	99,076
Forum	430
Discord	9
Paste	17
Tor	0

The platform sum is 99,532. It matches the monthly post total. [S1]

Selected language associations; non-exhaustive and potentially overlapping



Selected language associations are non-exhaustive and potentially overlapping. Source: Odin by Brandefense, Peru-tagged posts, 1 January–22 November 2026; November partial [S1]. Tagged posts are not incidents.

Language association	Tagged posts
Spanish	64,021
English	11,438
Portuguese	85
Russian	1,509

Selected language associations are non-exhaustive and potentially overlapping. They do not establish nationality, residence or a domestic victim count. [S1]

Regional post volumes are visibility context rather than a country risk ranking



Counts describe visibility; they are not adjusted for country size or source coverage. Source: Odin by Brandefense, Peru-tagged posts, 1 January–22 November 2026; November partial [S1]. Tagged posts are not incidents.

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

Country	Tagged posts
Peru	99,532
Chile	27,891
Colombia	776,338
Ecuador	11,000
Bolivia	6,263

Source: Odin by Brandefense [S1]. Country sizes, source visibility and international advertising differ. No national attack probability is inferred.

The descriptive post observations measure visibility. Changes can reflect publication behaviour and source coverage. They do not establish changes in successful attacks, losses or national defensive capability. The closing month and cut-off day are partial. [S1]

4.2 A visible recycling dispute

A

CASE A

Citizen-record advertising and a repost correction (B01, B02)

Public-record themes

Claim unverified

CLAIM	A 7 January forum advertisement describes identity and contact fields in a Peru-associated citizen dataset. It includes an asserted national-scale quantity, which this report does not treat as measured people. [S1]
CHRONOLOGY	Other participants describe the material as older and give different years. One asks for a repost label; the original poster subsequently says the title was renamed. The sequence supports a visible correction discussion.
ESTABLISHED	The advertisement and dispute were published. The record does not independently establish file identity, a particular acquisition year, the original source or a new intrusion during January.
ALTERNATIVES	Older data may be repackaged, copied or combined. A correct-looking field list is also consistent with a historical export. The discussion cannot select a verified year from competing participant assertions.
RESPONSE	The data custodian should compare a relevant authorised alert with earlier disclosures and remediation. Preserve the difference between a new publication and a newly established security event.

Bottom line

The data custodian should compare a relevant authorised alert with earlier disclosures and remediation. Preserve the difference between a new publication and a newly established security event.

Evidence card B01	7 Jan 2026
[alias withheld] · Forum · Forum · English	
ORIGINAL: Data : DNI, full names, birth date, age, address, location, phones, civil status	
Held: A citizen-record advertisement describes identity and contact fields.	
Not established: File authenticity, source, age, a new intrusion, unique people or completed transfer.	

Evidence card B02	7 Jan 2026
[alias withheld] · Forum · Forum · English	
ORIGINAL: Just rename the thread as a REPOST with the correct title.	
Held: A participant asks for a repost label after others describe older material.	
Not established: Underlying file identity, verified acquisition date, or a confirmed 2026 intrusion.	

This case changes the chronology decision. A fresh advertisement is a current publication event. It may still matter for impersonation, but it does not reset the underlying theft date. Nor does a forum participant's recognition prove that the offered file is byte-identical to an earlier release.

A useful response record should state what matched: a title, field list, authorised sample, historical notice or confirmed owned record. Each provides a different level of support. The report does not describe an underlying file comparison or an acquisition from the seller.

4.3 Advertised access and organisational documents

CASE B

B

Privileged access advertised for a public-service portal

Evidence card B03 · 10 Feb 2026 · Forum · Public services

Claim unverified

CLAIM	A 10 February post advertises root, firewall and network-administration access for a public-service portal. The seller asks 200 USD. Those are advertised capabilities and an asking price, rather than validated access or transaction value. [S1]
ESTABLISHED	The source describes a privileged-access proposition. It does not establish a working account, the current owner, an exploitable vulnerability or an effect on public services.
ALTERNATIVES	Access may be stale, misrepresented, restricted to a supplier environment or advertised without possession. A panel description does not establish reach into every system connected to the public-facing service.

RESPONSE	An authorised service owner should validate the claimed asset and account, then examine remote administration, privileges, sessions and changes. Contain only the access supported by the organisation's evidence.

Bottom line

An authorised service owner should validate the claimed asset and account, then examine remote administration, privileges, sessions and changes. Contain only the access supported by the organisation's evidence.

CASE C

C

Health-related documents offered for publication

Evidence card B04 | 16 Feb 2026 | Forum | Health

Claim unverified

CLAIM	A 16 February forum post asserts publication of a regional health body's documents. It describes ordinary office-document formats. The underlying documents and their asserted volume remain unverified. [S1]
ESTABLISHED	The post records a document-publication claim. It does not establish patient impact, an intrusion route, current access or an affected-person count. A later reply about access to the advertised material does not verify its authenticity.
ALTERNATIVES	The material may be historical, supplier-held, public or inaccurately described. Naming a health organisation in a document does not establish access to clinical systems.
RESPONSE	The data custodian should establish relevant document categories and ownership through an authorised alert. Clinical leaders should assess continuity independently of the document claim.

Bottom line

The data custodian should establish relevant document categories and ownership through an authorised alert. Clinical leaders should assess continuity independently of the document claim.

Evidence card B03 — 10 Feb 2026

[alias withheld] | Forum | Forum | English

ORIGINAL

Permissions: Root RCE + Shell + Network Admin Panel

Held

A seller advertises privileged firewall and portal access. The seller claims remote code execution, highest-level privileges and command-line access; none is validated.

Not established

Usable current access, ownership, a verified exploit, completed sale or operational impact.

Evidence card B04 — 16 Feb 2026

[alias withheld] | Forum | Forum | English

ORIGINAL

Type of documents: XLSX, PDF, DOCX, and so on

Held

A post asserts publication of a regional health body's documents.

Not established

Authenticity, patient impact, a new intrusion, current access or verified volume.

CASE D

D

Benefit-related records offered for sale

Evidence card B05 | 4 Mar 2026 | Forum | Public services

Claim unverified

CLAIM	A 4 March advertisement describes identity, birth-date, contribution-period and employment-period fields associated with benefit administration. Claimed record and beneficiary quantities remain unverified and are not reproduced as affected people. [S1]
ESTABLISHED	The field categories and sales assertion appear in the post. The evidence does not establish the underlying source, acquisition date, unique beneficiaries, present access or a completed sale.
ALTERNATIVES	Historical administrative exports or overlapping records could explain the claimed material. An institution's role in benefit administration does not establish that its central system was the acquisition point.
RESPONSE	The custodian should compare the categories with its own records and notices. Customer-protection teams should independently authenticate requests to change benefit payments or identity details.

Bottom line

The custodian should compare the categories with its own records and notices. Customer-protection teams should independently authenticate requests to change benefit payments or identity details.

CASE E

E

Retail account access and operational documents

Evidence card B06 | 27 Mar 2026 | Forum | Retail

Claim unverified

CLAIM	A 27 March advertisement offers login and password access and describes retail operational documents. The asking price is 20,000 USD, negotiable. Some document dates described in the post predate the study year. [S1]
ESTABLISHED	The offer combines an access assertion with document advertising. It does not establish present privilege, a company-wide intrusion, document authenticity or any completed transaction.
ALTERNATIVES	An old export, a supplier account, a limited application role or inaccurate advertising could produce the same description. The price does not validate the claim.
RESPONSE	Identity and business owners should establish account ownership, current status and scope. Finance should independently authenticate payment or supplier changes if relevant operational records are validated.

Bottom line

Identity and business owners should establish account ownership, current status and scope. Finance should independently authenticate payment or supplier changes if relevant operational records are validated.

Evidence card B05 — 4 Mar 2026

[alias withheld] | Forum | Forum | English

ORIGINAL

Type of data: national ID, last name, name, birth date, contribution period, employment period

Held

A post offers records described as relating to benefit administration.

Not established

Authenticity, unique beneficiaries, acquisition date, current access or completed sale.

Evidence card B06 — 27 Mar 2026

[alias withheld] | Forum | Forum | English

ORIGINAL

Selling LOGIN AND PASSWORD

Held

A seller advertises access and describes retail operational documents.

Not established

Valid access, present privilege, authentic documents, completed sale or company-wide intrusion.

The two access advertisements describe different scopes and prices. They do not establish a representative market-price range. An asking price can reflect negotiation, packaging or a seller's unsupported assertion. The report estimates neither sales revenue nor the cost of a successful intrusion.

4.4 Recent activity: 8–22 November

The following four dossiers fall inside the recent window by retained post time. Their publication dates do not establish when any underlying data was obtained. A related official response belongs beside the relevant proposition, rather than being treated as confirmation of every detail. [S1]

CASE F

F

Business-registration fields presented as a new leak

Evidence card B07 | 8 Nov 2026 | Forum | Public-record themes

Claim unverified

CLAIM	An 8 November group-branded post describes business-registration fields and presents their publication as a leak. It uses the MortemTeam label. Group branding does not independently establish the poster's identity or responsibility. [S1]
ESTABLISHED	The field list includes business identifiers, legal names, status and addresses. The post does not establish non-public provenance, unauthorised system access, fresh theft or a verified business population.
COUNTERPOINT	Public reporting relays a public-sector body's denial of internal intrusion or extraction and its dispute of the claimed provenance. This remains the responding body's assessment, not independent file validation. [S27]
ALTERNATIVES	Public or historical registry material could be represented as a new intrusion. That remains an alternative; this report has not established that the advertised file matches a specific public dataset.
RESPONSE	Establish whether a relevant alert contains genuinely non-public information and evidence of unauthorised access. Preserve the actor assertion, authority response and unresolved file provenance as separate propositions.

Bottom line

Establish whether a relevant alert contains genuinely non-public information and evidence of unauthorised access. Preserve the actor assertion, authority response and unresolved file provenance as separate propositions.

CASE G

G

Student, guardian and attendance records

Evidence card B08 | 13 Nov 2026 | Forum | Education

Claim unverified

CLAIM	A 13 November group-branded post alleges student, guardian and attendance data from an education provider. It also asserts a technical entry route, which is not validated here. The actor's political taunt is omitted. [S1]
ESTABLISHED	The record describes several data categories. Student, guardian and attendance quantities are different units and cannot be added into an affected-person figure. The post does not establish a successful intrusion or a working vulnerability.
ALTERNATIVES	The advertised information may be historical, overlapping, supplier-held or inaccurately described. Shared branding with another post does not establish the same operator or acquisition event.
RESPONSE	An authorised owner should examine application access and relevant logs. If actual records are validated, involve privacy and safeguarding teams to scope any children's information and appropriate communication.

Bottom line

An authorised owner should examine application access and relevant logs. If actual records are validated, involve privacy and safeguarding teams to scope any children's information and appropriate communication.

Evidence card B07 — 8 Nov 2026

[alias withheld] | Forum | Forum | English

ORIGINAL

Data Included: [business identifier], Legal Name, [registration status fields], Address

Held

A post describes business-registration fields and presents their publication as a leak.

Not established

Non-public provenance, unauthorised system access, fresh theft, unique businesses or verified volume.

Evidence card B08 — 13 Nov 2026

[alias withheld] | Forum | Forum | English

ORIGINAL

Data Included: full student roster - DNI, names, date of birth, sex, level, grade, section, home address

Held

A group-branded post claims student, guardian and attendance records from an education provider.

Not established

A verified vulnerability, authentic records, affected-student totals or successful intrusion.

CASE H

H Education-management information and account access

Evidence card B09 | 16 Nov 2026 | Forum | Education

Claim unverified

CLAIM	A 16 November Spanish-language offer combines administrator or director information with account access to an education-management platform. It describes identity, contact and photo-related fields. [S1]
ESTABLISHED	The advertisement makes both a data assertion and an access assertion. It does not establish working credentials, present privilege, platform ownership, authentic data or a new intrusion.
ALTERNATIVES	The information and the account may have different ages or origins. A password in an offer does not establish that the account remained valid when the post was published.
RESPONSE	Validate ownership, account status and privilege. Scope relevant personal data separately and revoke access when owned-system evidence supports that action.

Bottom line

Validate ownership, account status and privilege. Scope relevant personal data separately and revoke access when owned-system evidence supports that action.

CASE I

I Employment-history records and account-related fields

Evidence card B10 | 20 Nov 2026 | Forum | Public services

Claim unverified

CLAIM	Two 20 November forum observations carry matching substantive advertising for employment histories and related personal information associated with a public-service body. They differ in forum-rendering details. [S1]
ESTABLISHED	Matching advertising was published. It does not establish identical underlying files, two independent intrusions, unique people, working accounts or a completed sale.
ALTERNATIVES	The observations may reflect a repeat advertisement or an overlapping historical export. Personal-information and account-field descriptions do not establish that any advertised account could be used.

RESPONSE

The custodian should validate categories and freshness. Identity and fraud teams should separately assess actual account use and payment-change evidence.

Bottom line

The custodian should validate categories and freshness. Identity and fraud teams should separately assess actual account use and payment-change evidence.

Evidence card B09 — 16 Nov 2026

[alias withheld] | Forum | Forum | Spanish

ORIGINAL

ACCESO A UNA DE SUS PLATAFORMAS DE GESTION POR USUARIO Y CONTRASEÑA

TRANSLATION

Access to one of its management platforms using a username and password.

Held
A post combines an education-management data offer with an account-access assertion.

Not established
Working credentials, present privilege, authentic data, ownership or a new intrusion.

Evidence card B10 — 20 Nov 2026

[alias withheld] | Forum | Forum | Spanish

ORIGINAL

TIPO DE USUARIO, TIPO DE CONTRATO, NOMBRES, APELLIDOS, ESTADO DE ACTIVIDAD

TRANSLATION

User type, contract type, first names, surnames, activity status.

Held
A post advertises employment-history records and account-related fields for a public-service body.

Not established
Authenticity, unique people, a new intrusion, valid accounts or completed sale.

4.5 Additional themes and exclusions

Publication period	Retained assertion	Disposition and useful decision
January	Telecom-customer records discussed in a forum quotation	Mention; quoted discussion is not an independently established telecom intrusion
April	Official-document offer, with some material described as older	Mention; validate categories and chronology before assigning a new event
April–May	Telecom-subscription datasets with similar field descriptions	Mention; similarity does not establish file identity or separate intrusions
June and October	Parcel-delivery data narrative in forum replies	Mention; later publication is not independent confirmation
August	Food-service customer data described as older material	Mention; distinguish a later offer from the acquisition date

Publication period	Retained assertion	Disposition and useful decision
October	Health-related records with unresolved origin	Mention; privacy scoping depends on validated records
October	Education-directory records advertised as a leak	Mention; public-directory provenance is a plausible alternative
November	Training and tax-document claims	Mention; personal samples and technical assertions remain unverified
November	Justice-related lookup service asserted	Mention; no access test or working route is published
14 November	Defacement-feed relay names a Peru-associated site	Mention; appearance in a relay does not establish independently verified impact
15 November	A request explicitly seeks point-of-sale services in Peru	Demand observation; no acquisition, working service or completed transaction established
22 November	A lookup-bot response displays identity-field output	Mention; provenance, freshness and source-system access unverified
Across the window	International card, proxy, SMS and account-service catalogues include Peru	Visibility context; no domestic intrusion inferred
Across the window	Requests for contact lists or login pairs	Demand observation; possession and fulfilment unestablished
Across the window	Courtesy replies and content-unlock messages	Excluded as corroboration of the underlying incident claim

Source: retained post evidence [S1]. These rows are themes rather than an additional confirmed-incident total. A single discussion can generate several retained messages, and several advertisements can describe overlapping material.

4.6 Validation questions that change a response

Proposition	Evidence needed from an authorised owner	Decision it can support
The data belongs to this institution	Reliable ownership and content match	Scope the relevant data and notification assessment
An offered account remains active	Account status, privilege and sign-in records	Contain the validated access and sessions
The advertisement describes a new event	Chronology beyond the new posting date	Open a new incident or link a historical disclosure
A technical route was used	Owned application and system evidence	Fix the demonstrated weakness and scope access
Two posts describe the same material	More than matching titles or quantities	Avoid duplicate counting while retaining uncertainty
A public service was disrupted	Service and user-task evidence	Activate the appropriate continuity plan

The report does not acquire advertised files, purchase access or contact sellers. Its case assessments concern the retained evidence and public corroboration. A stronger conclusion would require evidence of the specific proposition, not a more confident reading of the same advertisement.

KEY TAKEAWAYS

01

Nine dossiers preserve different claims rather than nine confirmed intrusions.

02

The recent window includes publication events with unresolved acquisition dates.

03

Matching advertisements, plausible fields and asking prices do not validate possession, access or completed sales.

CHAPTER 05

Public incidents and sector response

05

THIS CHAPTER ANSWERS

Which public accounts establish an event, and how should each sector respond?

5

public case dossiers with different evidence and incident units

5.1 Reading and counting rules 39
5.2 Supplier-account access and public messaging 39
5.3 Insurance: information access without significant service interruption 40
5.4 Health: payment authority and clinical continuity 41
5.5 Official fraud warnings and enforcement 42
5.6 Additional source-read campaigns, denials and exclusions 43
5.7 Sector decisions without sector risk scores 44

CHAPTER 05

Public incidents and sector response

IN SHORT

Public accounts support distinct decisions about supplier access, insurer customer information, unauthorised transfers, brand impersonation and alleged illegal data sales. The five dossiers are not five confirmed network intrusions. Keep the organisation's established facts separate from criminal quantities and technical speculation. Choose containment, customer protection, payment review or investigative support according to the specific evidence, while maintaining essential services.

5.1 Reading and counting rules

The dossiers below include three reported security or fraud events, an official impersonation warning and an enforcement operation. They are not a national incident count. The nine underground dossiers in Chapter 4 are separate claim assessments and are not added to these events. [S17][S18][S23][S20][S22]

A confirmation can establish access or a disputed transfer without establishing a perpetrator, entry route or final affected population. An organisation's statement reproduced by the press is attributed accordingly. An authority's denial is a source position, rather than independent proof about an offered file.

Names are used only when official confirmation and wider reporting support them. Otherwise the target is described by a broad role. Article addresses that would restore a withheld victim's name are cited at the publisher's root, with the article URL withheld.

5.2 Supplier-account access and public messaging

J

CASE J

Unauthorised messages through a public-alert service

Publicly reported case

Source account; limits retained

REPORTED CONFIRMATION	On 20 May, the responsible authority said a supplier account was used without authorisation to send false emergency messages. Latina Noticias reproduces the authority's statement. [S17]
BOUNDARY	The account does not establish a DDoS mechanism, a political operator, wider internal access or a relationship to the February portal advertisement. Later stories describing the May event are not new intrusions.

INTERPRETATION	The ability to issue trusted public messages is a critical privilege. Service availability and message integrity need separate assurance before reopening.
RESPONSE	The service owner should inventory message-issuance privileges, test supplier-account suspension, preserve authorisation records and rehearse a trusted correction channel.

Bottom line

The service owner should inventory message-issuance privileges, test supplier-account suspension, preserve authorisation records and rehearse a trusted correction channel.

The practical exercise should begin with an unauthorised message rather than an assumed encrypted server. Establish who can stop further issuance and who can approve a legitimate correction. Test whether the process still works when the usual supplier contact or administrator is unavailable.

Supplier oversight should also preserve the difference between account ownership and organisational responsibility. The authority's account identifies the relationship through which access occurred. It does not establish that the supplier's entire environment was accessed or that all of its customers were affected.

5.3 Insurance: information access without significant service interruption

K

CASE K

Customer-information access at an insurer

Publicly reported case

Source account; limits retained

REPORTED CONFIRMATION	The insurer told El Comercio that it detected unauthorised customer-information access on 7 October. The supervisor confirmed that it had been notified and was following the incident. [S18][S19]
BOUNDARY	Detection is not the intrusion-start date. The number of affected customers, entry route and final scope remained unresolved in the cited account. A criminal volume assertion is not adopted here.
INTERPRETATION	Normal service operation and a confidentiality incident can coexist. A service-restoration milestone does not close personal-data scoping or customer support.
RESPONSE	Establish the actual data categories, preserve the awareness timeline and maintain scoped customer guidance while investigation continues.

Bottom line

Establish the actual data categories, preserve the awareness timeline and maintain scoped customer guidance while investigation continues.

This case changes a common decision shortcut. Teams should not use the absence of a major outage to close an information-access assessment. The privacy record should identify the actual categories established and the remaining questions, with an owner for each update.

A supervisor's receipt of a report does not independently validate every actor assertion. It establishes the supervisory process described by the source. The report does not attribute the incident to a particular operator merely because a leak-site label subsequently named the organisation.

5.4 Health: payment authority and clinical continuity

CASE L

L

Unauthorised transfers reported by a health-service network

Publicly reported case

Source account; limits retained

REPORTED CONFIRMATION	The institution reported five transfers it did not recognise as authorised, dated 14 August and totalling S/1,406,991. Two outlets reproduce its account. [S23][S24]
BOUNDARY	The source does not establish the technical entry route, a bank-system intrusion or the responsible person. The reported amount is specific to these transfers, not a national cybercrime-loss estimate.
INTERPRETATION	Payment authorisation, evidence preservation and clinical continuity need separate owners. A complaint is not a conviction, and a claim against a financial counterparty does not establish that counterparty's systems were accessed.
RESPONSE	Treasury should preserve payment records, review approvals and beneficiary changes, and coordinate an evidence-based recall or recovery request through trusted banking contacts.

Bottom line

Treasury should preserve payment records, review approvals and beneficiary changes, and coordinate an evidence-based recall or recovery request through trusted banking contacts.

Health leaders should also maintain continuity when finance access is restricted. Identify critical payments and the approvals needed to continue safe services. Reopening a payment workflow should demonstrate valid authorisation and an auditable exception process.

The health-document claims in Chapter 4 and the health-related ransomware listings in Chapter 7 are separate populations. No common actor, shared dataset or causal connection to these transfers is established.

5.5 Official fraud warnings and enforcement

CASE M

M

Petroperú warns about a manipulated investment video

Publicly reported case

Source account; limits retained

OFFICIAL ACCOUNT	On 12 June, Petroperú warned that a video manipulated an executive's voice and image to promote an investment scheme that the company said did not exist. Wider reporting followed. [S20][S21]
BOUNDARY	The warning does not establish access to the company's systems, an affected-investor count or a quantified loss.
INTERPRETATION	A believable executive image can create a verification problem for customers without a network intrusion at the impersonated company.
RESPONSE	Publish the legitimate investment and payment process, give customers an independent verification route and brief customer-facing staff on the specific deception.

Bottom line

Publish the legitimate investment and payment process, give customers an independent verification route and brief customer-facing staff on the specific deception.

CASE N

N

An operation against alleged illegal personal-data sales

Publicly reported case

Source account; limits retained

OFFICIAL ACCOUNT	A 3 July identity-authority notice describes a joint police operation on 29 June involving alleged sales of personal information and false certificates. It records investigative action and seized material. [S22]
BOUNDARY	

The notice does not establish a new intrusion into the authority's core database or a conviction. A data-selling allegation, an access allegation and a proven source-system event remain different propositions.

INTERPRETATION	Data protection extends beyond a central-system intrusion investigation. Distribution, impersonation and document verification can require separate action.
RESPONSE	Preserve relevant reports through authorised channels, verify documents at their legitimate source and distinguish proven facts from the investigation's allegations.

Bottom line

Preserve relevant reports through authorised channels, verify documents at their legitimate source and distinguish proven facts from the investigation's allegations.

5.6 Additional source-read campaigns, denials and exclusions

Publication	Source account	Treatment in this report
February	Financial supervisor publishes a phased open-finance roadmap [S29]	Regulatory context, not implemented controls or a security incident
April	Financial supervisor announces sanctions-framework changes [S30]	Regulatory context; no penalty amount or case outcome inferred
August	Official newspaper relays a transport-fine and QR impersonation warning [S26]	Fraud campaign context; reported complaints are not confirmed intrusions
September	Public news agency reports 42,161 prosecutor computer-crime complaints in 2024, 42,980 in 2025 and 29,118 in January–July 2026 [S25]	Complaint population (matched 2024–2025 annual totals and partial-year 2026), separate from posts, listings and confirmed intrusions
November	Identity-service notices attribute interruption to an electrical event [S34]	Continuity context; excluded from the hostile cyberattack count
November	Regulatory discussion revisits a bank's earlier incident [S28]	Historical follow-up; no new 2026 intrusion inferred
August	A public investigation covers state data-security events across 2020–2026 [S35]	Multi-year context; not a 2026 event total

The September public news agency report of Ministerio Público statistics records 42,161 computer-crime complaints in 2024, 42,980 in 2025 and 29,118 for January–July 2026 [S25]. The matched full-year totals rose slightly from 2024 to 2025, while the 2026 count covers seven months and remains separate from underground posts, ransomware listings and confirmed intrusions.

The November identity-service interruption also falls outside the recent window. A story's publication date, the incident date and a later regulatory milestone must remain separate. The report does not supply technical causes or final legal conclusions that the source did not establish.

5.7 Sector decisions without sector risk scores

Sector	Evidence distinction	First owned-environment decision
Public administration	Access claims, false messages and document sales differ	Establish the affected function and control its actual privileges
Finance and insurance	Customer-information access can occur without a major outage	Run privacy scoping and customer protection alongside technical response
Health	Document claims, payment events and ransomware listings are separate	Preserve clinical continuity while validating data or payment evidence
Education	Student, guardian and attendance data have different units	Validate categories and account access, with safeguarding ownership
Energy and industry	Impersonation can affect customers without internal access	Authenticate payment and investment requests through known channels
Retail, transport and suppliers	Operational records can support contextual fraud	Verify beneficiary and supplier changes independently

These are response distinctions supported by the cases. They are not sector ratings, national prevalence estimates or claims that every organisation has the same systems. The selected exposure portfolio has its own denominator and limitations in Chapter 3.

KEY TAKEAWAYS

01

Five public dossiers include different kinds of event, warning and investigation.

02

Continuity, privacy, payment authority and brand protection require separate decisions.

03

Preserve event, detection, publication and follow-up dates instead of creating new intrusions from later coverage.

CHAPTER 06

Unauthorised messages, access claims and service availability

THIS CHAPTER ANSWERS

Which service effects are established, and what would justify a stronger attribution?

3

separate questions: message integrity, service availability and data access

6.1 Timeline with evidence labels 46

6.2 Claim versus authority account 47

6.3 Availability and integrity need different tests 47

6.4 Prepare for disruption without inventing a campaign 47

6.5 Communications should preserve uncertainty 48

CHAPTER 06

Unauthorised messages, access claims and service availability

IN SHORT

The May public-alert event established unauthorised use of a supplier account and false messaging, according to the authority's account reported by the press. It does not establish a DDoS mechanism or a political operator. Other access and data claims remain unverified. Prepare separately for service unavailability, unauthorised messages and possible information loss, with distinct evidence and reopening tests for each.

6.1 Timeline with evidence labels

7 Jan 2026	**Forum participants** Citizen-data advertisement disputed as older material; no new intrusion established (B01, B02) [S1]
10 Feb 2026	**Forum advertiser** Privileged public-service access claimed; usability unverified (B03) [S1]
20 May 2026	**Authority statement reported by press** Supplier-account access and false emergency messages acknowledged [S17]
12 Jun 2026	**Petroperú** AI-manipulated investment video warning; no internal intrusion established [S20]
7 Oct 2026	**Insurer statement reported by press** Customer-information access detected; start date unresolved [S18]
8 Nov 2026	**Group-branded forum post** Business-registration publication presented as a leak (B07) [S1]
9 Nov 2026	**Authority response reported by press** Internal intrusion or extraction denied in relation to the dataset claim [S27]
14 Nov 2026	**Defacement-feed post** One website appearance claimed; operational impact unverified [S1]
16 Nov 2026	**Kaspersky research** Retadup research published about earlier multi-country blocked attempts [S32]

The timeline combines post dates, a detection date and public statements. Its row labels identify evidence type, not independent confirmation of every assertion. A research publication in November can describe earlier activity. [S1][S17][S18][S32]

6.2 Claim versus authority account

Point	Actor assertion	Official account	Independent limit
Public-service access	A February advertiser claims privileged access to a portal [S1]	No matching official confirmation established	No link to the May event is demonstrated
False public alerts	Public discussion described a malicious event	May authority account identifies unauthorised supplier-account use and false alerts, as reported [S17]	Actor identity, motive and wider access remain unresolved
November business records	Group-branded post presents data publication as a leak [S1]	Authority response denies evidence of institutional intrusion or extraction [S27]	No independent offered-file authenticity or provenance assessment
Political language	Some claim material uses political framing	No state attribution is established here	Rhetoric is not evidence of nationality, direction or election interference

A visible operational effect and a claimed actor role require different evidence. The report does not join the February advertisement, May alert event or November data claim by shared sector or country alone.

6.3 Availability and integrity need different tests

A DDoS response asks whether users can reach the service and complete critical tasks. A message-integrity response asks who can issue content and whether publication is authorised. A data-access response asks which records were accessed and by whom.

For an alert service, a responding website does not demonstrate that the message-issuance path is safe. For a transactional portal, restored login does not demonstrate that unauthorised sessions were revoked. For a customer database, uninterrupted operation does not rule out unauthorised information access.

The incident commander should identify the failed function before selecting a recovery milestone. Technical teams then preserve the evidence needed for that function: service telemetry, account activity, administrative changes or the relevant data-access records.

6.4 Prepare for disruption without inventing a campaign

The reviewed material does not establish a nationally measured DDoS campaign or a verified politically directed operation against the election process. That coverage result does not establish an absence of such activity outside the evidence reviewed.

Organisations can still prepare continuity. Agree who can request provider mitigation, which public information remains available through an independent channel, and which user tasks receive priority. Test contact routes while the normal identity or messaging service is unavailable.

Avoid blanket restrictions that create an unassessed service exclusion. Any emergency traffic-control measure should have a stated duration, an accountable owner and a route for legitimate users. Reassess it against actual service effects and the available evidence.

6.5 Communications should preserve uncertainty

A useful first statement identifies the affected function, the known time, the action taken and the next update. Keep the claim and the confirmed effect in separate sentences. Do not publish an actor's unsupported quantity or motive simply because it circulates widely.

When a supplier account is involved, distinguish the supplier relationship from an allegation against the supplier's entire environment. State only the access scope supported by the authority or organisation. Customer guidance should use a trusted channel and should not repeat the fraudulent link.

KEY TAKEAWAYS

01

False messaging, DDoS and data access require distinct evidence.

02

A nearby advertisement does not establish a link to an official incident.

03

Reopening tests should match the failed function and preserve uncertainty in public statements.

CHAPTER 07

Threat actors, ransomware and supported relationships

THIS CHAPTER ANSWERS

Which labels matter operationally, and what evidence supports their relationships?

58

Peru ransomware listings, each recording a criminal assertion

7.1 Ransomware listings and regional context 50
7.2 Claimant labels and the response they justify 52
7.3 Three listing observations in the recent window 54
7.4 Espionage research with a Peru component 55
7.5 Technique matrix and authorised validation 56
7.6 Recent malware research is not a November victim count 56
7.7 Relationship map and evidence boundaries 57

CHAPTER 07

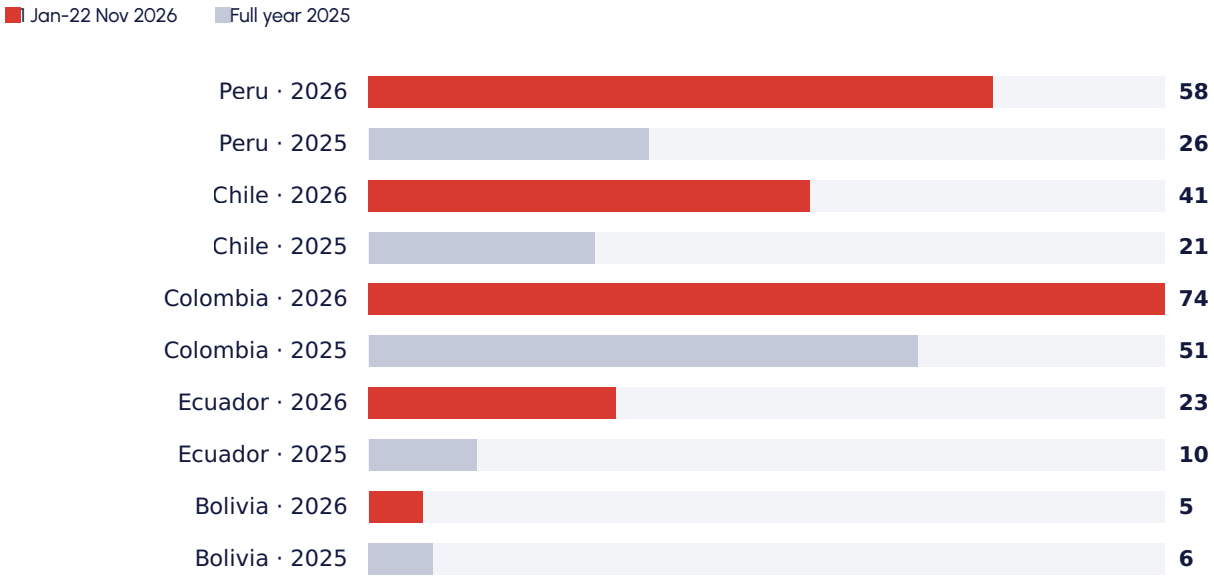
Threat actors, ransomware and supported relationships

IN SHORT

Ransompedia records 58 Peru listings across 20 claimant labels. Qilin, The Gentlemen and Nova together account for 28 listings. These are neither verified intrusions nor unique organisations. Separate vendor research places Peru within an espionage campaign and a multi-country malware observation. Attribute each assessment to its source, and prepare recovery, identity investigation and endpoint review without assuming a common operator across the populations.

7.1 Ransomware listings and regional context

Peru has 58 listings in the study window; peer counts describe different visibility populations



The 2026 window is partial; the 2025 comparison covers the full year. Counts describe source visibility, not a national risk ranking. Source: Brandefense Ransompedia, 1 January–22 November 2026; November partial [S2]. Listings remain criminal claims.

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

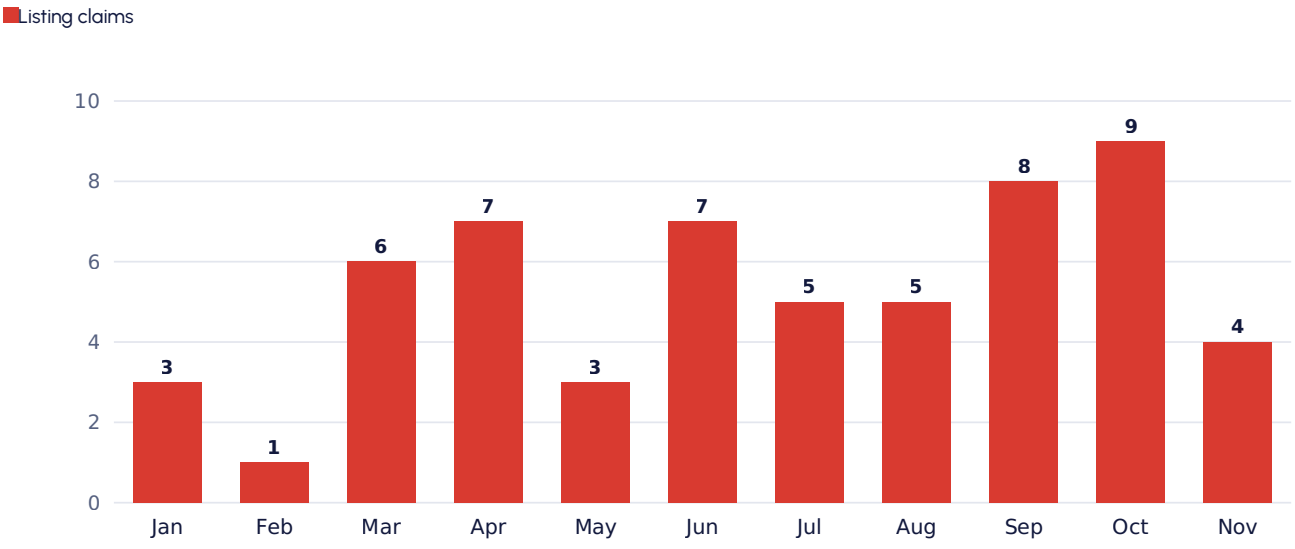
Country	Listings in the requested 2026 window	Listings in all of 2025
Peru	58	26
Chile	41	21
Colombia	74	51
Ecuador	23	10
Bolivia	5	6

Source: Brandefense Ransompedia [S2]. This compares a partial year with a full year. It is not a matched-period growth rate. The counts are not adjusted for country size, sector population or disclosure practice.

The listing population can repeat an organisation, use related names or change an industry label. A public listing establishes an extortion assertion. It does not establish encryption, the authenticity or quantity of stolen material, a payment or a unique affected organisation.

The public-reporting audit also found differences between claimed attack dates, listing dates and an aggregator's discovery date. Those dates are not interchangeable. The report keeps the own-source listing date for its listing population and keeps confirmed incident dates separate.

Listing observations are distributed across the year; November remains partial



Source: Brandefense Ransompedia, 1 January–22 November 2026; November partial [S2]. Listings remain criminal claims.

Month	Listings	Month	Listings
January	3	July	5
February	1	August	5
March	6	September	8
April	7	October	9
May	3	November through cut-off	4
June	7	Total	58

Source: Brandefense Ransompedia [S2]. A monthly listing pattern is not an intrusion-start pattern. The observed peak does not establish when the listed organisations were first accessed.

7.2 Claimant labels and the response they justify

Listing label	Peru listings	Interpretation
Qilin	16	Most frequent label in this listing population
The Gentlemen	7	Separate extortion-label observations
Nova	5	Separate extortion-label observations
SafePay	3	Includes a recent financial-services listing
RansomHouse	3	Repeated health-related observations require care with unique-incident interpretation
DragonForce	3	Listing assertions, not an independently confirmed entry route
Kazu	3	Related health-service labels do not establish independent victims
APT73	3	Label presence does not establish a state attribution
Other labels	15	Remaining observations across 12 labels
Total	58	Listings, not independent organisations

Source: Brandefense Ransompedia [S2]. The first three labels account for 28 of 58 observations, or 48.3%. The remaining 30 belong to other labels. The table does not establish the number of people operating each name.

Qilin

Extortion listing label | No state attribution assessed

IN PERU, 2026

2026

16 Peru listings in the requested window

CLAIMED TARGETS

Broad sector roles; no unverified victim names

SEEN IN PUBLIC REPORTING

[S2] Ransompedia records 16 listing observations.

OUR ASSESSMENT

Prepare validated recovery and disclosure decisions; a listing does not establish encryption, theft, a common operator or payment.

CONFIDENCE

High for the observed listing count; underlying assertions remain claims

The Gentlemen

Extortion listing label | No state attribution assessed

IN PERU, 2026

2026

7 Peru listings in the requested window

CLAIMED TARGETS

Broad sector roles; no unverified victim names

SEEN IN PUBLIC REPORTING

[S2] Ransompedia records 7 listing observations.

OUR ASSESSMENT

Prepare validated recovery and disclosure decisions; a listing does not establish encryption, theft, a common operator or payment.

CONFIDENCE

High for the observed listing count; underlying assertions remain claims

Nova

Extortion listing label | No state attribution assessed

IN PERU, 2026

2026

5 Peru listings in the requested window

CLAIMED TARGETS

Broad sector roles; no unverified victim names

SEEN IN PUBLIC REPORTING

[S2] Ransompedia records 5 listing observations.

OUR ASSESSMENT

Prepare validated recovery and disclosure decisions; a listing does not establish encryption, theft, a common operator or payment.

CONFIDENCE

High for the observed listing count; underlying assertions remain claims

Recovery should not depend on which group names an organisation. Validate actual system and data effects, retain the relevant listing as evidence, and test restoration from a protected recovery copy. Communications and legal teams should keep the criminal assertion separate from the confirmed impact.

7.3 Three listing observations in the recent window

Listing date	Broad role	Claimant label	Status
2026-11-11	Local public administration	The Gentlemen	Listing claim; no official incident confirmation established
2026-11-16	Media and communications services	Qilin	Listing claim; no official incident confirmation established
2026-11-21	Financial services	SafePay	Listing claim; no official incident confirmation established

Source: Brandefense Ransompedia [S2]. An additional pharmaceutical listing dated 7 November is outside the recent window. Its appearance in later reporting does not change that date.

These three rows are part of the 58-listing total. They are not additional incidents to add to the post dossiers or public cases. The victim labels remain broad, and no criminal destination or exposed-file link is published.

7.4 Espionage research with a Peru component

ESET's 17 September research describes SparroWocky deployment against government entities in Peru within a campaign spanning 2025–2026. ESET attributes the campaign to FamousSparrow and describes the group as China-aligned. The attribution remains ESET's assessment. [S31]

ESET's 28 October APT activity update for Q2–Q3 2026 reports continued FamousSparrow activity in South America during April–September 2026, without giving a Peru-specific target count [S45]. That follow-up marks a country-level visibility limit rather than evidence of additional Peru incidents.

FamousSparrow

Vendor-attributed espionage campaign | China-aligned, as assessed by ESET

IN PERU, 2026

2025–2026
Peru included in ESET regional campaign reporting

CLAIMED TARGETS

Government entities, as described by ESET; no named Peru victim

SEEN IN PUBLIC REPORTING

[S31] Vendor research; attribution remains the source assessment.

[S45] October Q2–Q3 2026 update notes continued South America activity without a Peru-specific count.

OUR ASSESSMENT

Review relevant owned endpoints and applications. No Peru-specific technique frequency is established.

CONFIDENCE
Source-qualified campaign assessment

The report does not convert that regional research into a named Peruvian victim, a national intrusion total or proof that every technique occurred in Peru. It does not adopt the source's geopolitical explanation. The campaign and the underground advertisements remain separate evidence populations.

7.5 Technique matrix and authorised validation

TECHNIQUES NAMED IN THE VENDOR RESEARCH, BY TACTIC

Initial Access	Persistence	Collection
T1190 Exploit Public-Facing Application	T1543.003 Windows Service	T1113 Screen Capture

Vendor campaign/capability mapping; not a Peru frequency table. [S31]

Vendor-mapped technique	Scope	Suggested validation task
T1190: public-facing application exploitation	ESET campaign mapping [S31]	Inventory owned public applications and review relevant server activity
T1543.003: Windows service persistence	ESET capability mapping [S31]	Review newly created or changed services against approved deployment records
T1113: screen capture	ESET capability mapping [S31]	Correlate unexpected capture behaviour with endpoint context and authorised software

The matrix is a vendor-research mapping, not a Peru technique-frequency table. The suggested tasks are defensive review questions. No production detection rule or engine-validation result is claimed.

A useful endpoint review combines several observations and compares them with approved administrative activity. A service installation or screen-capture capability alone can have legitimate explanations. Confirm process context, business ownership and related activity before escalating a single observation into an actor attribution.

7.6 Recent malware research is not a November victim count

Kaspersky's 16 November publication reports about 15,000 blocked Retadup attempts across several countries during January–September 2026, including Peru. It describes USB propagation and CoffeeLoader delivery. The figure is neither a Peru total nor successful infections. [S32]

Retadup / CoffeeLoader

Malware relationship in vendor research | No state attribution assessed

IN PERU, 2026

2026-11-16

Publication about earlier multi-country attempts

CLAIMED TARGETS

Countries include Peru; no national victim count

SEEN IN PUBLIC REPORTING

[S32] Kaspersky research; attempts and infections remain distinct.

OUR ASSESSMENT

Review removable-media handling and endpoint context using authorised tests.

CONFIDENCE

Source-qualified malware research

This adds a removable-media review to the recent-activity decisions. Owners should control how older storage devices enter managed systems and test endpoint response using an authorised exercise. The November publication date must not be used to date all of the reported attempts.

7.7 Relationship map and evidence boundaries

MortemTeam label

Branding in retained forum posts | No motive or state attribution established

IN PERU, 2026

2026-11-08

Business-record assertion, B07

2026-11-13

Education-data assertion, B08

CLAIMED TARGETS

Broad public-record and education themes

IN THEIR WORDS

"Data Included: [business identifier], Legal Name"

B07

SEEN IN PUBLIC REPORTING

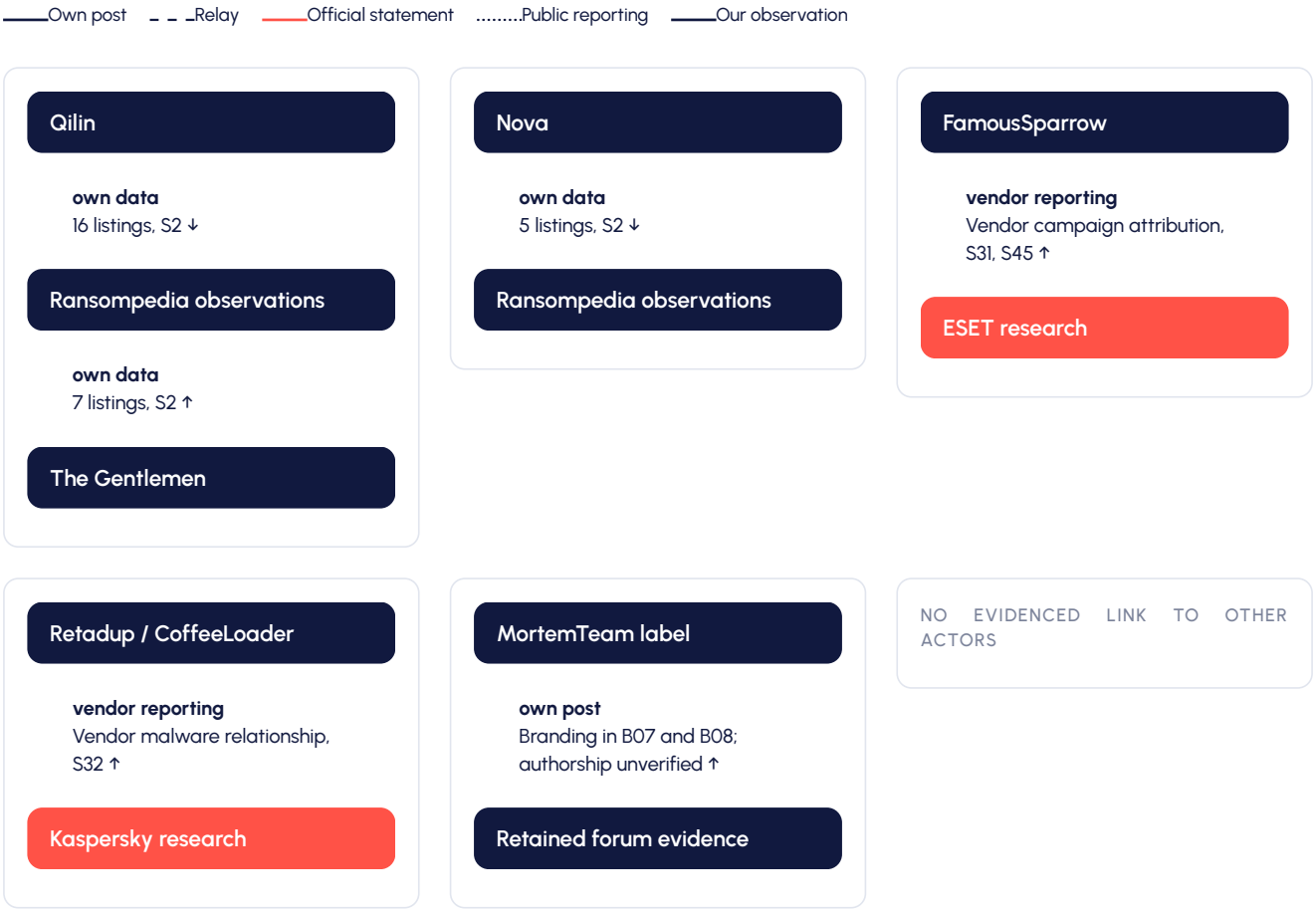
[S1] The label appears in post bodies; authorship is not independently established.

OUR ASSESSMENT

A common label does not establish a common operator, identical files or a verified intrusion.

CONFIDENCE

High for visible branding; authorship and underlying claims unverified



The map connects each label or campaign to the source that supports it. Ransompedia edges are **own data**. The ESET and Kaspersky edges are **vendor reporting**. Forum-branding edges describe a label in a post, rather than verified authorship. [S1][S2][S31][S32][S45]

There is no supported common-operator edge between the extortion labels, the group-branded education posts, the espionage campaign and Retadup. A shared country is not such an edge. Any future relationship claim needs a concrete shared element and its own confidence assessment.

KEY TAKEAWAYS

01

The 58 listings remain claims and can repeat organisations.

02

Vendor attribution and capability mapping retain their campaign and geographic limits.

03

Prepare recovery and endpoint review without assuming that unrelated populations share an operator.

CHAPTER 08

Fraud economy: identity, persuasion and payment

THIS CHAPTER ANSWERS

How can information and trusted-looking messages become a fraud risk without proving an original intrusion?

15

distinct card records in the narrowly scoped retained-post observations

8.1 An analytical model, not an observed transaction chain 61
8.2 Payment-card observations have a narrow scope 61
8.3 Identity and certificate sales 62
8.4 Impersonation can use an authoritative image 62
8.5 Institutional themes and transport-fine lures 62
8.6 Advertised prices are not realised market value 63

CHAPTER 08

Fraud economy: identity, persuasion and payment

IN SHORT

The evidence separates identity-data advertising, account-access offers, impersonation warnings and reported unauthorised transfers. These are different stages and do not establish one connected criminal chain. The strongest response is to validate the specific account or information and give customers a trusted way to check suspicious requests. Authenticate payment and account-recovery changes through a trusted independent channel.

8.1 An analytical model, not an observed transaction chain

A useful planning model has four stages: information that makes a story credible, a persuasive contact, an account or approval decision, and a payment or data transfer. This is an **analytical model**. The report has not established a common operator, completed sale or causal chain linking the reviewed examples.

The citizen and employment-record claims illustrate advertised information. Petroperú's warning illustrates a publicly acknowledged impersonation attempt. The health-service transfer account illustrates a reported financial event. Each supports a separate control decision; combining them would overstate the evidence. [S1] [S20][S23]

For information alerts, validate provenance and age. For persuasive contacts, confirm the request through a known channel. For account decisions, review the actual privileges and recent changes. For payments, preserve approvals and beneficiary evidence while contacting the financial institution through established routes.

8.2 Payment-card observations have a narrow scope

SCOPE OF THE CARD FIGURES

The reviewed post population contains 15 card-record observations. Their validity, ownership and use are unverified. This limited population does not estimate national card exposure or fraud losses.

The retained-post observations contain 15 distinct card records in 13 posts, with 16 occurrences. Six card records have an issuer association and nine do not. These disjoint groups total 15. Their validity, account ownership and actual use are not established. [S1]

A checker-style status or an assertion that a card is "live" remains the poster's statement. It is not independent evidence of a successful authorisation, completed purchase or cash loss. Issuers should validate a relevant alert through their own authorised records before choosing customer contact, restrictions or reissue.

The issuer-associated observations and the selected financial-domain portfolio in Chapter 9 are different populations. They do not establish a join between a particular cardholder, device and organisation. The report publishes no card details, individual account identifiers or national card-loss estimate.

8.3 Identity and certificate sales

The July official operation describes alleged illegal sales of personal information and false certificates. The underground dossiers separately advertise citizen, benefit and employment information. The evidence does not establish that the operation concerned any of those advertisements or their underlying files. [S22][S1]

A document's apparent official format is not an identity decision. Customer and staff workflows should validate important documents through the legitimate issuer or an approved verification process. Record the result without circulating unnecessary personal material to a wider response group.

Telephone numbers and recovery details also need a clear owner. A caller who knows personal history has not necessarily passed an independent identity check. Organisations should define which changes require another trusted factor or confirmation route, especially where the requested action affects payment or privileged access.

8.4 Impersonation can use an authoritative image

Petroperú's official warning supports a specific brand-response decision: publish the real process and provide an independent check. It does not establish a company-network intrusion or a measured national increase in AI-assisted fraud. [S20]

The lesson is about verification. Staff should not treat a familiar face, voice or executive title as sufficient approval for a payment or account change. Preserve the established approval process even when the request appears urgent or comes through an unusual channel.

For customers, a useful warning identifies the action to avoid and the legitimate route to use. It should not repeat a fraudulent contact, direct people to an actor's page or promise that every deceptive message can be identified by visual quality.

8.5 Institutional themes and transport-fine lures

The official newspaper's August account describes a transport-fine impersonation warning involving messages, links and QR codes. It provides campaign context, not a count of confirmed network intrusions. [S26]

A public-service theme can induce action without exploiting a technical vulnerability at the impersonated institution. Customer operations should explain how a legitimate notice can be checked independently. Security should preserve relevant reports and coordinate any removal request through the authorised process.

The report does not infer a motive or nationality from the language used in a message. An institutional logo or a plausible administrative deadline is part of the assertion being evaluated. It is not proof that the message came from the institution.

8.6 Advertised prices are not realised market value

Post date	Offer type	Advertised price	What remains unestablished
2026-02-10	Privileged public-service access	200 USD	Working access, scope, possession and sale
2026-03-27	Retail login access and operational records	20,000 USD, negotiable	Present privilege, document authenticity and sale

Source: retained advertisements [S1]. These two asking prices are selected case details. They do not establish a national median, a completed transaction, a representative range or the economic value of the advertised material.

A high price does not validate possession. A low price does not establish fabrication. Assess the proposition using the relevant owned evidence, with the advertised price retained only as part of what the seller asserted.

KEY TAKEAWAYS

01

The information-to-payment sequence is a planning model, not a demonstrated common criminal chain.

02

The 15 card records belong to a limited post population; validity, ownership and use remain unverified.

03

Preserve independent verification for documents, account changes and payments, even when a request appears authoritative.

CHAPTER 09

Banking and customer protection

09

THIS CHAPTER ANSWERS

Which financial-sector decisions follow from the available evidence without inventing a bank exposure total?

25

financial and insurance domain candidates in the selected portfolio

9.1 Scope and available results 65
9.2 Insurer access and customer guidance 66
9.3 Payment review belongs with the account owner 66
9.4 Historical incidents should remain historical 67
9.5 Open finance and supervisory readiness 67
9.6 What to test with a financial service owner 67

CHAPTER 09

Banking and customer protection

IN SHORT

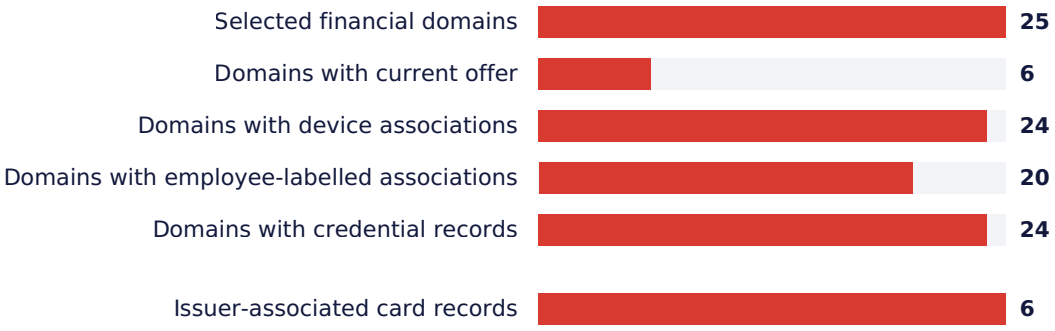
The financial portfolio contains 25 selected domain candidates, while the narrow card-post population and public financial events have different units. Exposure signals are available, but no individual customer, card or device join is established. The insurer account, health-service transfers and retrospective bank reporting support separate privacy, payment and chronology decisions. Validate current owned-account evidence, preserve payment authority and distinguish a customer-information incident from a service outage or a bank-system intrusion.

9.1 Scope and available results

Population	Available statement	Limit
Selected financial and insurance domains	25 candidates	Related services and legal independence remain unvalidated
Credential and device exposure	6 current-offer domains; 24 with device associations; 24 with credential records	Domain associations, not confirmed bank-system incidents
Narrow card-post population	15 card records across the report's retained posts	Not unique customers, national card exposure or bank-system access
Customer-information incident	One source-qualified insurer dossier	Not a complete financial-sector incident population
Health-service payment event	Five disputed transfers in a specific institution's account	Not a demonstrated bank-system intrusion
Historical bank discussion	Later reporting about an earlier incident	Not a newly established 2026 intrusion

The scope of the selected exposure observations does not establish independent banks, unique customers or confirmed intrusions. The separate card figures describe 15 card-record observations in the reviewed post population. Their validity, ownership and use are unverified. This limited population does not estimate national card exposure or fraud losses. [S1]

Financial-domain signals and card records remain separate populations



Domain candidates and issuer-associated card records are separate populations; they are not joined to customers, accounts or devices. Source: Odin by Brandefense, 250 selected domain candidates, 22 November 2026 [S3]. Associations can overlap and include older observations. [S1]

The selected financial and insurance group has 25 domains. Current offers concern 6; device associations concern 24, employee-labelled device associations concern 20, and credential-record associations concern 24. These signals require owned validation and do not establish independent banks or affected customers. [S3]

9.2 Insurer access and customer guidance

The October insurer account establishes a confidentiality investigation even though the supervisor did not report significant service interruption. It does not establish a final customer total or the actor's advertised quantity. Chapter 5 retains those source limits. [S18]

The operational response should identify what customers can meaningfully do. If contact or policy information is validated as affected, warn about plausible impersonation using those categories. Do not imply that all financial credentials were exposed or that a customer must replace every payment instrument.

A customer notice should provide an independent contact route, explain the known categories and identify what remains unresolved. Customer operations should preserve incoming fraud reports so that the incident team can distinguish anticipated misuse from actual subsequent events.

9.3 Payment review belongs with the account owner

The health-service transfers illustrate why institutional account ownership and approval authority matter. A claim against a banking counterparty is not proof of intrusion into that bank. Treasury and the institution's security owner should preserve the actual payment and approval records. [S23]

Review who could create or amend beneficiaries, approve transactions, change authentication or act under an emergency exception. Confirm that the trusted contact route still works when the usual email account is unavailable. Record the outcome of any recovery request without promising reversal.

Where an account restriction protects investigation, the business owner should decide how essential legitimate payments continue. A controlled alternative process needs a named approver and an audit trail. The report does not establish that a specific institution lacked these controls.

9.4 Historical incidents should remain historical

The November bank discussion concerns an earlier incident and a regulatory process. It is not treated as a newly confirmed 2026 intrusion. The report makes no final legal finding about liability or a general exemption from penalties. [S28]

This distinction affects monitoring and communications. A repeated data advertisement can require a new review of current misuse without creating a new source-system event. Link it to earlier disclosures only when the evidence supports that relationship, and retain any uncertainty about the actual file or account.

An incident register should therefore support both an underlying-event date and a new publication date. The response can be current while the material is historical. A customer should not receive a misleading statement that a new intrusion occurred merely because an older story returned to the news.

9.5 Open finance and supervisory readiness

The supervisor's February roadmap describes phased open-finance development. Future phases are not described here as implemented controls. An organisation should map the services and third-party permissions it actually operates, rather than assuming that a roadmap has already changed every interface. [S29]

The existing cybersecurity regulation addresses authentication, access records and supplier responsibilities. A relevant review should test whether the organisation can identify an authorised third party, its permitted data and the point at which access is revoked. [S7]

For incident reporting, use the rule in force and the organisation's actual supervisory scope. The September unified-reporting proposal is a change-monitoring item. Chapter 10 separates it from existing duties and the later customer-communication provisions. [S8][S10]

9.6 What to test with a financial service owner

Use a synthetic customer-information alert, a disputed payment and a supplier-access withdrawal as three separate exercises. Each should produce a clear determination and an owner. A single generic "breach exercise" can hide the differences between them.

For the information alert, identify categories and the communication decision. For the payment, preserve authority and beneficiary evidence. For supplier access, demonstrate that the permission is withdrawn and legitimate service continues through the agreed fallback.

A board-facing metric can then report unresolved validated alerts, completed service exercises and accepted exceptions. It should not substitute historical credential totals or underground advertising volume for evidence that the controls work.

KEY TAKEAWAYS

01

Financial domains, card records, customers and bank-system incidents are different units.

02

Privacy assessment and payment-authority review should run alongside technical containment.

03

Preserve historical chronology and follow the supervisory rule actually in force.

CHAPTER 10

Regulatory response and reporting decisions

10

THIS CHAPTER ANSWERS

Which duties apply now, and which changes require preparation for a later date?

48 hours

maximum awareness-based deadlines in two distinct reporting regimes

10.1 Applicability table 70

10.2 Personal-data incidents need a reasoned notification decision 71

10.3 Digital-security reporting is a separate determination 71

10.4 Financial duties, proposed changes and future communications 71

10.5 What a reporting exercise should demonstrate 72

CHAPTER 10

Regulatory response and reporting decisions

IN SHORT

Peru's personal-data, digital-service and financial reporting duties require separate applicability decisions. Two regimes use a 48-hour maximum, but their scope and recipients differ. Financial cybersecurity reporting already applies; September's unified procedure was presented as a proposal. Customer-communication amendments have a later commencement clause. Preserve the awareness time, identify the applicable duty and rehearse reporting with the supplier and business owners who hold the necessary evidence.

This chapter is an operational planning aid. Legal teams must determine applicability against the current official texts and the organisation's actual role. It does not replace legal advice.

10.1 Applicability table

Instrument	Status and scope	Trigger or timing	Operational owner and evidence
Supreme Decree 016-2024-JUS, Article 34	Personal-data protection regulation; in force before this study window	Qualifying personal-data incident: notify ANPD within 48 hours of awareness; delayed notification needs reasons	Privacy lead and controller; awareness record and notification rationale [S6]
Same regulation, Articles 34–36	Controller, affected-person communication and processor duties remain distinct	Affected-person communication depends on the stated rights-impact condition; processor informs controller immediately	Privacy, customer operations and supplier owner; scoped notice and receipt [S6]
Supreme Decree 126-2025-PCM, Article 32	Digital Trust Framework regulation, effective 2 February 2026	Critical digital-security incidents: CNSD within 48 hours of provider awareness; other levels follow applicable classification rules	Digital-security officer and service owner; classification and reporting record [S5]
SBS Resolution 504-2021, Article 15	Applicable supervised financial entities	Report a significant cybersecurity incident as soon as recognised; verified or presumable adverse impact is relevant	Security and compliance; supervisory report and forensic record [S7]

Instrument	Status and scope	Trigger or timing	Operational owner and evidence
SBS September unified reporting procedure	Consultation proposal in the verified September material	Proposed initial, intermediate and final reporting is not treated here as an enacted replacement	Regulatory owner; verify final rule before changing the live reporting calendar [S8][S9]
SBS Resolution 01741-2026, Articles 55–56	Customer-communication amendments with general commencement 360 days after publication	The customer-incident provisions are a later preparation requirement under the cited text	Compliance and customer communications; implementation plan and effective-date check [S10]

10.2 Personal-data incidents need a reasoned notification decision

Article 34.1 has alternative triggers. They include large exposure by quantity or type, a large affected population, sensitive data, or evident harm to other rights or freedoms. Internal remediation does not remove the qualifying ANPD notification duty. Article 34.5 also addresses CNSD notification when the incident occurs through the digital environment. [S6]

Communication to affected people has its own condition and exception. The regulation requires clear communication without undue delay within the stated 48-hour period when the rights-impact condition applies. Article 34.4 addresses incidents without that impact that were fully resolved. [S6]

Do not substitute the phrase "no service disruption" for a personal-data assessment. The October insurer case demonstrates why availability and confidentiality need separate records. A restored service may still require an affected-person assessment, while an outage may involve no personal-data exposure.

10.3 Digital-security reporting is a separate determination

The Digital Trust Framework regulation was published on 4 November 2025. Its 90-day commencement clause places entry into force on 2 February 2026. Article 32 sets the critical-incident maximum from provider awareness; Article 34.4 addresses suppliers communicating incidents to the provider. [S5]

The practical requirement is to obtain timely supplier facts. Contracts and contact arrangements should identify who informs the service owner, which incident information is available and how an urgent assessment reaches the reporting owner. Do not wait for a public criminal claim to define the internal awareness time.

The reporting record should distinguish criticality, the actual service effect and the presence of personal data. Where several duties apply, retain separate recipients and determinations. One regulator's involvement does not automatically close another authority's requirement.

10.4 Financial duties, proposed changes and future communications

The verified SBS regulation already requires reporting significant cybersecurity incidents and making the forensic report available to the supervisor. Its listed adverse impacts include information loss, fraud, reputation and operational interruption. The duty is not limited to encryption or a public leak-site listing. [S7]

The September 2026 proposal sought a unified operational-incident procedure. The issuer's notice describes consultation through 16 October. The proposed two-hour, five-hour and business-day limits must not be inserted into a current playbook as enacted obligations on that evidence alone. [S8][S9]

Resolution 01741-2026 was published on 2 July. Article Three sets a general 360-day delay, with separate immediate exceptions unrelated to the incident-communication articles. This places Articles 55–56 on 27 June 2027 under the cited commencement clause. [S10]

Those provisions distinguish mass communication within 24 hours from direct communication within 10 business days, with a justified additional 10-business-day extension. They address the specified customer-impact and significance conditions. Prepare the channels, but verify later amendments and applicability before activation as a legal deadline. [S10]

10.5 What a reporting exercise should demonstrate

Choose a synthetic supplier incident involving a critical service and possible customer data. Record when the provider first knows enough to begin assessment. Ask each owner to state the reporting trigger, recipient, applicable maximum and facts still missing.

The exercise should produce a short approved decision record. Include the known facts, the legal entity, the service and data categories, the reason for notifying or not notifying, the notification owner and the next update time. Preserve an actual acknowledgement when a report is sent.

Keep criminal complaints, technical assistance and public customer messaging separate from regulator notifications. A police operation, an authority's supervision and a seller's assertion are different evidence events. No notification is claimed in this report unless the cited source establishes it.

KEY TAKEAWAYS

01

Similar maximum deadlines do not create identical legal duties.

02

Separate rules in force from consultations and later commencement dates.

03

Rehearse a shared fact record with distinct reporting owners, recipients and decisions.

CHAPTER 11

Outlook and conditional planning assumptions

11

THIS CHAPTER ANSWERS

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

4

conditional scenarios with explicit decision signals

11.1 Key judgements and their limits 74
11.2 Four conditional scenarios 75
11.3 What the recent window changes 75
11.4 Signals this report cannot supply 75

CHAPTER 11

Outlook and conditional planning assumptions

IN SHORT

Prepare for continued identity-data advertising, extortion claims, supplier-access incidents and contextual fraud. These are conditional planning assumptions, not predictions of national attack counts. Historical material can remain relevant to current misuse, while recent publication can describe earlier activity. Give each scenario an owner, a signal that changes the response and a condition that would reduce concern. Review the plan against validated local evidence rather than post volume alone.

11.1 Key judgements and their limits

Judgement	Confidence and basis	What could change it
New advertisements can concern older records	High for the observed January discussion; file identity remains unresolved [S1]	Validated owned records and independent acquisition chronology
Public-service access claims deserve account-level validation	High for the access advertisement; low for its underlying usability [S1]	Authorised account-status and sign-in evidence
Confidentiality response can remain necessary without a major outage	High for the insurer's source-qualified account [S18]	A later scoped update establishing different categories or impact
Several extortion labels require recovery readiness	High for the listing population, not for every underlying assertion [S2]	Validated local incident effects or authoritative corrections to a listing
Removable-media review belongs beside account security	Supported by the cited vendor research; Peru-specific scale unknown [S32]	Owned endpoint evidence and the organisation's actual removable-media use

Confidence attaches to a proposition. Confidence that a post or listing exists is not confidence that its contents are accurate. A source's attribution is retained as its assessment, rather than converted into an independent finding by this report.

11.2 Four conditional scenarios

Planning assumption	Signal that raises concern	Response owner and action	Signal that reduces concern
Historical identity material is reused in a convincing contact	Validated owned information appears alongside a suspicious account or payment request	Fraud and customer operations authenticate the request independently and preserve evidence	Material is unrelated or already remediated, with no current misuse evidence
An advertised privileged account is still usable	Owned account is active, appropriately matched and shows concerning access	Identity and incident response contain the validated account and sessions	Account is inactive or unrelated and the disposition is documented
A supplier account can issue trusted messages or change a critical service	Unexpected supplier activity or an unauthorised message is confirmed	Service and supplier owners suspend the relevant privilege and activate a correction or fallback route	Reviewed actions are authorised and the issuance path passes its reopening test
A listed organisation has a real continuity or information-loss event	Internal investigation establishes affected systems, records or business functions	Incident command tests safe restoration and activates scoped privacy and customer decisions	Evidence narrows the event or the specific assertion is credibly corrected

These scenarios do not establish that the reviewed advertisements caused the public events. They identify conditions under which a security leader should change an operational decision. Their value lies in the observable trigger and closure evidence, rather than an unsupported probability.

11.3 What the recent window changes

The closing fortnight adds business-record, education-management and employment-history advertising. It also includes three ransomware listing observations and a vendor research publication about earlier malware attempts. These are distinct additions to visibility, not a combined new-incident count. [S1][S2][S32]

The immediate response is to assign each relevant signal to its validation owner. A school-data assertion needs data and safeguarding review if records are validated. An account assertion needs current-status and use evidence. A ransomware listing needs internal impact assessment and a continuity decision.

A recent denial should also change the wording. Preserve the claimed provenance and the authority's or company's response without treating either as a substitute for independent file validation. That keeps the analysis useful while the underlying proposition remains unresolved.

11.4 Signals this report cannot supply

The available evidence does not establish national loss, attack probability, unique affected people or a complete census of intrusions. It does not establish a shared operator across the reviewed populations or an effect on an electoral outcome.

No forecast is derived from a source's language, a seller's price or a large advertised record count. The exposure portfolio is selected and has separate coverage limits. Its unavailable values cannot supply a national trend.

Leaders should revisit the scenarios when new owned evidence arrives. An update should state which proposition changed, what evidence changed it and which response decision follows. Preserve earlier uncertainty rather than rewriting a historical claim as if it had always been confirmed.

KEY TAKEAWAYS

01

Conditional scenarios need an observable trigger and an accountable owner.

02

Recent publication does not automatically establish recent acquisition or intrusion.

03

Change the response when the evidence changes, and record the reason.

CHAPTER 12

The 30/60/90-day action plan

12

THIS CHAPTER ANSWERS

Who acts on the evidence, and what demonstrates completion?

18

conditional actions with owners and completion evidence

12.1 Action lanes 78
12.2 Role-specific first decisions 80
12.3 Completion scorecard 81
12.4 How Brandefense can help 82

CHAPTER 12

The 30/60/90-day action plan

IN SHORT

Begin with a reliable route for relevant alerts, then validate the specific account, information or service effect. In parallel, prepare continuity and reporting decisions with business and supplier owners. The plan below sets proposed management targets, not legal deadlines or claims about existing organisational controls. Preserve exceptions and evidence of each outcome. Assign the owners now and test the highest-consequence service before expanding the programme.

12.1 Action lanes

1Days 1–30

Confirm a route for relevant account and data alerts; investigate a synthetic alert

ACCOUNTABLE OWNER
CISO and intelligence lead

COMPLETION EVIDENCE
Alert reaches the named owner and receives a documented disposition

Validate owned accounts when a relevant current offer is received

ACCOUNTABLE OWNER
Identity lead

COMPLETION EVIDENCE
Ownership, status, privilege, recent use and prior remediation recorded

Revoke relevant sessions and authentication grants when validated evidence requires containment

ACCOUNTABLE OWNER
Identity and incident response

COMPLETION EVIDENCE
Access test demonstrates withdrawal; legitimate recovery is documented

Inventory supplier privileges over critical services and trusted message issuance

ACCOUNTABLE OWNER
Service and supplier owners

COMPLETION EVIDENCE
Named accounts, suspension authority, contacts and fallback recorded

Map applicable personal-data, digital-service and financial reporting duties

ACCOUNTABLE OWNER
Legal, privacy and compliance

COMPLETION EVIDENCE
Awareness triggers, recipients, owners and current texts recorded

Preserve independent payment and beneficiary-change approval during an incident

ACCOUNTABLE OWNER
Treasury and fraud lead

COMPLETION EVIDENCE
Synthetic request receives the required separate verification

2Days 31–60

Test a critical service while its normal identity dependency is unavailable

ACCOUNTABLE OWNER
Business continuity and service owner

COMPLETION EVIDENCE
Minimum safe service and reopening criteria demonstrated

Test suspension of a supplier's relevant access and a trusted correction message

ACCOUNTABLE OWNER
Supplier and communications owners

COMPLETION EVIDENCE
Suspension and correction succeed through the agreed alternative route

Scope validated personal data by actual category and affected group

ACCOUNTABLE OWNER
Data owner and privacy lead

COMPLETION EVIDENCE
Approved category assessment and notification rationale

Test application authorisation where a relevant education or portal claim is validated

ACCOUNTABLE OWNER
Application owner

COMPLETION EVIDENCE
Authorised review records results and closes the demonstrated weakness

Verify supported PHP remediation for owned affected deployments

ACCOUNTABLE OWNER
Infrastructure and application owners

COMPLETION EVIDENCE
Running version or applicable distributor advisory is checked after change

Review removable-media use against the organisation's actual workflows

ACCOUNTABLE OWNER
Endpoint and operations leads

COMPLETION EVIDENCE
Approved handling route and an authorised detection exercise

3Days 61–90	
Restore a critical system using a protected recovery copy	
ACCOUNTABLE OWNER Recovery and business owners	COMPLETION EVIDENCE Service completes its critical task in isolation before approved reopening
Review authorised mail senders before changing email-authentication enforcement	
ACCOUNTABLE OWNER Messaging lead	COMPLETION EVIDENCE Legitimate mail paths and controlled spoofing tests documented
Rehearse a customer impersonation warning through an independent contact route	
ACCOUNTABLE OWNER Customer operations and communications	COMPLETION EVIDENCE Staff and customers can find and use the legitimate verification process
Review historical advertisements against prior notices and remediation	
ACCOUNTABLE OWNER Intelligence and data owners	COMPLETION EVIDENCE Each relevant item is current, historical, unrelated or unresolved with a reason
Check the regulatory change register for final rules and commencement dates	
ACCOUNTABLE OWNER Compliance lead	COMPLETION EVIDENCE Current status and an approved implementation calendar
Present remaining validated risks and accepted exceptions to leadership	
ACCOUNTABLE OWNER CISO and business risk owners	COMPLETION EVIDENCE Signed decisions with owners, due dates and review conditions

The periods are proposed planning targets. Applicable legal maximums can require action much sooner, and a validated active privileged account can require immediate containment. Do not wait for the plan's later lane when the specific evidence or reporting duty warrants earlier action.

12.2 Role-specific first decisions

Board and executives. Ask which critical service has passed an interruption and reopening exercise. Resource the unresolved dependencies and require an owner for accepted exceptions. Do not use the report's publication counts as a measure of control effectiveness.

CISO and incident command. Confirm the alert route and decision record. Separate account validation, data scoping, continuity and notifications. Record which proposition is established and which evidence would change the response.

SOC and identity teams. Examine relevant sign-ins, session grants, privilege changes and endpoint context after ownership is validated. Document historical or unrelated alerts. A seller's assertion alone is not an instruction to disable an entire organisation.

Application and infrastructure teams. Validate effective authorisation and deployed software versions in owned systems. Preserve evidence of remediation and a functional retest. A vendor capability mapping is a review input, not proof of the same technique in the local environment.

Treasury and customer protection. Preserve independent verification for payment, beneficiary and recovery changes. Give customers a known route to check suspicious requests. Where information misuse is suspected, distinguish a plausible scenario from a reported completed fraud.

Legal, privacy and communications. Preserve awareness times, determine each applicable duty and give a next update time. Keep actor assertions, organisation confirmations and remaining unknowns in distinct sentences. Do not publish a final liability conclusion from an unresolved proceeding.

12.3 Completion scorecard

Decision area	Proposed management target	Evidence and exception rule
Alert routing	In place by day 30	Synthetic alert arrives and is assigned; missing access has an owner
Relevant current account alerts	Every validated alert has a disposition	Containment or documented historical/ unrelated outcome; unresolved cases remain visible
Critical supplier access	Reviewed by day 30 and exercised by day 60	Suspension authority works; exceptions approved by the business owner
Minimum safe service	Tested by day 60	Actual critical user task succeeds through the fallback
Protected restoration	Demonstrated by day 90	Recovery and safe reopening records, in-cluding dependent identity services
Reporting readiness	Applicable duties mapped by day 30	Correct trigger, recipient and owner; actual legal deadlines override planning lanes
Customer verification	Tested by day 90	A suspicious request can be checked through a trusted independent route

These are proposed management outcomes, not measured improvements produced by this report. The organ-isation should set its actual targets according to service criticality, validated exposure and legal duties. Retain a reason when the target changes.

12.4 How Brandefense can help

The report illustrates the use of Brandefense Blackhole post evidence, Ransompedia listings and a selected exposure portfolio. A relevant discussion should begin with the organisation's owned assets, its existing alert routes and the validation decisions it needs to make.

Bring a critical service, a supplier dependency and a current response question. Ask how the evidence would reach the accountable team and what that team would need to validate it. A demonstration does not establish that a particular organisation is affected or guarantee prevention, recovery or notification compliance.

Request a Brandefense demo. [S36]

KEY TAKEAWAYS

01

Start with alert routing and validation, while preparing continuity and reporting in parallel.

02

Match containment and reopening to the established service, account or data effect.

03

Measure completed decisions and tested outcomes, with explicit owners for exceptions.

APPENDICES

Appendices

A–D

THIS CHAPTER ANSWERS

How should the evidence and its limits be interpreted?

2026

primary post-time window, with separate observation dates where stated

Appendix A. Scope, evidence and confidence 84

Appendix B. Post evidence register 87

Appendix C. Sources 88

Appendix D. Plain-language glossary 91

Appendix A. Scope, evidence and confidence

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

A.1 Research contract

The country is Peru, code PE. The primary window runs from 1 January to 22 November 2026 by post time. Recent activity covers 8–22 November. The extraction and source-check date is 22 November; the cut-off day was still in progress. The report was first published on 22 November 2026 and revised on 23 November 2026.

The audience is security leadership, incident responders, identity and application teams, fraud teams, legal advisers and service owners. The decisions concern validation, account containment, customer protection, minimum safe service, reporting and recovery.

A.2 Sources and separate populations

Own sources include dark-web posts collected by Odin by Brandefense, public ransomware leak-site listing observations in Ransompedia, a selected organisation portfolio and passive DNS, TLS and web-control observations where available. External sources include official texts, issuer statements, vendor research and public reporting. [S1][S2][S3]

A post is a published message. An advertisement is an assertion about an offer. A listing records a criminal claim. A complaint records what was reported under the source's definition. A case dossier bundles a decision question and its supporting evidence. None is automatically a verified intrusion.

The same underlying subject can appear in several posts, listings or later articles. Records can overlap across sources and domains. The report does not estimate unique people from those populations and does not add them into a national attack total.

A.3 Portfolio and passive observations

The portfolio contains 250 purposive domain candidates in ten merged sector groups. It is not a national prevalence sample or a revenue ranking. Domain ownership, related services and independent legal identity remain unvalidated.

Exposure associations and current credential offers require their own observation date. Cumulative records are not a 2026-only incident population. A device association does not establish employment or current access to an organisation's internal systems. Only a validated national Atlas headline may be published; sector and organisation ratings are absent.

Passive configuration observations retain the denominator available for each control. Missing results remain unknown. Not finding a record is not proof that no control exists, and a certificate or homepage observation is not a complete application-security assessment. [S3]

A.4 Ransomware and comparisons

The 58 Peru listings are dated within the requested 2026 window. They can repeat an organisation or use different role and industry labels. A listing is not independent proof of encryption, theft, a payment or final loss. [S2]

The regional comparison uses Chile, Colombia, Ecuador and Bolivia. Peer selection is explained in §2.4. Raw listing and post counts do not adjust for country size, disclosure practice or source visibility. The 2026 window is partial; the 2025 listing comparison covers the whole year.

A.5 Card scope

The reviewed post population contains 15 card-record observations. Their validity, ownership and use are unverified. This limited population does not estimate national card exposure or fraud losses. [S1]

The card records, issuer associations, device observations and selected financial domains are different populations. No individual customer, device or account join is established. A status printed in a post is not a validated payment outcome.

A.6 Claim assessment and confidence

Confidence attaches to the proposition being assessed. A dated retained post supports high confidence that the assertion was published. It does not supply the same confidence in the offered file, account or claimed technical route.

Each dossier separates the assertion, established evidence, alternatives, limits and proportionate response. A repeated title or field list can support similar advertising without establishing identical files, an independent source or a completed transfer.

The relationship map connects labels to supporting sources. Unsupported actor associations are omitted. The fraud sequence is explicitly an analytical model, rather than an observed common-operator chain.

A.7 Public-source coverage and chronology

The reviewed public material includes official and press-reported accounts, authority warnings, legal texts and vendor research. The search covered Spanish, English, Portuguese and Russian reporting. Official-source availability and archival coverage remain uneven, so the report does not claim an exhaustive national incident census.

Some official originals were unavailable for source reading. Where a readable original press article reproduces an authority's statement, the report attributes it to that account. Unread leads are excluded from factual incident conclusions. Later publication is not substituted for an earlier event date.

The incident register includes dispositions for retained claim observations and public-source candidates. The closing-period review distinguishes new publications, historical follow-ups, denials, research and events outside the recent window. Source gaps limit coverage; they do not establish that an event did not occur.

A.8 Naming and neutrality

A victim organisation is named only where official confirmation and wider reporting support the name. Other targets use broad role labels. Citations use the publisher's root with an article-URL-withheld notice when the article address would identify a withheld victim.

Actor assertions and state attributions remain their sources' positions. Slurs, recruitment appeals, contacts and working criminal links are omitted. The report takes no position on elections, presidential successions, Congress, parties, protests, government decisions or foreign relations.

Appendix B. Post evidence register

The ten post cards support nine dossiers. B01 and B02 belong to the same recycling discussion. Dates are retained post dates, not independently established acquisition dates. All aliases are withheld in this edition; group branding is assessed separately. [S1]

Card	Date	Venue	Original language	Dossier
B01	2026-01-07	Forum	English	A: citizen-record advertisement
B02	2026-01-07	Forum	English	A: older-material discussion
B03	2026-02-10	Forum	English	B: public-service access
B04	2026-02-16	Forum	English	C: health documents
B05	2026-03-04	Forum	English	D: benefit records
B06	2026-03-27	Forum	English	E: retail access
B07	2026-11-08	Forum	English	F: business records
B08	2026-11-13	Forum	English	G: student and attendance records
B09	2026-11-16	Forum	Spanish	H: education management
B10	2026-11-20	Forum	Spanish	I: employment histories

Appendix C. Sources

Source numbers that do not appear were retired during review and are not cited.

S1: Odin by Brandefense. Peru-associated underground posts, post dates 1 January–22 November 2026. Verified on 22 November 2026. Own-source observation.

S2: Brandefense Ransompedia. Peru and four regional peers, ransomware listing observations. Verified on 22 November 2026. Own-source observation.

S3: Odin by Brandefense. Selected portfolio exposure and passive configuration observations. Verified on 22 November 2026. Own-source observation.

S4: DataReportal. Digital 2027: Peru, October 2026 overview. https://datareportal.com/reports/digital-2027-peru Verified on 22 November 2026. Supporting passage or vulnerability record checked.

S5: El Peruano. Regulation of the Digital Trust Framework, Supreme Decree 126-2025-PCM. https://busquedas.elperuano.pe/dispositivo/EX/2455024-1 Verified on 22 November 2026. Supporting passage or vulnerability record checked.

S6: El Peruano / ANPD. Personal Data Protection Regulation, Supreme Decree 016-2024-JUS. https://cdn.www.gob.pe/uploads/document/file/7568330/6426760-decreto-supremo-n-016-2024-jus-reglamento-de-la-ley-n-29733-ley-de-proteccion-de-datos-personales-publicado-nov-2024.pdf Verified on 22 November 2026. Supporting passage or vulnerability record checked.

S7: SBS. Information security and cybersecurity regulation, Resolution 504-2021, consolidated version. https://intranet2.sbs.gob.pe/dv_int_cn/2046/v5.0/Adjuntos/504-2021.R%20.pdf Verified on 22 November 2026. Supporting passage or vulnerability record checked.

S8: SBS. Proposed unified operational-incident reporting procedure, 16 September 2026. https://www.sbs.gob.pe/noticia/detallenoticia/idnoticia/4000 Verified on 22 November 2026. Supporting passage or vulnerability record checked.

S9: SBS. Prepublication notice for proposed operational-incident reporting procedure. https://intranet2.sbs.gob.pe/Preproyectos/9732JNQOUDCIR5EEENNVGOJQHTGLK7ZKCBB.PDF Verified on 22 November 2026. Supporting passage or vulnerability record checked.

S10: El Peruano. Financial customer communications, SBS Resolution 01741-2026. https://busquedas.elperuano.pe/dispositivo/NL/2530621-1 Verified on 22 November 2026. Supporting passage or vulnerability record checked.

S11: El Peruano. CNSD preventive PHP warning, 26 October 2026. https://www.elperuano.pe/noticia/307672-alerta-por-fallas-informaticas-globales-pcm-activa-medidas-para-proteger-los-datos-de-los-ciudadanos Verified on 22 November 2026. Supporting passage or vulnerability record checked.

S12: PHP Group. Security advisory GHSA-w8hw-w9fx-j79w, 21 October 2026. https://github.com/php/php-src/security/advisories/GHSA-w8hw-w9fx-j79w Verified on 22 November 2026. Supporting passage or vulnerability record checked.

S13: PHP Group. Security advisory GHSA-6wmf-4rv5-p3rp, 21 October 2026. https://github.com/php/php-src/security/advisories/GHSA-6wmf-4rv5-p3rp Verified on 22 November 2026. Supporting passage or vulnerability record checked.

S14: NIST National Vulnerability Database. CVE-2026-109618 record. https://nvd.nist.gov/vuln/detail/CVE-2026-109618 Verified on 22 November 2026. Supporting passage or vulnerability record checked.

S15: NIST National Vulnerability Database. CVE-2026-109619 record. https://nvd.nist.gov/vuln/detail/CVE-2026-109619 Verified on 22 November 2026. Supporting passage or vulnerability record checked.

S17: Latina Noticias. Authority account of unauthorised supplier-account use, 20 May 2026. https://latinanoticias.pe/ (article URL withheld). Verified on 22 November 2026. Article URL withheld; supporting source account read.

S18: El Comercio. Insurer and supervisor statements on customer-information access, 15 October 2026. https://elcomercio.pe/ (article URL withheld). Verified on 22 November 2026. Article URL withheld; supporting source account read.

S19: Infobae. Wider reporting on insurer customer-information incident, 13 October 2026. https://www.infobae.com/ (article URL withheld). Verified on 22 November 2026. Article URL withheld; supporting source account read.

S20: Petroperú. Company warning about an AI-manipulated investment video, 12 June 2026. https://www.petroperu.com.pe/petroperu-alerta-sobre-falso-video-del-presidente-de-directorio-creado-con-inteligencia-artificial Verified on 22 November 2026. Supporting passage or vulnerability record checked.

S21: Gestión. Wider reporting on the company investment-video warning, 14 June 2026. https://gestion.pe/economia/empresas/petroperu-alerta-sobre-video-falso-creado-con-inteligencia-artificial-para-promover-estafa-noticia/ Verified on 22 November 2026. Supporting passage or vulnerability record checked.

S22: RENIEC. Official account of an alleged illegal personal-data sales investigation, 3 July 2026. https://identidad.reniec.gob.pe/b/reniec-participo-de-operativo-contra-la-comercializacion-ilegal-de-datos-personales-en-piura Verified on 22 November 2026. Supporting passage or vulnerability record checked.

S23: El Comercio. Health-service account of unauthorised transfers, 19 August 2026. https://elcomercio.pe/ (article URL withheld). Verified on 22 November 2026. Article URL withheld; supporting source account read.

S24: Infobae. Wider reporting on unauthorised health-service transfers, 19 August 2026. https://www.infobae.com/ (article URL withheld). Verified on 22 November 2026. Article URL withheld; supporting source account read.

S25: Andina. Prosecutor computer-crime complaint statistics for 2024, 2025 and January–July 2026, published 30 September 2026. https://andina.pe/agencia/noticia-como-colaboran-tiktok-roblox-y-meta-las-investigaciones-ciberdelitos-1094008.aspx Verified on 23 November 2026. Supporting passage or vulnerability record checked.

S26: El Peruano. Officially reported warning on transport-fine impersonation, 4 August 2026. https://elperuano.pe/ (article URL withheld). Verified on 22 November 2026. Article URL withheld; supporting source account read.

S27: La República. Authority response to a business-record dataset claim, 9 November 2026. https://larepublica.pe/ (article URL withheld). Verified on 22 November 2026. Article URL withheld; supporting source account read.

S28: Derechos Digitales. Retrospective discussion of an earlier bank incident, 15 November 2026. https://www.derechosdigitales.org/ (article URL withheld). Verified on 22 November 2026. Article URL withheld; supporting source account read.

S29: SBS. Open-finance roadmap, 25 February 2026. https://www.sbs.gob.pe/noticia/detallenoticia/idnoticia/3897 Verified on 22 November 2026. Supporting passage or vulnerability record checked.

S30: SBS. Announcement of updated sanctions framework, 10 April 2026. https://www.sbs.gob.pe/noticia/detallenoticia/idnoticia/3914 Verified on 22 November 2026. Supporting passage or vulnerability record checked.

S31: ESET. FamousSparrow regional research, 17 September 2026. https://www.welivesecurity.com/es/investigaciones/famoussparrow-america-latina-sparrowocky/ Verified on 22 November 2026. Supporting passage or vulnerability record checked.

S32: Kaspersky. Retadup research, 16 November 2026. https://www.kaspersky.com/about/press-releases/kaspersky-dead-retadup-worm-tried-to-infect-at-least-15000-devices-seven-years-after-its-takedown Verified on 22 November 2026. Supporting passage or vulnerability record checked.

S34: RENIEC. Issuer notice of an electrical service interruption, 2 November 2026. https://identidad.reniec.gob.pe/ (article URL withheld). Verified on 22 November 2026. Article URL withheld; supporting source account read.

S35: Ojo Público. Multi-year state data-security investigation, 9 August 2026. https://ojo-publico.com/6464/datos-vulnerados-graves-fallas-seguridad-el-estado-peruano Verified on 22 November 2026. Supporting passage or vulnerability record checked.

S36: Brandefense. Platform demonstration information. https://brandefense.io/request-a-demo/ Verified on 22 November 2026. Supporting passage or vulnerability record checked.

S37: RFC Editor / IETF. RFC 9989, DMARC specification. https://www.rfc-editor.org/info/rfc9989/ Verified on 22 November 2026. Supporting passage or vulnerability record checked.

S38: FIRST. Traffic Light Protocol version 2.0. https://www.first.org/tlp/ Verified on 22 November 2026. Supporting passage or vulnerability record checked.

S39: RFC Editor / IETF. RFC 7208, Sender Policy Framework. https://www.rfc-editor.org/rfc/rfc7208.html Verified on 22 November 2026. Abstract checked.

S40: RFC Editor / IETF. RFC 8659, DNS Certification Authority Authorization. https://www.rfc-editor.org/rfc/rfc8659.html Verified on 22 November 2026. Abstract checked.

S41: RFC Editor / IETF. RFC 8446, Transport Layer Security. https://www.rfc-editor.org/rfc/rfc8446.html Verified on 22 November 2026. Abstract checked.

S42: Microsoft. Security Bulletin MS15-095, RCE abbreviation and code-execution description. https://learn.microsoft.com/en-us/security-updates/securitybulletins/2015/ms15-095 Verified on 22 November 2026. Abbreviation and code-execution description checked.

S43: Red Hat. RHEL 8 System Design Guide, section 6.3.1: root account. https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/8/html/system_design_guide/customizing-the-system-in-the-installer_system-design-guide Verified on 22 November 2026. Root privilege description checked.

S44: GNU. Bash Reference Manual, section 1.2: shell definition. https://www.gnu.org/software/bash/manual/html_node/What-is-a-shell_003f.html Verified on 22 November 2026. Command-interpreter definition checked.

S45: ESET. ESET APT Activity Report Q2 2026–Q3 2026, 28 October 2026. https://www.welivesecurity.com/en/eset-research/eset-apt-activity-report-q2-2026-q3-2026/ Verified on 23 November 2026. Supporting passage or vulnerability record checked.

Appendix D. Plain-language glossary

- **Actor claim:** what a poster or group asserts; publication does not establish accuracy.
- **Atlas national headline:** a single validated exposure summary for the selected portfolio; it is not a national attack probability.
- **BIN:** an issuer-identification prefix in a payment-card number; no card prefix is published here.
- **CAA:** Certification Authority Authorization, a DNS record specifying which certificate authorities may issue certificates for a domain. [S40]
- **C4 certificate:** a Peruvian registration certificate; authenticity requires verification through the legitimate issuer.
- **CNSD:** Centro Nacional de Seguridad Digital, the national digital-security centre.
- **Credential offer:** an advertisement for login information, without proof that the account still works.
- **DDoS:** distributed traffic intended to make a service unavailable; a claim alone does not establish disruption.
- **DNI:** Documento Nacional de Identidad, Peru's national identity document.
- **DMARC:** an email-authentication policy that helps receiving systems handle messages failing the domain's checks. [S37]
- **DNSSEC:** signatures that help validate DNS information; a configuration observation does not establish complete service security.
- **Endpoint:** a device such as a workstation or server; its ownership and activity require local validation.
- **HSTS:** a web policy telling a browser to use HTTPS for the site.
- **Identity recovery:** the process for regaining account access, including checks on who may change authentication details.
- **MFA:** multi-factor authentication, requiring more than one independent factor to sign in.
- **Phishing:** a deceptive request designed to obtain information, access or an action by impersonating a trusted source.
- **Ransompedia listing:** a recorded public criminal assertion, not a confirmed intrusion or unique organisation.
- **RCE:** remote code execution, the ability to run code on a system from elsewhere. In B03 this is an unvalidated seller claim. [S42]
- **Root:** the account with the highest system privileges. B03 does not validate that the seller holds those privileges. [S43]
- **Session revocation:** ending an existing authenticated session so it can no longer be used.
- **Shell:** a command interpreter, used for command-line access. B03 does not validate that the seller has such access. [S44]
- **SPF:** Sender Policy Framework, an email standard letting domain administrators specify which servers may send mail using their domain. [S39]
- **Supplier privilege:** a permission held by an external provider, with a scope and owner that require validation.
- **TLS:** Transport Layer Security, a protocol protecting connections against eavesdropping and alteration. [S41]

- **TLP:CLEAR:** information may be shared without restriction under the traffic-light protocol; other legal duties still apply. [S38]

About this report

Prepared by Odin by Brandefense as the Brandefense Country Report · Peru 2026. The English master and Peruvian Spanish edition share the same evidence boundaries, numbers and identifiers. The Spanish edition carries a visible AI-translation notice and identifies the English master as controlling where they differ.

The report describes the evidence available at the research cut-off. It does not claim a national census, establish a political position or attribute a crime beyond the cited evidence. Recommendations are proposed actions, not assertions about whether a particular organisation has implemented them.

© 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