BRANDEFENSE COUNTRY REPORT · INDONESIA 2026

Brandefense Indonesia Cyber Threat Landscape Report 2026

Exposure signals, contested claims and accountable defence

Odin by Brandefense

Research window: 1 January-22 November 2026

Version 1.0 · Public Research Edition · TLP:CLEAR · 8-22 November 2026

101/250
Assessed domains with a credential listed for sale when checked

18
Dossiers with different evidence status

28
Extortion-group labels in Ransompedia

90
Days of sequenced improvement, not a delay for live threats

CONTENTS

Contents

01	Executive summary	06
	Report map	11
02	Digital context	12
03	Selected-organisation exposure	16
04	Dark-web evidence	26
05	Sector decisions	53
06	Disruption and claim assessment	58
07	Threat actors and relationships	63
08	Fraud economy	78
09	Banking and financial services	83
10	Regulatory response	89
11	Conditional outlook	95
12	Accountable action plan	99
	Appendices	105
A	Appendix A. Scope and evidence boundaries	106
B	Appendix B. Redacted evidence register	108
C	Appendix C. Source verification records	110
D	Appendix D. Glossary	113

Board and executive leadership	01 10 11 12
CISO and incident commander	01 04 06 07 12
Identity and application owners	03 04 05 08 09
Infrastructure and continuity owners	02 03 05 06 12
Privacy, legal and communications	04 06 09 10
Financial-crime and customer operations	05 08 09 12

About this edition

Brandefense Country Report · Indonesia 2026

AI assisted research and drafting. This English master governs translated editions.

Observation window: 1 January to 22 November 2026. Recent period: 8 to 22 November 2026. Observations were captured before the end of 22 November.

Indonesia's evidence supports distinct decisions for access validation, service continuity and notification readiness, while limiting what advertisements and publication dates can establish.

Headline	Meaning
101/250	Assessed organisation domains with a credential listed for sale when checked
59/100	National Atlas headline for the selected portfolio
74	Indonesia-tagged extortion listings in Ransompedia during the observation window
28	Group labels associated with those listings
6	Listings dated within the recent period
241/250	Selected candidate domains with passive observations; nine were unavailable

The listing figures describe Ransompedia observations. They do not establish 74 confirmed ransomware incidents, 74 unique victims or 74 successful intrusions. The selected portfolio does not represent all Indonesian organisations. [S2][S3][S4]

Contents and reading routes

Chapter	The question it answers
1. Executive summary	Which decisions should leadership fund and require now?
2. Digital context	Which dependencies shape the consequences of exposure?
3. Selected-organisation exposure	What can the selected portfolio establish about observable controls?
4. Dark-web evidence	Which claims merit validation, and which propositions remain unresolved?
5. Sector decisions	How do the same signals create different operational consequences?
6. Disruption and claim assessment	How should defenders distinguish warnings, outages and attack claims?
7. Threat actors and relationships	Which actor links are supported by which evidence?
8. Fraud economy	How do access, identity material and payment records require different responses?
9. Banking and financial services	How should financial institutions combine transaction, identity and service evidence?
10. Regulatory response	Which recipients, triggers and deadlines apply?
11. Conditional outlook	Which signals would change the assessment?
12. Accountable action plan	Who owns the next 30, 60 and 90 days of work?
Appendix A	Scope, populations and confidence language
Appendix B	Redacted case and evidence register
Appendix C	Sources and verification dates
Appendix D	Glossary

Leaders can begin with Chapters 1, 10 and 12. Security operations teams can follow Chapters 4, 6 and 7 into the evidence register. Identity, infrastructure and application owners can use Chapters 3, 5, 8 and 9.

The report distinguishes an observed publication from its underlying allegation. It also separates an organisation's disclosure, an official investigative account and vendor research. A source's attribution remains that source's assessment.

Evidence label	What it supports	What it does not automatically support
Own observation	A retained post, listing or measured condition exists within its stated population	The advertised access works or a theft occurred
Actor claim	A persona advertised an allegation or capability	A confirmed incident, completed sale or identified operator
Official or controller account	The particular facts the authority or organisation reported	Every seller allegation associated with the same theme
Vendor research	The activity and interpretation described by the named publisher	An Indonesian official attribution or complete national picture
Analytical inference	A stated interpretation connecting supported propositions	A new observation or independent confirmation

Dates retain their meaning throughout. A post date records publication. A listing date records an extortion listing. Discovery, notification, attack activity and public reporting can occur on different days.

CHAPTER 01

Executive summary

01

THIS CHAPTER ANSWERS

Which decisions follow from Indonesia's evidence without treating claims as confirmed incidents?

74

Extortion listings observed during the window

1.1 Six findings for leadership 07
1.2 Four decisions for leaders 08
1.3 The year in numbers 08
1.4 What changes a response decision 09
1.5 How to use the report 09

CHAPTER 01

Executive summary

IN SHORT

Indonesia's evidence requires three response tracks: validate advertised access, prepare for service disruption and preserve notification readiness. Ransompedia records 74 extortion listings across 28 group labels. Public cases include a financial theft investigation, customer-platform access and website abuse. Vendor reporting adds targeted campaigns, with important limits on dates and attribution. These populations do not form a national incident total. Assign owners to validate live access, rehearse recovery and maintain regulator-ready incident records.

1.1 Six findings for leadership

1. **Extortion listings span several operationally important sectors.** Ransompedia records 74 Indonesia-tagged listings during the window. Energy and extractives account for 13, while digital and professional services account for 12. These are listing categories, not confirmed loss events. [S2]

1. **Recent access offers require current-account evidence.** A 22 November post advertised university VPN access and claimed domain-administrator privilege. An October offer alleged agricultural remote access. Cards B03 and B04 preserve the advertisements. Identity owners should validate accounts, sessions and permissions before deciding containment. [S1]

1. **Official cases demonstrate several kinds of consequence.** Police describe transaction losses in a regional-bank investigation and a school-funding case. Other sources concern customer-platform access, disputed personnel-data exposure and website defacement. Their units and evidentiary status differ. Adding their records, accounts, websites and money would produce a meaningless total. [S35][S36][S40][S41][S44]

1. **Publication in 2026 does not establish activity in 2026.** Check Point's February Amaranth-Dragon report describes Indonesia operations in August and September 2025. Kaspersky's StrikeShark publication does not supply an exact intrusion date in the supporting account. The report therefore preserves historical and unknown-date distinctions. [S21][S43]

1. **Reporting readiness has several clocks.** The PDP statute specifies written notice within 3 × 24 hours in the event of a protection failure. Scoped IIV, OJK and BI requirements have separate recipients and triggers. A common incident record should support those duties without replacing their distinct legal tests. [S6][S12][S15][S18]

1. **Current credential listings require validation across the selected portfolio.** In the exposure snapshot, 101 of 250 assessed organisation domains had a credential listed for sale. The national Atlas headline is 59/100. These signals establish neither active account validity nor confirmed intrusion. Assign current-account and endpoint checks to their relevant owners. [S4]

1.2 Four decisions for leaders

Fund identity validation and evidence retention. Require the identity owner to determine whether advertised accounts remain valid, who owns them and whether earlier remediation already addressed them. Preserve the evidence behind each decision.

Require recovery evidence from service owners. Ask for an observed restoration exercise covering a business service, its identity dependencies and its external suppliers. A backup inventory alone does not establish a recovery outcome.

Approve a shared notification workflow. Legal, privacy, security and business owners should agree how facts enter an incident record. The workflow must retain discovery times, occurrence estimates, affected systems and delivery acknowledgements.

Separate customer protection from public attribution. Communications can explain service status and protective steps while investigators assess access, data scope and responsibility. An unsupported actor label adds little to immediate customer protection.

1.3 The year in numbers

101/250

Assessed domains with a credential listed for sale when checked

WHAT IT IS NOT

Confirmed breaches or active accounts

59/100

National Atlas headline for the selected portfolio

WHAT IT IS NOT

National prevalence or incident probability

332,251

Country-tagged posts in the metadata population

WHAT IT IS NOT

Verified targeting, retained relevant posts or distinct incidents

74

Ransompedia listings dated within the report window

WHAT IT IS NOT

Confirmed Indonesian ransomware incidents

28

Group labels attached to those listings

WHAT IT IS NOT

A proven count of independent criminal organisations

6

Ransompedia listings in the recent period

WHAT IT IS NOT

All cyber incidents from 8 to 22 November

241/250

Candidate domains with passive observations

WHAT IT IS NOT

National coverage or an organisational rating

166/241	12	3 × 24 hours	1 hour
Domains with DMARC quarantine/reject policy observed	Listings in digital and professional services	PDP statute's written-notice requirement in its stated circumstances	BI initial cyber-notification period within the regulation's scope
WHAT IT IS NOT	WHAT IT IS NOT	WHAT IT IS NOT	WHAT IT IS NOT
Complete delivery enforcement or proof that mail was blocked	A measure of downstream supplier impact	A universal replacement for sector reporting	A deadline for every Indonesian business

Passive results describe observations for 241 of 250 candidate domains. Their control-specific coverage does not establish attack success or national prevalence. [S3][S4]

The recent six listings involve four labels: Panzer, N0n, INC Ransom and Pixelleaks. N0n and INC Ransom each account for two. The other labels each account for one. Those six listings form part of November's nine observed listings, alongside three dated from 1 to 7 November. Neither publication frequency nor a label's presence establishes successful intrusion or encryption. [S2]

1.4 What changes a response decision

An alert should identify the proposition that requires validation. For an access offer, that proposition concerns current access. For a data offer, it concerns provenance and scope. For a disruption warning, it concerns service impact and readiness.

A validated active account requires a different response from a previously disabled account in a recirculated dataset. Both deserve a recorded disposition. Only the first supports immediate containment based on current access.

A listing can justify contact with the organisation's incident owner and a review of existing telemetry. It cannot establish the initial access route, malware execution, encryption or ransom payment without additional evidence.

The same discipline applies to official reporting. A police announcement establishes an investigative account. A controller notice establishes what the controller disclosed. An unresolved investigation should not become a final finding of fault in a summary.

1.5 How to use the report

The sector chapters translate evidence into owner-specific work. The actor chapter keeps relationships tied to their sources. The legal chapter preserves recipients and timing. The action plan provides triggers and completion evidence for each task.

Appendix A explains why the figures remain separate. Appendix B links dossiers and cards. Appendix C records the sources used, including their verification dates. No public raw victim identifiers or contact details are reproduced.

KEY TAKEAWAYS

01

Validate current access before deciding containment

02

Require service restoration evidence from named owners

03

Prepare one factual incident record for several notification duties

Report map

Choose a route by the decision you own. Each route leads from a supported observation to a validation step and a documented result.

Board and executive leadership	Which capabilities and accountability need funding?	01 10 11 12
CISO and incident commander	Which propositions require validation or escalation?	01 04 06 07 12
Identity and application owners	Which accounts, sessions and integrations require checks?	03 04 05 08 09
Infrastructure and continuity owners	Which dependencies must survive disruption?	02 03 05 06 12
Privacy, legal and communications	Which facts support notification and public statements?	04 06 09 10
Financial-crime and customer operations	Which transaction or identity signals justify protective action?	05 08 09 12

Chapter	Read it to establish
1	The decisions and numerical limits that govern the report
2	A dependency-based view of digital services
3	The boundaries of selected-portfolio measurements
4	What each retained claim or public case can establish
5	How validation and impact differ across sectors
6	Why an advisory, an outage and an attack claim are separate events
7	Which edges in an actor map have supporting evidence
8	How to respond to identity and payment-material claims
9	How finance combines access, transaction and continuity controls
10	How to preserve legal scope, triggers and deadlines
11	Which changes would support escalation or de-escalation
12	How to assign and close work with evidence

CHAPTER 02

Digital context

02

THIS CHAPTER ANSWERS

Which digital dependencies shape the consequences of an access or availability incident?

3

Distinct clocks: activity, discovery and publication

2.1 A dated baseline for a current decision 13
2.2 Identity connects several consequences 14
2.3 Central coordination does not remove service ownership 14
2.4 Shared infrastructure can transmit collateral impact 14
2.5 Preparedness messages require operational translation 15
2.6 Context sets impact, not attribution 15

CHAPTER 02

Digital context

IN SHORT

Digital dependence makes identity, applications and shared services operational concerns. Context must retain its dates: the Digital 2026 Indonesia report was published in late 2025 using observations available then. Public 2026 accounts show how customer platforms, financial systems, websites and shared infrastructure create different consequences. They do not establish a single national attack trend. Map the dependencies of each critical service and test the decisions that follow a loss of access or availability.

2.1 A dated baseline for a current decision

DataReportal's Digital 2026 Indonesia report was published on 5 November 2025. Its supporting passage identifies October 2025 and other late-2025 observations as the latest available baseline. The report title should not be mistaken for a measurement made at this cutoff. [S81]

Late-2025 baseline	Figure	Unit and limit
Internet users	230 million	Users in the dated baseline
Internet penetration	80.5%	Share of the population in that baseline
Cellular connections	331 million; 116% of population	Connections are not unique people, and not all were internet-enabled

These observations were published in November 2025. They are not a measurement at the current cutoff or an affected population. [S81]

This report uses that source for digital-connectivity context. It does not turn internet use, mobile connections or platform identities into an estimate of affected people. A connected population and an affected population are different units.

For historical national-monitoring context, BSSN reported 403,990,813 traffic anomalies in 2023 and 330,527,636 traffic anomalies in 2024. [S96][S97] Those annual figures count traffic anomalies within BSSN monitoring coverage rather than confirmed intrusions or unique victims. [S96][S97] They provide a bounded year-on-year monitoring reference and cannot be combined with 2026 dark-web post counts, extortion listings or portfolio exposure observations.

The operational question is dependency. A customer journey can rely on registration, identity recovery, messaging, payment processing and a supplier's application. An incident can affect one component while others remain available.

A dependency map should identify who can authorize protective changes. It should also identify who can explain customer impact. Those responsibilities need not belong to the same team, but they should share a factual incident record.

2.2 Identity connects several consequences

The regional-bank investigation concerns unauthorized transactions and alleged system intrusion. The customer-platform disclosure concerns account-related information. The website investigation concerns access sold for content abuse. Each connects identity to a different operational outcome. [S36][S38][S44]

This distinction changes validation. A website administrator account requires review of content changes, access paths and deployment history. A financial account requires transaction evidence and customer protection. An application account requires assessment of the data and functions it could access.

A password appearing in a dataset cannot answer those questions alone. The organisation must determine whether the account exists, whether it remains enabled and whether associated sessions or tokens survive a password change.

The investigation should also distinguish employee, supplier and customer access. A corporate-looking address does not establish an employee relationship. A supplier's account can create a dependency without proving a supplier-wide incident.

2.3 Central coordination does not remove service ownership

Perpres 82/2022 describes national, sectoral and organisational incident-response teams for IIV. It makes BSSN the coordinator of protection and assigns sector responsibilities to ministries or regulators. Organisational response remains part of that structure. [S12][S13]

Central coordination helps establish reporting paths and assistance. It does not replace an application's asset owner or a service owner's restoration decision. An organisation still needs to know which identities, systems and suppliers support a critical service.

The same principle applies to financial supervision. OJK's 2026 commercial-bank IT regulation addresses governance, risk management, third parties and data protection. BI's framework addresses information security and cyber resilience within its own scope. [S16][S18]

A practical service register should connect those requirements to operations. It should show the business service, its data controller, technical owner, privileged identities, supplier dependencies and applicable reporting contacts.

2.4 Shared infrastructure can transmit collateral impact

Komdigi reported that access to a software-development service was disrupted for around four hours on 6 November. A shared IP address had entered malware-related blocking. Access was restored after that address was removed. [S47]

That account supports a blocking-related availability event. It does not support an intrusion into the development platform. It also illustrates why a shared address is an imperfect substitute for a service identity.

For defenders, the relevant decision is controlled change and recovery. A protective block should have an owner, an assessment of shared dependencies and a route for urgent review. Where possible, service-specific evidence should inform the decision.

Business continuity should include external identity, development, messaging and support dependencies. A business can lose a workflow without losing control of its own servers. The report therefore distinguishes attack response from broader service recovery.

2.5 Preparedness messages require operational translation

Komdigi's 10 November notices relay BSSN coordination and preparedness activity. The account recommends monitoring, patching, authentication measures and recovery readiness. It does not confirm that every warned-of attack occurred. [S48][S49]

A useful response converts the advisory into a short list of owned checks. The infrastructure owner confirms internet-facing patch status. The identity owner checks privileged access. The continuity owner verifies a recovery route.

The incident commander records what prompted those checks. An advisory can justify increased readiness while its underlying threat claim remains unverified. This avoids two errors: dismissing preparedness entirely or declaring a completed incident without evidence.

2.6 Context sets impact, not attribution

The public sources describe different sectors and dependencies. Historical BSSN traffic-anomaly totals for 2023 and 2024 likewise measure national monitoring volume rather than a single 2026 incident trend. [S96][S97] They do not demonstrate that every event shares an operator, motive or initial access method. Similar targets can reflect similar opportunities rather than coordination.

Vendor state-alignment assessments remain attributed to their publishers in Chapter 7. Language, a lure's subject and a public warning do not independently establish the operator's identity.

The report therefore uses context to explain business consequences. It does not infer a political cause for a cyber event or adopt the rhetoric of a threat actor. Operational decisions depend on access, impact and evidence.

KEY TAKEAWAYS

01
Keep baseline observation dates visible

02
Map identity and supplier dependencies to critical services

03
Convert preparedness notices into owned checks with recorded outcomes

CHAPTER 03

Selected-organisation exposure

03

THIS CHAPTER ANSWERS

What can a selected domain portfolio establish without claiming national prevalence?

101/250

Assessed domains with a credential listed for sale when checked

3.1 Universe and interpretation 17
3.2 Observable conditions and business decisions 17
3.3 Exposure records are prompts for validation 22
3.4 Observable sector signals retain their scope 24
3.5 Validation should end in a service-level result 24
3.6 Leadership questions for the portfolio 25

CHAPTER 03

Selected-organisation exposure

IN SHORT

Of 250 assessed organisation domains, 101 had a credential listed for sale when checked. The national Atlas headline is 59/100. The portfolio contains at least 1,178,666 device associations and 6,353,372 credential-record associations. These populations overlap and do not establish current compromise. Passive observations cover 241 domains, with separate coverage for TLS and HTTP. Validate current listings and employee relationships, then close control exceptions with production evidence.

3.1 Universe and interpretation

Population	Unit	Interpretation
Selected candidate portfolio	250 primary domains	A purposive portfolio for organisation-level context
Passive-control observations	Assessed domains for each control	A condition observed within the stated coverage
Current access advertisements	Organisations or accounts under a defined observation	A validation signal with its own time meaning
Credential and device associations	The stated record or association unit	Evidence requiring account and ownership checks
Public report cases	Dossiers with different evidence types	Examples of consequences, not a representative incident survey

The candidate portfolio is an analysis boundary. It is not a claim that the largest 250 organisations were measured completely. A domain can represent a service, group, subsidiary or shared operational boundary. [S4]

A control's denominator should follow the records actually assessed. An unavailable observation cannot become a zero. Nor does a missing response establish an absent control throughout the organisation.

The portfolio contains 250 candidate primary domains in ten merged sector cells. Each passive observation retains its own assessed denominator. [S4]

3.2 Observable conditions and business decisions

The national Atlas headline is 59/100 for the selected portfolio. Higher values indicate greater observed exposure. This figure is not a breach percentage, incident probability or control certification. Only the national headline is published. [S4]

59/100

National Atlas headline for the selected 250-domain portfolio

101/250

Assessed organisation domains with a credential listed for sale when checked

Atlas exposure data were read on 22 November 2026. Device and credential observations can include historical records and relationships outside the organisation's own workforce. The rating does not establish that those records first appeared during the report window. [S4]

Passive email and web observations describe conditions at the assessment point. A policy record can support a statement about that record. It cannot establish whether a phishing message reached a user or caused an account compromise. [S3]

The control owner should validate the result against the production service. A domain can have inherited settings, a separate sending service or a planned migration. Those explanations require evidence before the finding is closed.

The useful output is an owned exception list. Each exception should have a service owner, a consequence and a completion test. A change ticket closes only after the resulting condition is checked.

Observations were available for 241 of the 250 selected candidate domains on 22 November. Nine domains were unavailable. These are domain-level observations, not a count of independently verified organisations. [S3][S4]

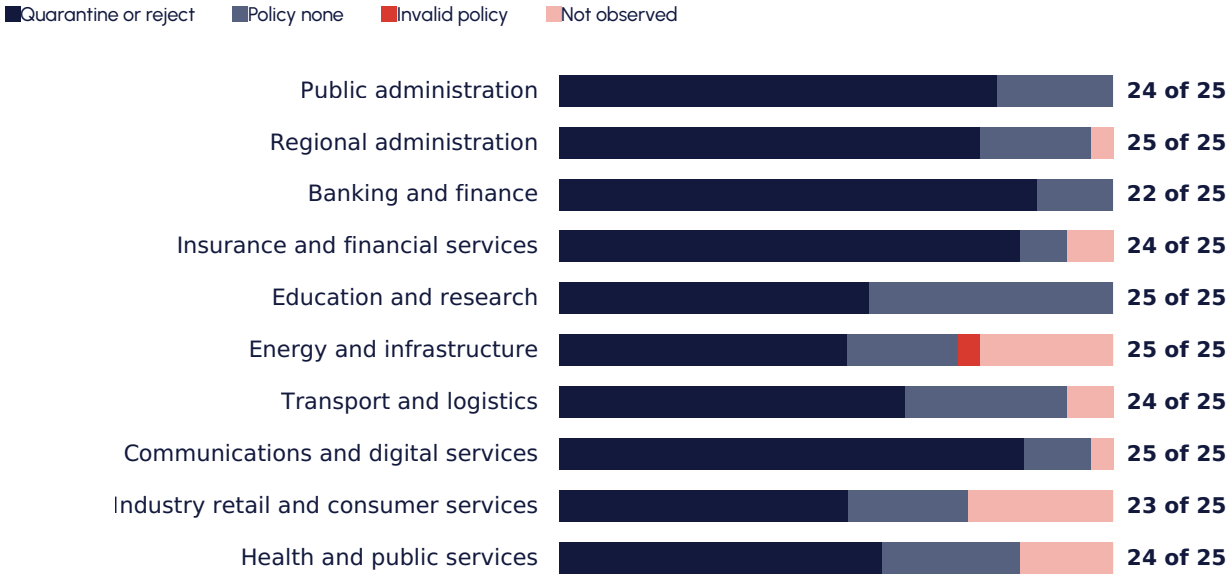
Control definitions and the limits of these observations appear in Appendix D.

Email or DNS observation	Count	Base
DMARC quarantine/reject policy observed	166	241
DMARC none policy observed	52	241
DMARC policy invalid	1	241
DMARC policy not observed	22	241
SPF record observed	230	241
DKIM-related record observed	169	241
DNSSEC delegation evidence observed	33	241

The DMARC quarantine/reject count comprises 63 reject and 103 quarantine policies. Policy presence does not establish complete delivery enforcement, including the treatment of every message. [S3]

SPF and DKIM-related records do not validate message delivery or authentication outcomes. A DKIM-related or DNSSEC observation that is not present here does not establish service-wide absence. Each owner should confirm the relevant production configuration.

DMARC policy observations vary across selected sector portfolios



Source: passive observations for 241 of 250 selected candidate domains, 22 November 2026 [S3]. Sector denominators are observed domains. Policy presence does not establish message enforcement; an unavailable observation does not prove an absent control.

Sector	Observed domains	DMARC quarantine/ reject	SPF	DKIM-related	DNSSEC evidence
Public administration	24	19	23	13	12
Regional administration	25	19	25	14	5
Banking & finance	22	19	22	13	4
Insurance and financial services	24	20	24	19	3
Education and research	25	14	25	23	3
Energy and infrastructure	25	13	23	15	0
Transport and logistics	24	15	24	20	1

Sector	Observed domains	DMARC quarantine/ reject	SPF	DKIM-related	DNSSEC evidence
Communications and digital services	25	21	23	21	4
Industry retail and consumer services	23	12	20	13	0
Health and public services	24	14	21	18	1

Each sector contains 25 selected candidate domains. The observed-domain column is the denominator for its email and DNS counts. Counts describe records observed, not sector ratings or phishing success. [S3][S4]

TLS status	Count	Base
Valid	205	241
Invalid	13	241
Unavailable	23	241

Sector	TLS valid	TLS invalid	TLS unavailable	Base
Public administration	18	1	5	24
Regional administration	20	3	2	25
Banking & finance	18	1	3	22
Insurance and financial services	20	1	3	24
Education and research	21	1	3	25
Energy and infrastructure	24	0	1	25
Transport and logistics	23	0	1	24
Communications and digital services	23	1	1	25
Industry retail and consumer services	17	5	1	23
Health and public services	21	0	3	24

TLS status and HTTP coverage are separate. HTTP observations were available for 154 of the 241 observed domains. The header counts below use 154, rather than 241, as their denominator. [S3]

Header observation	Count	Base
HSTS	103	154
Content Security Policy	67	154
Frame-protection header	93	154
Content-type protection header	91	154

Sector	HTTP observations	HSTS	CSP	Frame	Content type
Public administration	11	9	6	7	9
Regional administration	17	9	4	9	7
Banking & finance	10	9	7	5	8
Insurance and financial services	12	11	7	10	10
Education and research	16	9	7	12	10
Energy and infrastructure	20	12	10	11	12
Transport and logistics	15	9	3	7	7
Communications and digital services	18	13	9	13	10
Industry retail and consumer services	17	11	9	12	11
Health and public services	18	11	5	7	7

Each sector's HTTP-observation count is the denominator for its header counts. An unavailable HTTP observation does not establish that a header is absent throughout a service. These conditions do not establish exploitation, a data incident or control effectiveness. [S3]

3.3 Exposure records are prompts for validation

A historical credential record supports a different response from a currently advertised privileged account. The former requires freshness and prior-remediation checks. The latter requires urgent validation of the alleged current access.

Device associations also need interpretation. An association can involve an employee, contractor, customer or another relationship. The report does not infer the person's role from a domain string alone.

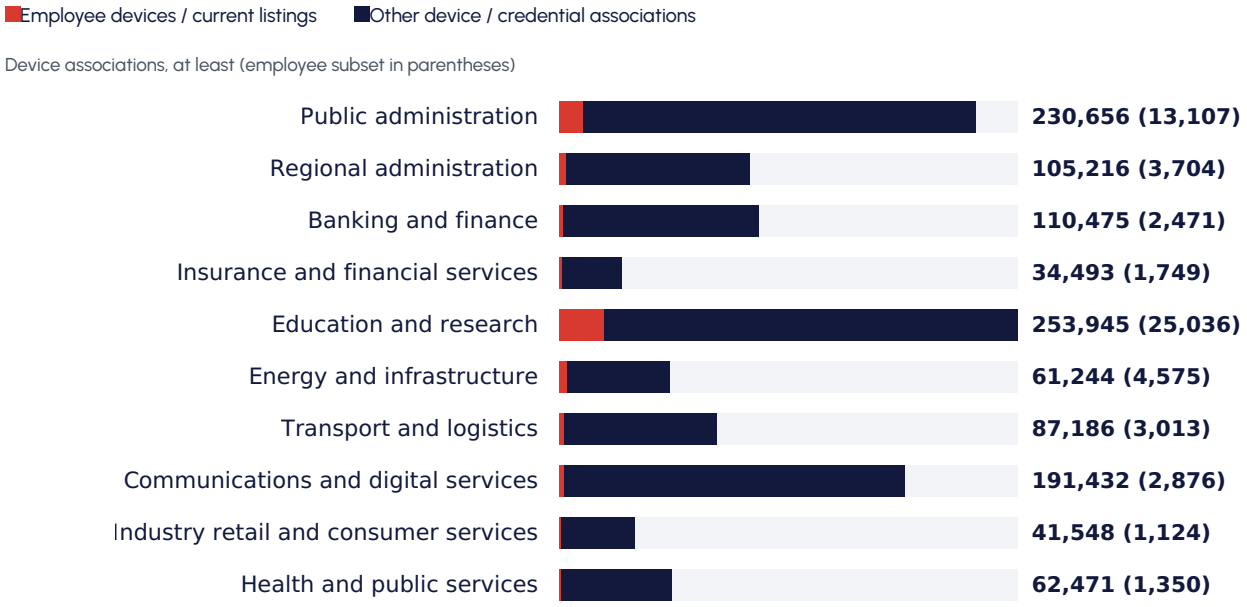
When identity owners validate exposure, they should record the account state at the decision time. That record should distinguish disabled, changed, active and unknown outcomes. Current-account evidence should precede disruptive resets.

Of 250 assessed organisation domains, 101 had a credential listed for sale when checked. Device associations were present for 243 domains; 234 had employee-device associations, and 246 had credential-record associations. These overlapping signals do not count confirmed intrusions. [S4]

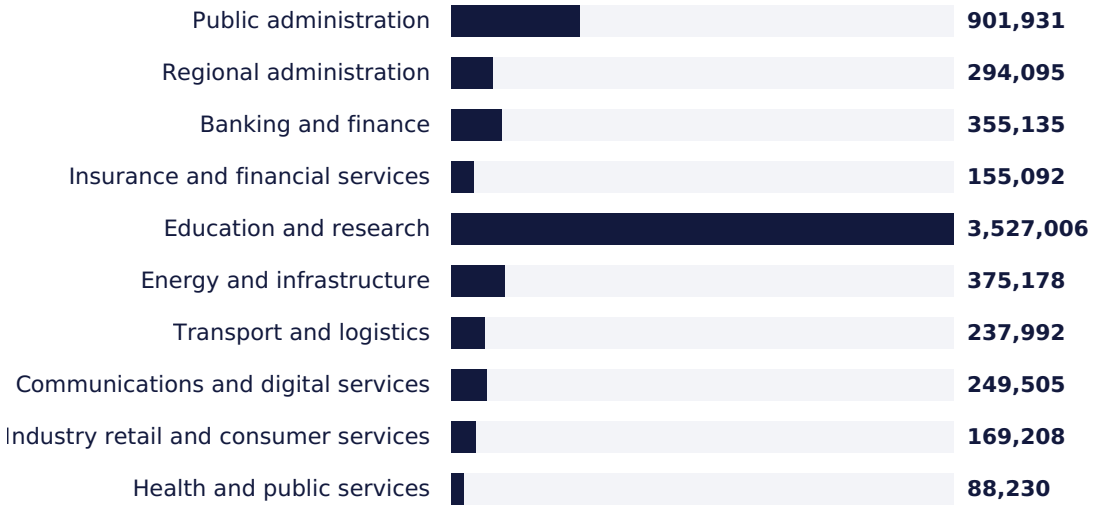
The portfolio contains at least 1,178,666 device associations, including 59,005 employee-device associations. Credential-record associations total 6,353,372. The snapshot also records 1,516 document associations and 32,205 lookalike observations in the preceding 30 days. [S4]

Employee-device associations form part of the device view and must not be added to it. Device associations can overlap across domains and include customer or other relationships. Credential records are not unique people, active accounts or confirmed thefts.

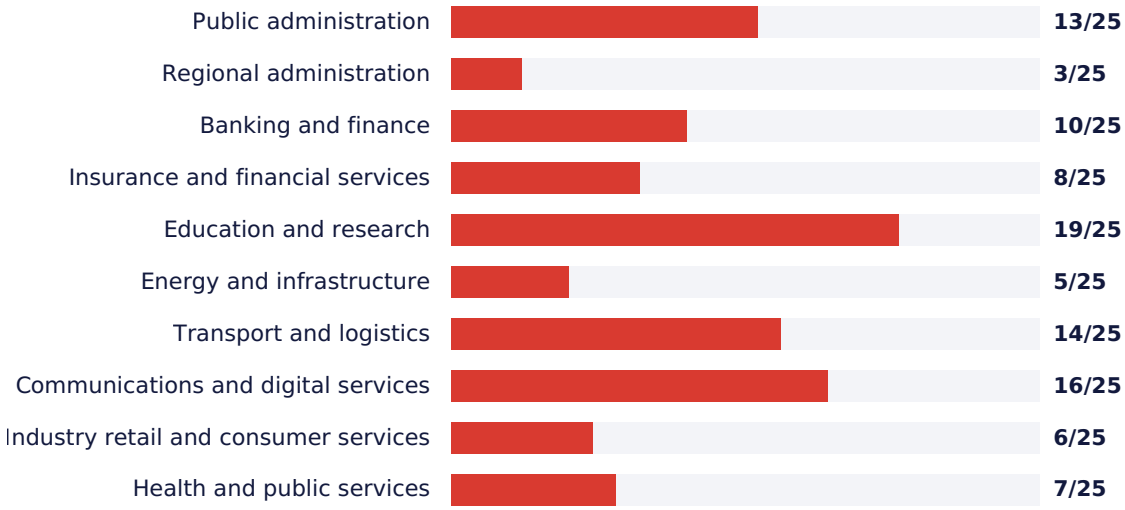
Sector device and credential populations differ in scale and meaning



Credential-record associations (separate scale)



Current credential listings by sector (coral)



Source: Brandefense Atlas exposure observations for 250 assessed domains, 22 November 2026 [S4]. Device associations are lower bounds; employee devices are a subset. Credential records are not unique people, active accounts or confirmed theft.

Sector	Domains	Devices, at least	Employee devices	Credential records	Currently listed domains	Documents	Lookalikes, 30 days
Public administration	25	230,656	13,107	901,931	13	252	359
Regional administration	25	105,216	3,704	294,095	3	45	167
Banking & finance	25	110,475	2,471	355,135	10	395	5,072
Insurance and financial services	25	34,493	1,749	155,092	8	55	6,110

Sector	Domains	Devices, at least	Employee devices	Credential records	Currently listed domains	Documents	Lookalikes, 30 days
Education and research	25	253,945	25,036	3,527,006	19	195	3,751
Energy and infrastructure	25	61,244	4,575	375,178	5	158	1,508
Transport and logistics	25	87,186	3,013	237,992	14	106	2,854
Communications and digital services	25	191,432	2,876	249,505	16	220	2,214
Industry retail and consumer services	25	41,548	1,124	169,208	6	39	9,046
Health and public services	25	62,471	1,350	88,230	7	51	1,124
Total	250	1,178,666	59,005	6,353,372	101	1,516	32,205

Each sector contains 25 assessed domains. Counts support anonymous description of this selected portfolio. Documents require ownership and sensitivity checks; name similarity alone does not establish malicious impersonation. Device totals are lower bounds, and no national prevalence follows from these counts. [S4]

3.4 Observable sector signals retain their scope

Sector discussion uses the observable conditions and case evidence presented here. No sector or group Atlas ratings are reported. A sector count does not estimate national prevalence.

A domain-associated exposure observation does not validate a retained access advertisement. An advertisement does not establish that a historical record remains active. Each evidence type retains its own population and validation task.

3.5 Validation should end in a service-level result

For an email-policy exception, completion means the domain owner confirmed the intended policy and the assessed record reflects it. A change request without a resulting observation is incomplete.

For an advertised account, completion means the identity owner established the account's status and reviewed relevant activity. Containment follows confirmed current risk. The incident owner records why broader action was or was not required.

For a lookalike or document-related signal, completion means the business owner assessed the relationship and consequence. A similar name alone does not establish impersonation. A mention alone does not establish internal-data loss.

3.6 Leadership questions for the portfolio

The board should ask whether critical services have owners for external exposure. It should also ask how quickly those owners can validate an account claim and how they prove a control change reached production.

The national headline helps frame portfolio priorities. Current listings and employee-device relationships still need an asset owner, a current-account check and a recorded validation result. Passive-control observations require their own service-level completion tests.

The portfolio chapter should therefore be read as a decision aid. Its value lies in connecting a bounded observation to a proportionate action and a documented result.

KEY TAKEAWAYS

01
Preserve the assessed denominator for every control

02
Validate account status before disruptive response

03
Close findings with production evidence from the service owner

CHAPTER 04

Dark-web evidence

04

THIS CHAPTER ANSWERS

Which observations justify investigation, and which claims remain unresolved?

18

Dossiers with different evidence status

4.1 The retained post population 27
4.2 From a claim to a decision 30
4.3 Nine retained-corpus dossiers 31
4.4 Six external dossiers 40
4.5 Additional access and extortion propositions 46
4.6 Repeated data does not establish repeated intrusion 49
4.7 The recent period has its own limits 49
4.8 Additional themes retain their narrower propositions 50
4.9 Further service and relay observations 51

CHAPTER 04

Dark-web evidence

IN SHORT

A post establishes that a claim was published. It does not establish working access, a completed sale or a new intrusion. Official and controller accounts support stronger propositions, but each retains its own limits. The dossiers below separate publication, activity, disclosure and follow-up dates. Their figures cannot be added into a national total. For every relevant allegation, identify the proposition to validate, the owner who can test it and the evidence that will close the decision.

4.1 The retained post population

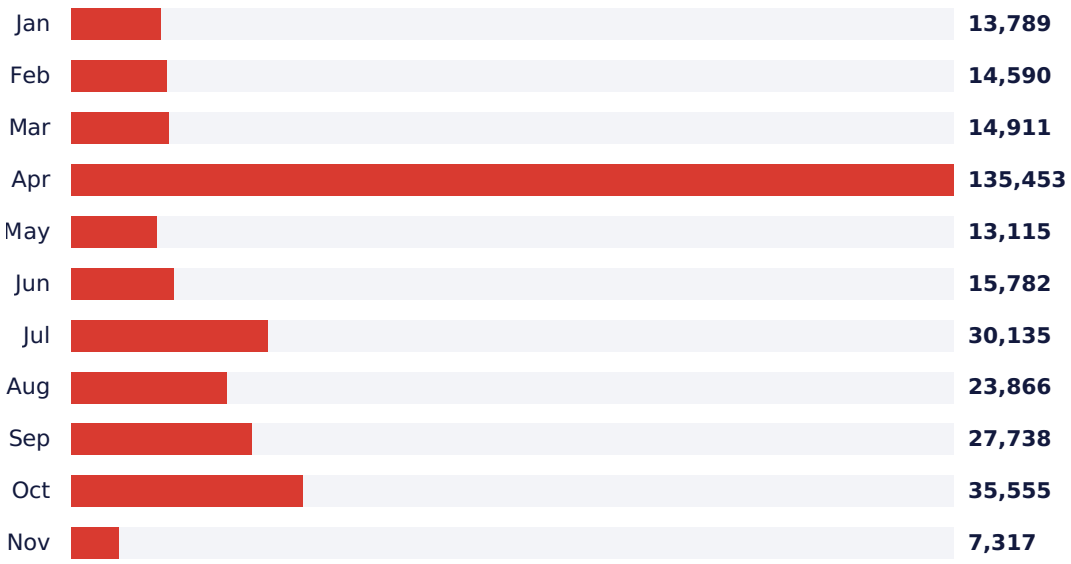
Brandefense Blackhole observations and Ransompedia listings answer different questions. Posts show what personas published in the retained corpus. Extortion listings show the dated listing population. A public incident account can describe an event that appears in neither population. [S1][S2]

A country tag does not establish that the target is in the country. A seller can reuse old data, repeat an advertisement or describe infrastructure outside the claimed victim's control. The report preserves those alternatives.

The retained corpus is therefore not presented as an Indonesian incident census. Exact population counts, where available, remain separate from the selected evidence cards and dossiers. Multiple messages can concern one allegation.

The country-tagged metadata total is 332,251 posts. The retained corpus contains 19,814 distinct posts within the window. These are different coverage populations; the retained corpus is not a fraction from which national relevance can be estimated. [S1]

April has the largest country-tagged metadata volume



Source: Brandefense Blackhole, 332,251 Indonesia-tagged metadata posts, 1 January–22 November 2026; closing day partial [S1]. Separate from the 19,814 retained posts; not targeting or incident counts.

Month	Country-tagged posts
January	13,789
February	14,590
March	14,911
April	135,453
May	13,115
June	15,782
July	30,135
August	23,866
September	27,738
October	35,555
November through extraction	7,317

The April value is a publication-volume observation. It does not establish a surge in targeting or successful intrusions. November is partial through the extraction on 22 November and cannot be compared with complete months as a full-month result. [S1]

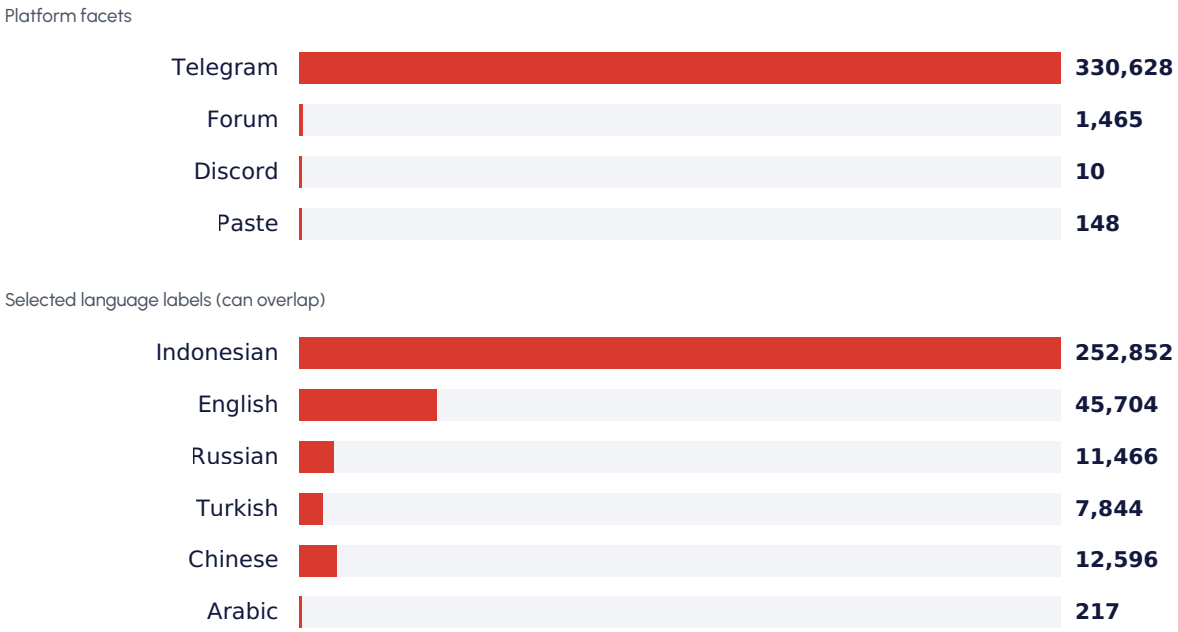
Platform	Country-tag facet	Retained corpus
Telegram	330,628	17,340
Forum	1,465	2,466
Paste	148	7
Discord	10	1

The table shows platforms with observations.

The platform facets and country-tag total both equal 332,251 as observed on 22 November 2026. This agreement concerns metadata, not verified targeting or confirmed incidents. [S1]

The retained forum count is not a subset of the country-tag forum facet. The populations have different coverage. Their totals should not be combined or used to calculate a national incident share.

Platform and language facets describe metadata visibility



Source: Brandefense Blackhole, 332,251 Indonesia-tagged metadata posts, 1 January–22 November 2026; closing day partial [S1]. Separate from the 19,814 retained posts; not targeting or incident counts.

Selected language label	Tagged posts
Indonesian	252,852
English	45,704
Chinese	12,596
Russian	11,466
Turkish	7,844
Arabic	217

Language labels can overlap, and the table shows six selected languages. It is not a mutually exclusive partition. Language does not identify an operator's nationality or establish who was targeted. [S1]

The retained recent country-tagged population contains 5,443 posts: 5,395 Telegram, 47 forum and one Discord. These are posts, not distinct incidents. The recent university and identity-material offers illustrate the need for current-state validation. [S1]

4.2 From a claim to a decision

A useful investigation begins with the advertised capability. "Data", "administrator" and "access" do not imply the same permissions. The service owner should determine which proposition matters to the organisation's present risk.

For a data offer, relevant questions concern provenance, time period and whether the material contains the organisation's information. For an access offer, relevant questions concern an existing account, current validity and the permissions it provides.

A credible-looking sample does not resolve every proposition. A historical sample can support data possession while leaving current access unproven. A screenshot can show a session without establishing its duration, origin or scope.

The response should preserve those differences. An identity alert should reach an identity owner. A customer-data allegation should reach the controller's privacy and incident teams. An extortion listing should activate an established review route.

Evidence state	Immediate question	Accountable owner	Completion evidence
Account or privileged-access claim	Is an owned account currently valid, and what can it reach?	Identity and service owners	Account state, session review and access scope
Data-sale allegation	Does the material match owned data, and from which period?	Data owner and privacy lead	Provenance assessment and bounded data scope
Extortion listing	Is there corroborating access, encryption or exfiltration evidence?	Incident commander	Telemetry review and documented incident disposition
Disruption claim	Did the service experience impact matching the claim?	Service and network owners	Availability and request evidence with timestamps
Historical recirculation	Was the material already remediated or disclosed?	Incident records and privacy owners	Link to earlier case and validation of remaining risk

4.3 Nine retained-corpus dossiers

A

CASE A

Banking-related access was advertised as current

Evidence card B01 | 17 Oct 2026 | Retained advertisement | A banking group

Claim unverified

CLAIM

A 17 October post offered alleged mobile-banking backend access, a promotional API database and customer or administrator information. The seller described the access as current. [S1]

CHRONOLOGY

The retained advertisement is dated 17 October 2026. Its assertion about live access is a claim about conditions at that time, not a verified observation of production access.

ESTABLISHED

The advertisement offers access and proposes buyer verification. It describes banking and promotional systems as distinct elements. Publication and the commercial proposition are supported.

ALTERNATIVES

The description could conflate service descriptions, promotional infrastructure and customer exposure. Recycled material, exaggeration or fabrication remain possible.

LIMITS

Current access, customer-data authenticity, permissions, bank-wide scope and a completed transaction remain unresolved. The post does not establish a confirmed banking incident.

RESPONSE

The service and identity owners should validate the alleged authentication boundary and review relevant access. Sensitive responses and account-recovery flows merit review where the service relationship is established.

Bottom line

Publication is observed; access, authenticity and outcome require proposition-specific validation.

Evidence card B01 17 Oct 2026

updap | Retained advertisement | Forum | English

ORIGINAL

This is not historical data. This is live production access right now.

Note. The statement below is the seller's claim, not a verified access observation.

Held

A retained advertisement offers access and buyer verification involving banking and promotional systems.

Not established

Current access, customer-data authenticity, permissions, bank-wide scope and completed sale remain unresolved.

CASE B

B A revenue-service offer mixed access and record populations

Claim unverified

Evidence card B02 | 31 Oct 2026 | Retained advertisement | A public-sector revenue service

CLAIM

A 31 October advertisement concerned a public-sector revenue service. It claimed privileged access and offered roughly 10.5 million submission records, 3.4 million taxpayer identifiers and about 23,000 refund cases for $3,500. [S1]

CHRONOLOGY

The post date establishes October circulation. It does not establish when the alleged material originated or when access was obtained.

ESTABLISHED

The advertisement contains those quantities, commercial terms and terminal-text claims. The quantities refer to different advertised populations.

ALTERNATIVES

The offer could combine older records with an access assertion. A plausible technical narrative or terminal display does not authenticate the alleged service or outcome.

LIMITS	Authenticity, unique records, file identity, access freshness and claimed privilege remain unresolved. The three advertised counts must not be added or described as unique people.
RESPONSE	The application owner should review privileged changes, integrations and bulk exports. The identity owner should validate any relevant current account. The incident commander should preserve separate conclusions about data and access.

Bottom line

Publication is observed; access, authenticity and outcome require proposition-specific validation.

Evidence card B02 — 31 Oct 2026

marlanwg | Retained advertisement | Forum | English

ORIGINAL

[count redacted] distinct [redacted document type] submission records

Note. Advertised populations differ and must not be added; a document-type reference is redacted.

Held

The advertisement contains quantified submission, identifier and refund-case claims with commercial terms.

Not established

Authenticity, record uniqueness, file identity, access freshness and claimed privilege remain unresolved.

C

CASE C

Agricultural remote access carried a privilege claim

Evidence card B03 | 29 Oct 2026 | Retained advertisement | An agricultural organisation

Claim unverified

CLAIM	A 29 October listing advertised OpenVPN access involving an agricultural organisation. It claimed server-administrator privilege, roughly 10,000 hosts and an asking price of $1,000. [S1]
CHRONOLOGY	The date records the listing. It does not establish the beginning or duration of access.
ESTABLISHED	The post supplies an access type, privilege description, network-size estimate and commercial term. These are the seller's representations.
ALTERNATIVES	The offer could be brokered, inaccurate or expired. Another agricultural listing need not concern the same organisation or access.

LIMITS	Target identity, session validity, privilege, host inventory and transaction remain unresolved. The advertised host count is not a measured affected-device count.
RESPONSE	Remote-access and identity owners should review relevant sign-ins, account state and privileged permissions. Confirmed unauthorized sessions require scoped containment and investigation.

Bottom line

Publication is observed; access, authenticity and outcome require proposition-specific validation.

Evidence card B03 29 Oct 2026

CocoMel0n | Retained advertisement | Forum | English

ORIGINAL

Privilege ..... Server Admin

Note. The advertised host count is not a measured affected-device population.

Held

The listing states an access type, claimed privilege, network-size estimate and asking price.

Not established

Target identity, active session, privilege, host inventory and transaction remain unresolved.

D

CASE D

Cutoff-day university access needs a current-state check

Evidence card B04 | 22 Nov 2026 | Retained advertisement | A university

Claim unverified

CLAIM	A 22 November post advertised GlobalProtect VPN access to a university. It claimed domain-administrator privilege and roughly 10,000 hosts. The stated price was 984,312 satoshis. [S1]
CHRONOLOGY	The post was observed on the cutoff day before day-end. It does not represent every later publication on 22 November.
ESTABLISHED	The retained post advertises remote access and a claimed privileged role. The price remains in its original unit.
ALTERNATIVES	The seller could be circulating an expired or unverified offer. The record does not link this university proposition to the October agricultural listing.
LIMITS	Institution identity, active sessions, domain-administrator capability, host count and sale remain unresolved. No fiat value is inferred.

RESPONSE	The identity owner should review relevant VPN sign-ins, dormant accounts and privileged-group changes. Session revocation should follow current internal evidence and a scoped response decision.

Bottom line

Publication is observed; access, authenticity and outcome require proposition-specific validation.

Evidence card B04 — 22 Nov 2026

AFKForever | Retained advertisement | Forum | English

ORIGINAL

Privilege ..... Domain Admin

Note. The price remains 984,312 satoshis; no fiat conversion is inferred. Observation preceded cutoff-day end.

Held

The cutoff-day post advertises university remote access and claimed privileged permissions.

Not established

Institution identity, active VPN access, domain-administrator capability, host count and sale remain unresolved.

CASE E

E

An identity-data offer withheld its alleged platform

Evidence card B05 | 21 Nov 2026 | Retained advertisement | An unnamed identity-verification platform

Claim unverified

CLAIM	A 21 November post advertised more than one million identity-verification entries. It described identity attributes, contact or banking fields and selfie images. The alleged platform was unnamed. [S1]
CHRONOLOGY	The publication falls in the recent period. Its claim of continuing daily intake does not establish an observed ongoing collection process.
ESTABLISHED	The post lists categories of information and advertises volume. It supports an identity-material offer.
ALTERNATIVES	Older material, aggregation or a misleading schema description could explain the proposition. The field list does not identify the controller.
LIMITS	Source, authenticity, volume, uniqueness, continuing intake and current access remain unresolved. The quantity is not a confirmed affected-person count.
RESPONSE	

Fraud owners should test identity-replay and repeated-use checks. Privacy and incident owners should preserve any credible relationship to owned data before attributing the offer to a platform.

Bottom line

Publication is observed; access, authenticity and outcome require proposition-specific validation.

Evidence card B05 21 Nov 2026

SUB-ZERO | Retained advertisement | Forum | English

ORIGINAL

Personal Data (PII) and Selfie Image

Note. The alleged platform is unnamed; field descriptions do not identify its controller.

Held

The post advertises identity-verification entries, field categories and selfie images.

Not established

Source, authenticity, volume, uniqueness, continuing intake and current access remain unresolved.

F

CASE F

A document buyer sought a real business relationship

Evidence card B06 | 4 Mar 2026 | Retained advertisement | Identity and business-registration documents

Claim unverified

CLAIM	A 4 March request sought real Indonesian identity and business-registration documents for an active company. It offered $100 per set and an intermediary term. [S1]
CHRONOLOGY	The date records a purchase request. It does not establish a later supply or use.
ESTABLISHED	The buyer expressly requested unexpired documents and rejected edited or fake material. This is demand-side evidence.
ALTERNATIVES	The intended purpose is unstated. The request alone cannot determine the legality or outcome of a later activity.
LIMITS	Supply, document transfer, successful verification, corporate authority and transaction remain unresolved. Authentic documents would not by themselves establish permission to represent the subject.
RESPONSE	Onboarding owners should verify the applicant's authority through an established independent relationship. Document checks should be connected to the current business and person, with a recorded decision.

Bottom line

Publication is observed; access, authenticity and outcome require proposition-specific validation.

Evidence card B06 4 Mar 2026

DrBisoun0urs | Retained advertisement | Forum | English

ORIGINAL

WTB real KTP + NIB from Indonesia.

Note. The original Indonesian document terms are retained; request outcome is unresolved.

Held

The buyer asks for real, unexpired identity and business documents and rejects edited material.

Not established

Supply, document transfer, successful verification, corporate authority and transaction remain unresolved.

CASE G

G ■ Messaging-account advertisements recurred over time

Evidence card B07 | 5 Jan 2026 | Retained advertisement | Indonesian-number messaging accounts

Claim unverified

CLAIM	A recurring series offered Indonesian-number messaging accounts and reusable account-material formats. One alias advertised $0.45 in January and $0.40 by late February or March. [S1]
CHRONOLOGY	The dossier spans January to 21 November, with additional menus on 8 and 19 November. Repetition establishes circulation at those dates, not continuing unauthorized access.
ESTABLISHED	Recurring menus and later advertisements explicitly describe fresh or aged accounts and reusable account material. These establish supply claims, not stolen provenance.
ALTERNATIVES	The accounts could be newly registered rather than stolen. Different aliases and price menus do not establish a common operator, the same file or a market-wide price trend.
LIMITS	Account provenance, file identity, completed purchases and common operation remain unresolved. Repeated advertisements are not additional breaches or unique victims.
RESPONSE	Account-security and fraud owners should review relevant enrolment, automation and session behavior. Current unauthorized use should be addressed through a scoped identity response.

Bottom line

Publication is observed; access, authenticity and outcome require proposition-specific validation.

Evidence card B07 5 Jan 2026

sellingood | Retained advertisement | Forum | English

ORIGINAL

Telegram Accounts for Sale - Desktop Tdata \ Session+Json Files

Note. The first advertisement in the series is dated 5 January; later dates appear in the dossier.

Held

Repeated posts support an advertisement series; separate July advertisements also describe transferable account material.

Not established

Account provenance, file identity, completed purchases and common operation remain unresolved.

CASE H

H

Insurance-workflow records were advertised repeatedly

Evidence card B08 | 12 Jan 2026 | Retained advertisement | An insurance-workflow platform | Claim unverified

CLAIM	Posts described roughly 199,000 insurance-workflow records, including applications, API history, policy-related material and identity fields. The record categories were mixed. [S1]
CHRONOLOGY	Related titles appeared on 12 January, 18 February and 1 October. The October publication does not establish a new October intrusion.
ESTABLISHED	The titles repeat a proposition. The October narrative describes several tables and information categories.
ALTERNATIVES	Older holdings, copied claims or recirculated material could explain the repeated descriptions. Similar titles and fields do not prove identical files.
LIMITS	Dataset identity, provenance, unique people, current access and a 2026 breach remain unresolved. A row count is not an insured-person count.
RESPONSE	Data and application owners should review export permissions, document authorization and sensitive API logs. A credible match should enter the privacy assessment with a bounded period and field scope.

Bottom line

Publication is observed; access, authenticity and outcome require proposition-specific validation.

Evidence card B08 — 12 Jan 2026

Darmanboy24 | Retained advertisement | Forum | English

ORIGINAL

This dump includes policy applications, API history, loan data, ID cards (KTP)

Note. Related titles appeared 12 January, 18 February and 1 October; publication does not establish a new intrusion.

Held

January, February and October titles repeat an insurance-workflow data proposition.

Not established

Dataset identity, provenance, unique people, current access and a 2026 breach remain unresolved.

CASE I

Technology-service events were presented as a large data claim

Claim unverified

Evidence card B09 | 12 Nov 2026 | Retained advertisement | A technology-services company

CLAIM	A 12 November post concerning a technology-services company advertised approximately 6.58 million internal events. It described account, user, event-delivery and credential-related field categories. [S1]
CHRONOLOGY	The post claimed an earlier October event. November circulation does not independently establish either the asserted activity date or a new November intrusion.
ESTABLISHED	The publication contains an event-volume claim and a mixed field description. It says no ransom was involved.
ALTERNATIVES	A copied or misattributed event stream could explain the material. A schema and narrative do not authenticate the provider or file.
LIMITS	Attribution, file identity, secret validity, current access and unique user count remain unresolved. The 6.58 million events must not become 6.58 million users.
RESPONSE	Application and identity owners should review relevant exports and credential relationships. Validated exposure should trigger scoped credential rotation and downstream-access review.

Bottom line

Publication is observed; access, authenticity and outcome require proposition-specific validation.

Evidence card B09 12 Nov 2026

updap | Retained advertisement | Forum | English

ORIGINAL

6.58M Events [...]

Note. Events are not users; the alleged October activity date remains a claim.

Held

The post advertises an event stream with mixed field categories and says no ransom was involved.

Not established

Attribution, file identity, secret validity, current access and unique user count remain unresolved.

4.4 Six external dossiers

The following cases draw on read public sources. They illustrate consequences and evidence boundaries. Their selection does not establish relative sector prevalence. Only the controller disclosure in Case J is named. Other dossiers use broad roles.

J

CASE J

Fore Coffee disclosed unauthorized access

Consumer services

Controller disclosure

CLAIM	Fore Coffee confirmed unauthorized access to its customer platform. Its preliminary scope was up to about 5.7 million accounts. This was a controller disclosure rather than a seller-only allegation. [S44]
CHRONOLOGY	The notice was published on 28 October. On 5 November, reporting quoted Komdigi saying the company's report had arrived on 28 October. The subsequent examination belongs to the same case. [S44][S45]
ESTABLISHED	The controller described potentially affected contact and profile information, hashed PINs and purchase history. The scope varied by user. It said the platform was secured within 24 hours of detection. [S44]
ALTERNATIVES	A preliminary account count can change as the investigation develops. The notice's account unit does not establish a count of unique individuals or prove that every field was affected for every account.
LIMITS	The controller said national identity numbers (NIK), ID-card (KTP) photos and payment information were unaffected, with no misuse indicated at disclos-

ure. Those findings remain controller-attributed. The intrusion start and final regulatory responsibility remain unresolved. [S44][S45]

RESPONSE	The application and identity owners should validate affected account states and available access logs. The privacy lead should record field-specific scope and notification decisions. Customer operations should base advice on the current case record.

Bottom line

Unauthorized access was disclosed; account and data scope remain preliminary.

The defensive lesson concerns precision. An organisation should distinguish information confirmed affected, potentially affected and outside its stated scope. The same distinctions should appear in customer advice, regulator reports and subsequent updates.

A password or PIN change can be one protective step. It does not establish that associated sessions, recovery routes or integrations were reviewed. Completion requires evidence from the relevant identity and application owners.

K

CASE K

A regional-bank investigation followed transaction losses

Financial services

Police investigative account

CLAIM	Police reported a regional-bank system intrusion dated 22 February 2026. Their July account reported transfers from accounts belonging to 6,609 customers and approximately Rp144 billion in losses. These are the police investigation's reported figures. [S36]
CHRONOLOGY	The bank's legal representative reported suspected hacking on 23 February. Early reporting described a forensic audit and restricted digital access. The 15 July police announcement was a follow-up to the February event. [S36][S37]
ESTABLISHED	The early account supports the complaint and service restrictions. The later police account describes conversion of funds to cryptocurrency and approximately Rp18.94 billion in frozen assets. Frozen assets are distinct from money returned to customers. [S36][S37]
ALTERNATIVES	The public accounts describe different stages of an investigation. A preliminary estimate, an investigative loss figure and a final adjudicated loss are separate propositions.
LIMITS	The allegations against suspects are not criminal convictions. The reported customer count is not a count of ransomware victims. The sources do not support assigning this event to an extortion label seen elsewhere.

RESPONSE	Financial-crime and security owners should reconcile transaction evidence, authentication records and customer complaints. The incident commander should preserve the February activity date alongside later investigative milestones. Legal should track the status of allegations.

Bottom line

Transaction and asset figures retain their investigative status and units.

This case makes transaction integrity a first-class incident concern. An investigation should not wait for encryption or a public extortion post before reviewing abnormal transfers and account changes.

Recovery reporting should also preserve units. A frozen amount, a suspected loss and a reimbursed amount describe different outcomes. Leadership should require the evidence behind each figure before publishing a recovery claim.

L

CASE L

A funding-system investigation crossed two years

Education finance

Police investigative account

CLAIM	Police described brute-force access to an education-funding system and two alleged thefts. One occurred on 17 December 2025. The other occurred on 20 January 2026. [S35]
CHRONOLOGY	The announcement was published on 3 April 2026. It attributed Rp344,802,770 to the December event and Rp598 million to the January event. Only the latter falls within this report's activity window. [S35]
ESTABLISHED	The source supports an official investigative account of system access and financial loss. It reports a cumulative Rp942,802,770 across both dates. That cumulative amount must not be presented as entirely a 2026 loss. [S35]
ALTERNATIVES	The public account does not establish that each funding-system user had the same control weakness. Nor does one described technique establish a nationwide campaign against the sector.
LIMITS	This is a police investigation, not a court finding. The report does not identify additional affected schools, infer wider data extraction or connect the case to an unrelated access advertisement.
RESPONSE	The finance and identity owners should review account protections, payment approval and transaction reconciliation together. The incident record should keep each transaction date and amount separate. Remediation should address the validated access route.

Bottom line

Only the January 2026 transaction belongs to this activity window.

The case illustrates why a publication-based chronology needs an activity-date column. A 2026 announcement can contain losses from a previous year. The annual report should preserve that boundary.

It also shows that access protection and payment approval are complementary. An organisation should test whether an unauthorized login can proceed directly to a financial change. The exercise should produce an owned exception and a verified correction.

CASE M

M

A website-access market served content abuse

Cross-sector websites

Police investigative account

CLAIM	Police described an investigation involving access to 260 websites. Their sector breakdown included 80 school sites, 20 university sites, 13 government sites and 147 company sites. [S38]
CHRONOLOGY	The account was published on 30 July and later updated on 28 September. The update does not establish a second set of 260 intrusions. Individual intrusion dates were not supplied. [S38]
ESTABLISHED	Police said access was sold through a messaging venue for gambling promotion. BSSN's historical June 2023 response guide concerns government and education websites displaying gambling content. The guidance does not independently confirm each investigated website. [S38][S39]
ALTERNATIVES	The observed business model concerns website access and content placement. It does not establish that every website suffered data extraction or that one initial access route applied throughout.
LIMITS	Websites, institutions and defendants are different units. The reported 260 sites must not become 260 confirmed victims in every other dataset. A displayed advertisement does not by itself establish access to financial or personnel systems.
RESPONSE	Web-service owners should review privileged accounts, deployment changes and content integrity. Incident teams should preserve evidence before restoration. Closure should include the validated access route and a check for persistence.

Bottom line

Website access and content abuse do not establish data theft at every site.

A clean homepage is an incomplete recovery test. A content change can be visible while additional access remains hidden. Restoration should include administrator access, application components and the path used to publish content.

Sector ownership also matters. A central technology team may support many websites while departments control content credentials. The recovery record should identify both technical and content-administration responsibilities.

CASE N

N

A personnel-application report contained a dispute

Public administration

Disputed account

CLAIM	Reporting cited a BSSN document describing 13 sample personnel rows and suspected access associated with an infostealer-derived account. [S40]
CHRONOLOGY	The report described discovery on 22 June, a local notification on 23 June and a BSSN document dated 24 June. The article was published on 27 June. These dates refer to different case milestones. [S40]
ESTABLISHED	The local official acknowledged notification and mitigation. The reporting described name and telephone matches in the sample. The official also denied an actual leak or harmful impact. Both positions remain visible. [S40]
ALTERNATIVES	Matching sample information can support authenticity of some rows without establishing how they were obtained. It does not independently prove a current privileged session, complete application extraction or a distinct new database.
LIMITS	The press account describes a BSSN document and a local official's response. The disagreement remains unresolved. Thirteen sample rows do not establish the total affected population.
RESPONSE	The identity owner should validate the implicated account and session history. The application owner should compare access permissions with the alleged material. Privacy and incident owners should record the unresolved propositions and protective actions.

Bottom line

The exposure indicator and the official denial remain distinct propositions.

A denial of impact and a credible exposure indicator can coexist while evidence is assessed. The appropriate response is to test the account and data propositions. Neither proposition should be settled by the headline alone.

This is also a model for disputed seller claims. An investigation can record a supported sample match while withholding a broader compromise conclusion. That creates a defensible basis for proportionate protective work.

CASE O

Local-service websites displayed unauthorized content

Local public services

Official quoted in reporting

CLAIM	A local e-government official confirmed that two websites had displayed unauthorized advertising content. The report described gambling and other commercial adverts. The service roles are kept broad here. [S41]
CHRONOLOGY	The official described taking the sites down on 9 August. Reporting followed on 10 August. Those dates support a response milestone and a publication milestone, rather than an exact intrusion start. [S41]
ESTABLISHED	The account supports visible content abuse and the decision to remove public access while responding. It also describes distributed content administration. It does not establish that all related services shared the same access. [S41]
ALTERNATIVES	The official offered possible credential exposure as an explanation. The public account does not prove that root cause. An application weakness or another access path cannot be resolved from the available statement.
LIMITS	The report does not infer personal-data theft, transaction manipulation or compromise of the broader local-government network. The two websites do not become a national incident trend.
RESPONSE	The service owner should preserve content and access evidence, then restore from a trusted state. Identity owners should review administrator accounts. Completion should include a tested publication path and an assigned content owner.

Bottom line

Visible content abuse is supported; the initial access route remains unresolved.

4.5 Additional access and extortion propositions

P

CASE P

A health-insurance offer claimed both access and data

Evidence card B10 | 5 May 2026 | Retained advertisement | A health-insurance organisation

Claim unverified

CLAIM	A 5 May advertisement claimed access and a very large, population-scale set of records involving a health-insurance organisation. A 7 May post repeated the claim, followed by a 12 May reply. [S1]
CHRONOLOGY	The dates describe circulation. They do not establish a fresh intrusion on each date or the period represented by the alleged records.
ESTABLISHED	The advertisement links access with identity, membership, clinic, referral and diagnostic fields. The later reply quotes the same proposition.
ALTERNATIVES	Historical material, aggregation, inflated coverage or fabricated descriptions could explain the offer. A historical archive would not establish current access.
LIMITS	Authenticity, access freshness, export, unique population, customer impact and transaction remain unresolved. The advertised quantity is not national coverage or confirmed people.
RESPONSE	The data and service owners should review relevant bulk queries, exports and service-account permissions. Sensitive diagnostic or referral access should have a documented owner and scope.

Bottom line

Publication is observed; access, authenticity and outcome require proposition-specific validation.

Evidence card B10 — 5 May 2026

alwayschina | Retained advertisement | Forum | English

ORIGINAL

[ACCESS + DB] [a health-insurance organisation] – [record count redacted]

Note. The advertised record count is withheld; it is not national coverage or confirmed people.

Held

May advertisements join an access claim with a large data claim; a later reply quotes the proposition.

Not established

Authenticity, current access, unique population, customer impact, export and transaction remain unresolved.

CASE Q

An agricultural-sector post demanded payment for deletion

Claim unverified

Evidence card B11 | 14 May 2026 | Retained advertisement | An agricultural public body

CLAIM	A 14 May post claimed more than 243 GB of information involving an agricultural public body. It demanded $10,000 for deletion before publication. [S1]
CHRONOLOGY	The post described continuing collection. That statement does not establish an observed continuing intrusion.
ESTABLISHED	The message contains a deletion-for-payment demand and describes documents, employee information and organisational data.
ALTERNATIVES	The volume could be exaggerated or the claimed collection could mix public, private and older holdings. A demand does not independently prove control of the alleged material.
LIMITS	Archive identity, size, compromise, deletion capability, payment and publication outcome remain unresolved. The asking amount is not a loss.
RESPONSE	The incident commander should preserve the threat and compare it with internal access and export evidence. Legal, privacy and continuity owners should prepare decisions around the systems and data actually implicated.

Bottom line

Publication is observed; access, authenticity and outcome require proposition-specific validation.

Evidence card B11 — 14 May 2026

Kyyzo | Retained advertisement | Forum | English

ORIGINAL

We are demanding a ransom of $10,000 to delete all the data

Note. The demand is not evidence of payment, deletion or demonstrated archive control.

Held

The post makes a deletion-for-payment demand and describes organisational, document and employee information.

Not established

Archive identity, size, compromise, deletion capability, payment and publication outcome remain unresolved.

R

CASE R

Official-mailbox menus implied authority they did not establish

Claim unverified

Evidence card B12 | 12 Jun 2026 | Retained advertisement | Public-authority mailbox identities

CLAIM	A January menu and June posts offered alleged law-enforcement-related mailbox access for $200. The June text promoted misuse of official-request channels. [S1]
CHRONOLOGY	The retained dates are 31 January and 12 June. They establish advertisements, not a continuing session between those dates.
ESTABLISHED	The menus state a country, public-authority role and price. The later messages discuss requests to online platforms.
ALTERNATIVES	Access could be fabricated, expired, limited or mislabelled. Even possession of a mailbox would not by itself establish lawful authority or platform entitlement.
LIMITS	Mailbox ownership, current access, request privileges, accepted recipient action and transaction remain unresolved. A menu is not proof of successful impersonation.
RESPONSE	Teams receiving exceptional data requests should verify them through an established independent channel. Identity owners should review unusual sign-ins, forwarding and mailbox rules when evidence identifies a relevant account.

Bottom line

Publication is observed; access, authenticity and outcome require proposition-specific validation.

Evidence card B12 12 Jun 2026

Governer Retained advertisement Forum English

ORIGINAL

Selling Government & Law Enforcement Email Accounts

Note. The dossier also includes a 31 January menu. The quoted June advertisement does not establish successful request-channel abuse.

Held
The menus advertise public-authority mailboxes and a price; later posts discuss exceptional data requests.

Not established
Mailbox ownership, current access, request privileges, accepted recipient action and transaction remain unresolved.

4.6 Repeated data does not establish repeated intrusion

Komdigi's 2 October account said BSSN had explained recently circulating information as old data being recirculated. The authorities continued coordination concerning unlawful data sale. That account concerns the material addressed by the notice. [S46]

It should not be generalized to every contemporary offer. A different post can concern different material or a different time period. Conversely, publication in October does not by itself establish an October intrusion.

A case record should therefore retain four separate questions. When did the material originate? When was access alleged? When was the post published? What did the organisation or authority later establish?

4.7 The recent period has its own limits

Ransompedia records nine listings in November through the 22 November cutoff: three from 1 to 7 November and six in the recent period from 8 to 22 November. The observations were captured before the end of 22 November. The figures do not cover later publications that day or every cyber incident in that period. [S2]

The same period includes Check Point's 10 November research publication, government preparedness notices and BSSN's global-service advisory. Those are publication and coordination events with different underlying dates. [S28][S48][S50]

Recent reporting should increase attention to relevant service dependencies. It should not collapse warnings, listings and outages into a single attack count. Chapter 6 retains those distinctions in its timeline and comparison panel.

4.8 Additional themes retain their narrower propositions

Theme	Circulation dates	Supported proposition and limit
University staff accounts	2 August and 17 October	Repeated claims concerned staff accounts and password-related material; current validity and file identity remain unresolved
Public-service payment records	14 January to 11 February	Unverified repost circulation; the poster said proof was unavailable and expressed uncertainty about accuracy. Transaction claims do not establish people or infrastructure access
Regional banking records	21 January and 24 April	A historical title and mixed customer, card and log categories do not establish a new 2026 breach
Public-sector analytics material	7 October	Claimed exports, files, models and rows do not authenticate production origin or current access
Assistance and disability-related information	January to October	Sensitive-data categories merit validation; volume, provenance and political assertions remain unresolved
Retail and supplier information	March to November	March and April posts repeated a claimed 10 March event. Free and full row counts overlap; a fresh April incident and file identity remain unresolved
Local identity-registration material	8–19 November	Recent offers included explicitly older records; publication dates are not breach dates
Cooperative membership material	16 October to 19 November	A later 75,086-entry offer does not establish unique people or continuing access
Education-related identity material	14–22 November	Student, alumni, teacher and staff claims contain overlapping row or sheet totals
Transport-sector financial application	17 October	An alleged ledger-manipulation capability does not establish an exploit, affected tenant or successful payment change
Automated credential notices	From 26 June	Target-like labels do not establish an organisational breach or a working credential

Theme	Circulation dates	Supported proposition and limit
Public-authority personnel data	February to November	Reposts do not establish new intrusions. An April post gives conflicting counts, 417,000 versus 417, and describes prior-year access
Courier order data and administration	18 April	The seller claimed continuing administration access and a daily feed; access persistence, customer identity and transaction remain unresolved
Financial and agricultural remote-access menus	13 May	Same-day VPN menus do not establish current access, Indonesian system ownership or links to other offers
Data, verification-worker and SIM supply demand	February to November	Buyer requests do not establish intended use, consent, supply, accepted verification or a completed transaction
Enterprise and service-provider extortion	2–17 May	Seller allegations about provider relationships, unpaid demands and staged releases do not establish common compromise or release outcomes
Data aggregation and provenance	January to October	Uploader statements describe collected forum material; advertised search holdings do not establish fresh intrusion, provenance or unique people
Clinical and health-worker archives	February to May	Separate health-related propositions remain unverified; their advertised populations are not combined with the health-insurance offer
Food-sector organisation access	13 February	Claimed internal data and continuing access leave system identity, authenticity, current access and transaction unresolved

These retained themes broaden the decision coverage without adding confirmed incidents. Advertised record quantities are not combined. These themes are not counted as confirmed incidents. [S1]

4.9 Further service and relay observations

The organisation-related supplement has a separate coverage boundary and is not merged into the 19,814-post retained base. Alert relays also remain distinct from Ransompedia listing records. These additional propositions are not national incident totals. [S1][S2]

Theme	Publication dates	Supported proposition and limit
Web-property and hosting access menus	January to November	Sellers advertised administration or hosting access; replies disputed screenshots or access status. Ownership, current access and transactions remain unresolved
Legal-document publishing service	7 August	An advertisement claimed an active administrator session and publishing permissions. Entitlement, session validity and document alteration remain unresolved
Financial-account creation menus	January to November	Sellers described supplying identity material while buyers supplied contact details. This does not establish existing-account theft, bank intrusion, accepted verification or transactions
Communications-registration records	11 November	A registration-data offer claimed an internal 8 November date; origin, file identity, volume and current access remain unresolved
Energy-sector extortion relay	31 July	A relay attributed an allegation to The-gentlemen. Claimed engineering or industrial-control documents do not establish operational-system access or disruption
Regional-bank extortion relay	17 November	A relay attributed a claim to Panzer. It does not establish primary claim authenticity, impact or identity with earlier banking events
Support-reporting abuse template	18 October	A circulated template promoted account-reporting abuse; delivery, accepted complaints, account restrictions and underlying allegations remain unresolved

Service owners should connect these propositions to authorised access and document-integrity records. Fraud teams should preserve the distinction between advertised account creation and proven misuse. A relay should not inherit the status of a separately observed listing.

KEY TAKEAWAYS

01

State which proposition each claim supports

02

Keep activity and publication dates separate

03

Close investigations with an owned validation record

CHAPTER 05

Sector decisions

05

THIS CHAPTER ANSWERS

How does the same access or data signal change meaning across sectors?

8

Merged sector cells in the extortion-listing view

5.1 Sector distribution describes listings 54
5.2 Public services need application-level ownership 55
5.3 Education combines web access and financial workflows 55
5.4 Consumer services need field-specific communication 56
5.5 Digital suppliers can create asymmetric dependencies 56
5.6 Industrial and health consequences require restraint 56
5.7 A common validation record supports different owners 57

CHAPTER 05

Sector decisions

IN SHORT

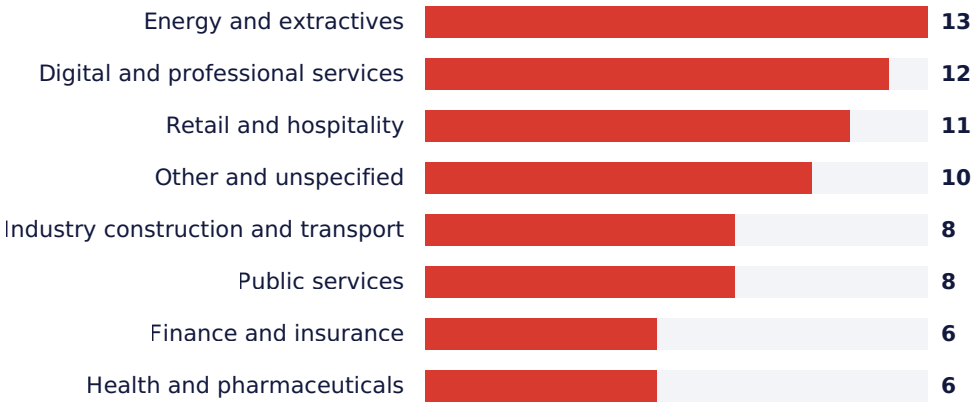
Sector consequences depend on the service and permission involved. Ransompedia's 74 listings span eight merged sector cells, while official cases show financial, application and website consequences. Listing counts do not measure service interruption or loss. Sector teams should use them to test exposure and recovery priorities against their own operations. Assign a service owner to each relevant signal and require evidence of access scope, data consequence and recoverability.

5.1 Sector distribution describes listings

Energy and extractives account for 13 Ransompedia listings. Digital and professional services account for 12, followed by retail and hospitality with 11. These three cells contain 36 of the 74 listings. [S2]

That concentration describes the retained listing population. It does not show which sector experiences the greatest national harm. A listed organisation might have experienced different outcomes, including an allegation that remains uncorroborated.

Extortion listings span eight sector cells



Source: Ransompedia country-tagged extortion listings, 1 January–22 November 2026; closing day partial [S2]. Listing claims are not confirmed incidents, unique victims or successful intrusions.

Sector cell	Listings	Decision supported	Not established
Energy and extractives	13	Review continuity and privileged supplier dependencies	Operational disruption or safety impact
Digital and professional services	12	Examine downstream access and customer notification responsibilities	Compromise of every customer
Retail and hospitality	11	Validate customer-platform and identity protections	National consumer fraud or loss

Sector cell	Listings	Decision supported	Not established
Other and unspecified	10	Resolve service context before prioritizing controls	A coherent common campaign
Industry, construction and transport	8	Identify scheduling, dispatch and production dependencies	A sector-wide operational event
Public services	8	Confirm IIV applicability, service owners and reporting routes	Compromise of central government systems
Finance and insurance	6	Connect access signals to transaction and reporting controls	All financial fraud or affected accounts
Health and pharmaceuticals	6	Test availability and sensitive-data response	Patient harm or quantified health disruption

5.2 Public services need application-level ownership

The personnel-application case contains an exposure indicator, an acknowledged notification and a disputed outcome. The local-service website case confirms visible content abuse. Their control owners and data consequences differ. [S40][S41]

A public-service security programme should therefore identify the owner of each application and publishing route. Central coordination is useful, but a central service inventory can still omit departmental credentials and delegated content administration.

For each application, the service owner should know the data controller, privileged identities, supplier access and recovery route. The incident record should identify which of those elements the evidence actually concerns.

An IIV designation changes reporting responsibilities. It does not mean every website of the same organisation has identical criticality. Legal and service owners should maintain that mapping before an incident.

5.3 Education combines web access and financial workflows

Police reporting describes both school-related website abuse and a funding-system financial investigation. The first concerns the sale of website access. The second describes alleged unauthorized financial activity. [S35][S38]

A sector response should preserve that distinction. A website restoration plan should not substitute for payment approval and reconciliation controls. A financial review should not assume that a public-facing site was the entry route.

Education organisations should identify the accounts that connect administrative applications with payment workflows. They should also test how temporary staff and suppliers receive, retain and lose access.

The completion evidence should match the workflow. A content-integrity review closes a website finding. A transaction reconciliation and access review close a financial-control finding. One cannot stand in for the other.

5.4 Consumer services need field-specific communication

The customer-platform disclosure concerns a provisional account population and varying data fields. The controller's account does not establish that every field applied to every user. Nor does an account count equal unique affected people. [S44]

Customer operations should prepare messages that preserve that scope. Advice should explain what users need to check and how official support will communicate. The response should avoid confirming details that the investigation has not established.

Application owners should review how contact information, recovery mechanisms and transaction histories intersect. A customer-data event can increase impersonation concerns even when the controller excludes payment information from its affected categories.

That is a planning implication rather than proof of subsequent fraud. Fraud teams should watch for relevant patterns and document actual observations. The report does not convert a potential consequence into a measured outcome.

5.5 Digital suppliers can create asymmetric dependencies

A digital-service listing deserves a review of customer-facing permissions and integrations. The important question is which services and credentials the supplier can reach. A supplier name in an extortion post does not answer it.

Customers should maintain an agreed route for urgent supplier enquiries. That route should request access scope, service status and protective actions. It should avoid asking the supplier to validate an unsupported actor attribution.

A shared service can also create availability impact without a supplier intrusion. The November blocking event shows why development and software dependencies belong in continuity planning. [S47]

The service owner should test a fallback for a critical external dependency. A documented supplier contract helps, but an observed fallback exercise provides different evidence.

5.6 Industrial and health consequences require restraint

The listing population includes industrial, transport, energy and health-related cells. It does not establish an interruption to production, logistics, clinical care or safety. Such consequences require service-level evidence. [S2]

Planning should still consider those dependencies. An organisation can identify which identity services, management platforms and suppliers support operational continuity. It can test recovery without asserting that a listed peer suffered an operational incident.

Health-related organisations should also distinguish clinical data, business administration and public websites. A claim about one should not be described as a compromise of all three.

5.7 A common validation record supports different owners

Sector decision	First validation	Trigger for escalation	Completion evidence
Sensitive-data allegation	Compare the alleged fields and period with owned data	Credible match or current access evidence	Bounded data-scope assessment
Privileged supplier access	Confirm account, permission and service relationship	Active unauthorized session or unexplained change	Access review and supplier disposition
Financial manipulation	Reconcile transactions and authentication events	Unauthorized change or unexplained transfer	Transaction case record and customer actions
Website abuse	Review content, privileged access and deployment history	Unauthorized change or persistence indicator	Trusted restoration and access-path correction
Availability warning	Compare service telemetry with claimed impact	Measured degradation matching the timeline	Service impact and recovery record

These tasks should share a case identifier when they concern the same event. Shared ownership of facts does not require one team to perform every investigation.

The executive decision is to fund the handoff. A signal should reach the function that can validate it. Closure should state what was established, what remained unknown and which service-level action followed.

KEY TAKEAWAYS

01
Use sector counts as listing observations

02
Match validation to the affected workflow

03
Require service-specific evidence before describing operational harm

CHAPTER 06

Disruption and claim assessment

06

THIS CHAPTER ANSWERS

How can defenders act on a warning while keeping attack claims and service outages separate?

6

Recent extortion listings, not a total of recent incidents

6.1 A warning can justify preparation 59
6.2 A chronology with evidence types 59
6.3 Compare propositions, not competing totals 60
6.4 Availability evidence should retain its dimensions 61
6.5 Outages create opportunities for deception 61
6.6 Communicate what the service record supports 62
6.7 Privileged technology access needs lawful purpose 62

CHAPTER 06

Disruption and claim assessment

IN SHORT

The recent period contains extortion listings, preparedness notices, a vendor research publication and a global-service advisory. These are different evidence types. Komdigi did not verify the authenticity or capability behind the threat described in its preparedness notice. BSSN's service-outage advisory relayed a non-malicious explanation. Defenders should still prepare for interruption, preserve measured impact and watch for opportunistic deception. Assign one incident owner to reconcile claims with service telemetry before issuing an impact statement.

6.1 A warning can justify preparation

Komdigi's 10 November notice relayed BSSN's 8 November advisory and subsequent letters concerning public systems. It described potential disruption and recommended monitoring, patching, authentication and recovery readiness. The underlying actor capability and authenticity remained unverified. [S48]

This supports a readiness decision. It does not establish that DDoS, defacement, DNS manipulation or phishing had already succeeded against each warned organisation. A scenario in an advisory remains a scenario until supported by event evidence.

The operational response should preserve that distinction. The incident commander can raise readiness, check contacts and review exposed services. Communications should describe preparation as preparation.

An increased monitoring posture also needs an end condition. The owner should state which service signals would trigger escalation and which observations would support a return to routine readiness.

6.2 A chronology with evidence types

30 Jul 2026	**Police** Reported a 260-website access-sale investigation; individual intrusion dates were not supplied [S38]
2 Oct 2026	**Komdigi** Described recirculation of older data addressed by its notice [S46]
17 Oct 2026	**updap** Advertised alleged banking backend and promotional-system access [S1]
29 Oct 2026	**CocoMel0n** Advertised agricultural remote access with claimed administrator privilege [S1]
31 Oct 2026	**marlanwg** Advertised data and privileged access involving a public-sector revenue service [S1]

8 Nov 2026	**Komdigi** Reported a blocking-related access interruption from 6 November [S47]
10 Nov 2026	**Komdigi** Relayed public-system preparedness notices while the threat's authenticity remained unresolved [S48]
13 Nov 2026	**BSSN** Relayed a global-service outage explanation without an indication of malicious activity [S50]
18 Nov 2026	**Police** Published an ethics dismissal with appeal; related criminal allegations remained unresolved [S66]
21 Nov 2026	**Police** Rejected an unsupported viral claim of a prolonged coordinated global outage [S51]
21 Nov 2026	**SUB-ZER0** Advertised alleged identity-verification material from an unnamed platform [S1]
22 Nov 2026	**AFKForever** Advertised alleged university VPN access on the cutoff day [S1]

The timeline places publication events beside other publication events. Where a source describes an earlier activity date, the entry states that distinction. Its entries are not a count of distinct intrusions.

The post aliases identify personas associated with publications. They do not identify the people operating the accounts. The timeline does not imply coordination among the listed personas.

6.3 Compare propositions, not competing totals

Point	Claim or warning	Official account	Interpretation
Public-system disruption threat	A circulating threat prompted preparedness concern [S48]	Komdigi relayed BSSN coordination while authenticity and capability remained unresolved [S48]	Preparation is supported; successful attacks are not established by this notice
Alleged current access	A persona advertised live banking-related access [S1]	No linked official confirmation is established by the supporting sources	Current access, scope and outcome require separate validation
Recirculated information	Contemporary posts can present data as new [S1]	Komdigi described old information recirculating in the material covered by its October notice [S46]	Neither every offer nor every contemporary dataset is resolved by that account
Development-platform availability	Users experienced an access interruption	Komdigi attributed the 6 November disruption to a shared-IP block and described restoration [S47]	Confirmed availability impact does not establish platform intrusion

Point	Claim or warning	Official account	Interpretation
Global-service interruption	A service outage can attract attack rumours	BSSN relayed an overloaded-process explanation and no indication of malicious activity [S50]	Operational recovery and opportunistic-phishing defence remain relevant
Viral prolonged-outage narrative	A claim alleged months of global banking and internet disruption	Police said credible supporting evidence was absent [S51]	A rumour is not a verified incident or a forecast

A claim-versus-official panel should not force unlike measures into a ratio. A request count, a duration, an account total and an actor's claimed target count answer different questions.

The right comparison is whether the evidence supports a particular proposition. Did a service degrade? Did unauthorized access occur? Was information exposed? Did the claimed operator cause the observed effect?

6.4 Availability evidence should retain its dimensions

A service owner should record when degradation began, which functions were affected and when they recovered. External reachability and authenticated customer workflows can differ. A homepage response does not prove that a transaction path worked.

For a DDoS allegation, network owners should compare request characteristics, infrastructure events and user impact. An actor's screenshot does not establish the duration or geographic reach of disruption.

For a defacement allegation, application owners should preserve the changed content and publishing history. A visible page change does not establish data extraction. It also does not establish that restoration removed the access path.

For a DNS-related warning, owners should check authorized records and change history. A different answer observed through one service can have several explanations. The incident record should preserve what was actually observed.

6.5 Outages create opportunities for deception

An official 13 November Kemenkes CSIRT relay of BSSN's advisory warned of opportunistic phishing while relaying a non-malicious outage explanation. That advice is relevant even when the underlying availability event was not a cyberattack. [S50]

Support teams should maintain an approved channel for outage updates and recovery instructions. Customers and employees need a way to distinguish official assistance from messages requesting credentials or software installation.

Security operations should review reports of deceptive recovery messages. The organisation should not claim that such messages caused compromise without evidence. A captured attempt and a successful account intrusion remain different outcomes.

6.6 Communicate what the service record supports

A first statement can identify a service interruption, protective restrictions and the next update route. It need not supply an actor name, a cause or an affected-person estimate before those propositions are established.

An updated statement should explain which facts changed. If a claimed attack was unrelated to the measured outage, the organisation should preserve that conclusion and its supporting evidence.

The recent period demonstrates the value of that discipline. Preparedness, operational incidents and rumours can occur close together. Proximity in time does not establish common cause.

6.7 Privileged technology access needs lawful purpose

An 18 November police publication reported an ethics dismissal concerning unauthorized use of law-enforcement technology. An appeal was filed. Related criminal allegations concerned interception, illegal access and electronic-data deletion. The ethics finding is not a criminal conviction. [S66]

Privileged-system owners should review lawful entitlements, approval and audit records. The control question is who can access sensitive capabilities and how authorized purpose is checked. The account does not establish a connection to the seller claims in this report.

KEY TAKEAWAYS

01
Prepare on credible warnings without declaring completed attacks

02
Compare claims with measured service impact

03
Keep customer recovery instructions on authenticated channels

CHAPTER 07

Threat actors and relationships

07

THIS CHAPTER ANSWERS

Which actor relationships have concrete evidence, and which remain a publisher's hypothesis?

28

Extortion-group labels in Ransompedia

7.1 The map distinguishes relationships 64
7.2 Amaranth-Dragon is historical activity disclosed in 2026 66
7.3 The WinRAR chronology supports patch verification 67
7.4 SilentDelivery explicitly includes Indonesia in 2026 68
7.5 Silver Fox combines country configuration and observed encounters 69
7.6 BlueMoon reporting adds a separate targeted campaign 70
7.7 StrikeShark leaves attribution and activity date unresolved 71
7.8 Extortion labels describe a visible listing ecosystem 72
7.9 Regional comparisons remain listing comparisons 74
7.10 Personas remain publication identities 75

CHAPTER 07

Threat actors and relationships

IN SHORT

The actor landscape combines seller personas, extortion labels and vendor-tracked campaigns. These categories are not interchangeable. Ransompedia records 28 group labels, while vendor reports name Indonesia in targeted activity with different dates and attribution limits. Shared tools, similar advertising or a common country reference do not establish one operator. Use the relationship map to trace each edge to its evidence, and base defensive work on observed capabilities rather than an unsupported attribution.

7.1 The map distinguishes relationships

An actor map should connect a persona to its post, a listing label to its listing and a vendor cluster to the activity the vendor described. Each edge has an evidence type.

A shared tool can support a tooling relationship. It does not automatically establish common control. A repeated title can support similar advertising. It does not establish identical files or a completed transfer.

The report therefore uses explicit relationship categories. Observations and claims remain distinct from official accounts and vendor interpretations. Unsupported connections are omitted rather than drawn as visually equivalent edges.

Own post Relay Official statement Public reporting Our observation

Amaranth-Dragon

public reporting
Historical 2025 activity disclosed in 2026 [S21] ↑

Check Point Research

public reporting
Indonesia explicitly named in SilentDelivery [S28] ↓

SilentDelivery

Silver Fox

public reporting
Indonesia RustSL encounters [S29] ↑

Kaspersky

public reporting
Publication with unresolved activity date [S43] ↓

StrikeShark

Proofpoint

public reporting
Targeting described from 3 September [S42] ↓

UNK_QuietRacket

Banking-related offer B01

own post
Publication alias [S1] ↑

updap

own post
Publication alias; no dataset-identity claim [S1] ↓

Event-data claim B09

sellingood

own post
Recurring advertisement series [S1] ↓

Account series B07

Ransompedia

own data
Dated listing population [S2] ↓

74 extortion listings

Official accounts

official
Controller and police accounts; case-specific limits [S35][S36] [S38][S44] ↓

Controller and police dossiers J–M

Press accounts of official responses

public reporting
Reported official responses with unresolved limits [S40][S41] ↓

Press-based dossiers N–O

NO EVIDENCED LINK TO OTHER ACTORS

Edge type	Supported example	Boundary
Own post	Persona to a retained advertisement [S1]	The persona's real identity and advertised outcome remain unresolved
Own data	Ransompedia to a dated extortion listing [S2]	A listing is not a verified intrusion
Official statement	Authority to the facts it reported [S35] [S36][S48]	Investigative allegations and readiness notices retain their status
Public reporting	Vendor cluster to a described campaign [S21][S28][S29][S42][S43]	Attribution belongs to the publisher
Analytical model	A proposed relationship with stated alternatives	It is not an independently observed connection

7.2 Amaranth-Dragon is historical activity disclosed in 2026

Check Point's 4 February 2026 original describes Amaranth-Dragon campaigns against government and law-enforcement targets across Southeast Asia. Its Indonesia sections concern 18 August and 5 September 2025. Those operations predate this report's activity window. [S21]

The publication remains relevant to patch and detection priorities. It should not become evidence of a new Indonesian intrusion in February 2026. The distinction belongs in the title, chronology and summary of any case card.

Check Point says 18 August was its first observed use of CVE-2025-8088 by this cluster. A later Indonesia campaign used a Telegram-controlled remote-access tool. The publisher describes uncertainty about initial delivery while suggesting malicious email attachments. [S21]

The attribution also has limits. Check Point reports tooling overlap with APT41 and assesses a possible connection or shared resources. This report attributes that assessment to Check Point. It does not treat the overlap as an Indonesian official finding.

Amaranth-Dragon

Vendor-tracked cluster | Check Point assesses a possible APT41 connection

IN INDONESIA, 2026

4 February

Check Point published historical activity involving Indonesia in August and September 2025. [S21]

CLAIMED TARGETS

Regional government and law-enforcement targets, as described by Check Point. Indonesia activity predates the report window. [S21]

SEEN IN PUBLIC REPORTING

[S21] Original February 2026 report describes 2025 operations and uncertain initial delivery.

OUR ASSESSMENT

Use the report for archive-tool patch validation and historical context. Do not count it as a new 2026 Indonesian incident.

CONFIDENCE

High confidence in publication and historical dates; connection to APT41 remains the publisher's assessment.

7.3 The WinRAR chronology supports patch verification

The CVE record identifies Windows WinRAR through version 7.12 as affected by CVE-2025-8088. The flaw concerns path traversal in crafted archives and can enable arbitrary code execution. The record was published on 8 August 2025. [S22][S24]

The vendor identifies version 7.13 as the fixed release, dated 30 July 2025. Its release notes were later updated on 12 August. This means the fixed release predates the CVE publication and the reported 18 August Amaranth operation. [S25][S26]

A patch-response assessment should therefore ask whether vulnerable Windows archive components remained deployed after a fixed version existed. It should not call that later exploitation a zero-day merely because the campaign adopted it quickly.

The vendor also identifies affected Windows RAR and UnRAR components. Unix, Linux and Android builds are outside the advisory's affected scope. The patch inventory should preserve those platform distinctions. [S25][S26]

Milestone	Date	Meaning
WinRAR 7.13 fixed release	30 July 2025	Vendor release date
CVE publication	8 August 2025	Published vulnerability record
ESET original research	11 August 2025	Public technical analysis [S27]
Vendor release-note update	12 August 2025	Updated advisory wording
First Amaranth exploitation observed by Check Point	18 August 2025	Publisher's campaign observation
Check Point publication	4 February 2026	Disclosure date, not activity date

The defensive task is inventory and validation. The endpoint owner should identify relevant Windows components, confirm the installed version and review suspicious archive-related activity where exposure warrants it.

A successful update does not establish that earlier exploitation never occurred. Conversely, the presence of an old version does not establish exploitation. Those propositions require different evidence.

7.4 SilentDelivery explicitly includes Indonesia in 2026

Check Point's 10 November 2026 investigation describes SilentDelivery activity tracked from early 2026. It names Indonesia among countries targeted through selective watering-hole activity. The websites described as maliciously altered belonged to government, shipping, IT and research sectors. [S28]

The publisher describes fake Chrome certificate warnings and a supposed certificate installer. The delivery chain led to SquadC or a SparrowDoor variant. A related phishing archive uploaded to an analysis service from Indonesia shared backdoor infrastructure with the watering-hole chain. [S28]

That is stronger evidence than a country mentioned only in a lure. It still does not supply a complete Indonesian victim list or establish that every visitor to an affected website was infected.

The publisher uses CopperDragon for a proposed supplier relationship among several clusters that Check Point describes as China-nexus. That remains Check Point's hypothesis. Shared tools or infrastructure do not establish one operator across all three clusters. [S28]

Indonesia is supported specifically by SilentDelivery. The other clusters' telecommunications activity in Latin America must not be transplanted into the Indonesian case. A global report can contain several geographically distinct observations.

SilentDelivery

Vendor-tracked operation | Connected to proposed China-nexus supplier CopperDragon, per Check Point

IN INDONESIA, 2026

Early 2026
Check Point began tracking selective watering-hole activity. [S28]

10 November
The original report explicitly named Indonesia among targeted countries. [S28]

CLAIMED TARGETS

Organisations in Indonesia and other countries using websites in government, shipping, IT and research sectors, as described by the publisher. [S28]

SEEN IN PUBLIC REPORTING

[S28] Watering-hole and linked phishing activity delivered SquadC or SparrowDoor variants.

OUR ASSESSMENT

Check Point proposes CopperDragon as a shared framework supplier across SilentDelivery and two other clusters. That potential-supplier hypothesis supports a tooling relationship, not a single operator for all clusters. [S28]

CONFIDENCE

High confidence in the publisher's stated Indonesia observation; supplier identity and common control remain qualified.

For defenders, the practical question concerns unexpected software installation after a trusted-site visit. Endpoint and browser-support owners should review installer launches, provenance and any associated remote-control activity.

User guidance should explain the approved route for browser and certificate issues. A trusted website's appearance does not authorize a request to install software. The support process should offer an accessible verification channel.

7.5 Silver Fox combines country configuration and observed encounters

Kaspersky's 30 April report describes tax-themed activity extending from December 2025 into early 2026. It explicitly reports RustSL encounters in Indonesia and places Indonesia among the countries with the most observed attacks in its telemetry. [S29]

The customized loaders included Indonesia in their execution-country list. Actual telemetry provides a separate proposition from configuration. A configured country alone would not establish observed encounters there.

The chain used a modified RustSL loader and ValleyRAT. Kaspersky also discovered a ValleyRAT plugin that loaded ABCDoor, a backdoor whose use predates 2026. These are the publisher's findings and naming. [S29]

The report's more than 1,600 malicious emails concern the overall campaign between early January and early February. They are not an Indonesian total. Neither an Indonesian organisation count nor an exact Indonesian first date is supplied.

Kaspersky attributes the operation to Silver Fox. This report does not automatically classify every described action as state espionage. The source's campaign attribution and observed capabilities are sufficient for the defensive assessment.

Silver Fox

Vendor-attributed campaign | Attribution by Kaspersky

IN INDONESIA, 2026

January–February

Kaspersky describes tax-themed activity and Indonesia RustSL encounters. [S29]

CLAIMED TARGETS

Indonesia users appear in the publisher's telemetry. The campaign-wide email total is not an Indonesian total. [S29]

30 April
Original report describes ValleyRAT and ABCDoor. [S29]

SEEN IN PUBLIC REPORTING

[S29] The original identifies country configuration and actual encounters separately.

OUR ASSESSMENT

Prioritise suspicious document delivery and loader activity. The report does not identify a named Indonesian victim or establish state sponsorship.

CONFIDENCE
High confidence in the publication and reported encounters; exact Indonesian victim scope remains unresolved.

The control priority is document and executable handling around official-looking communications. The incident owner should trace the observed chain before deciding whether a user merely received a lure or ran a payload.

7.6 BlueMoon reporting adds a separate targeted campaign

Proofpoint's 9 September report describes UNK_QuietRacket activity targeting government, consulting and finance in Indonesia and Singapore from 3 September. Conference-related lures led into browser and Windows exploitation that the publisher called BlueMoon. [S42]

Proofpoint assesses suspected China alignment. That is the publisher's assessment, not an attribution made by this report or an Indonesian authority. No named Indonesian victim is established by the supporting account.

The source also says no final payload was observed on a second command channel. An exploit chain and a final payload are different propositions. The report preserves that limit rather than completing the chain by assumption.

UNK_QuietRacket

Vendor-tracked activity | Suspected China alignment, per Proofpoint

IN INDONESIA, 2026

3 September
Proofpoint dates targeted activity involving Indonesia and Singapore from this day. [S42]

CLAIMED TARGETS

Government, consulting and finance in Indonesia and Singapore, as stated by Proofpoint. [S42]

9 September
Proofpoint published the BlueMoon analysis. [S42]

SEEN IN PUBLIC REPORTING

[S42] Conference lures and browser/Windows exploitation are described; a final payload on a second channel was not observed.

OUR ASSESSMENT

Review the lure-to-endpoint sequence without completing missing parts of the chain by assumption.

CONFIDENCE
High confidence in the publisher's stated activity; alignment remains the publisher's assessment.

The defensive relevance is a trusted-looking invitation followed by unexpected browser or endpoint behavior. Email, endpoint and identity teams should review the sequence together. A lure's subject should not become evidence of the operator's identity.

7.7 StrikeShark leaves attribution and activity date unresolved

Kaspersky's 24 June report describes activity affecting a diplomatic entity located in Indonesia. It associates vulnerable Exchange services with a chain using SharkLoader and Cobalt Strike, including reconnaissance and credential access. [S43]

The supporting account does not supply an exact intrusion date. The publication therefore belongs in the reporting chronology. It does not establish a fresh 24 June intrusion.

Kaspersky did not confidently attribute the activity to a known APT or criminal group. Data exfiltration was not established in the supporting passage. The report should not replace those limits with a more familiar actor label.

StrikeShark

Vendor-named activity | Unattributed in supporting research

IN INDONESIA, 2026

24 June
Kaspersky published activity involving a diplomatic entity located in Indonesia. [S43]

CLAIMED TARGETS

A diplomatic entity located in Indonesia. The supporting account does not supply an exact intrusion date. [S43]

SEEN IN PUBLIC REPORTING

[S43] Research describes vulnerable Exchange services, SharkLoader, Cobalt Strike, reconnaissance and credential access.

OUR ASSESSMENT

Investigate relevant exposed collaboration services and post-access behavior. Do not infer exfiltration or a known operator.

CONFIDENCE

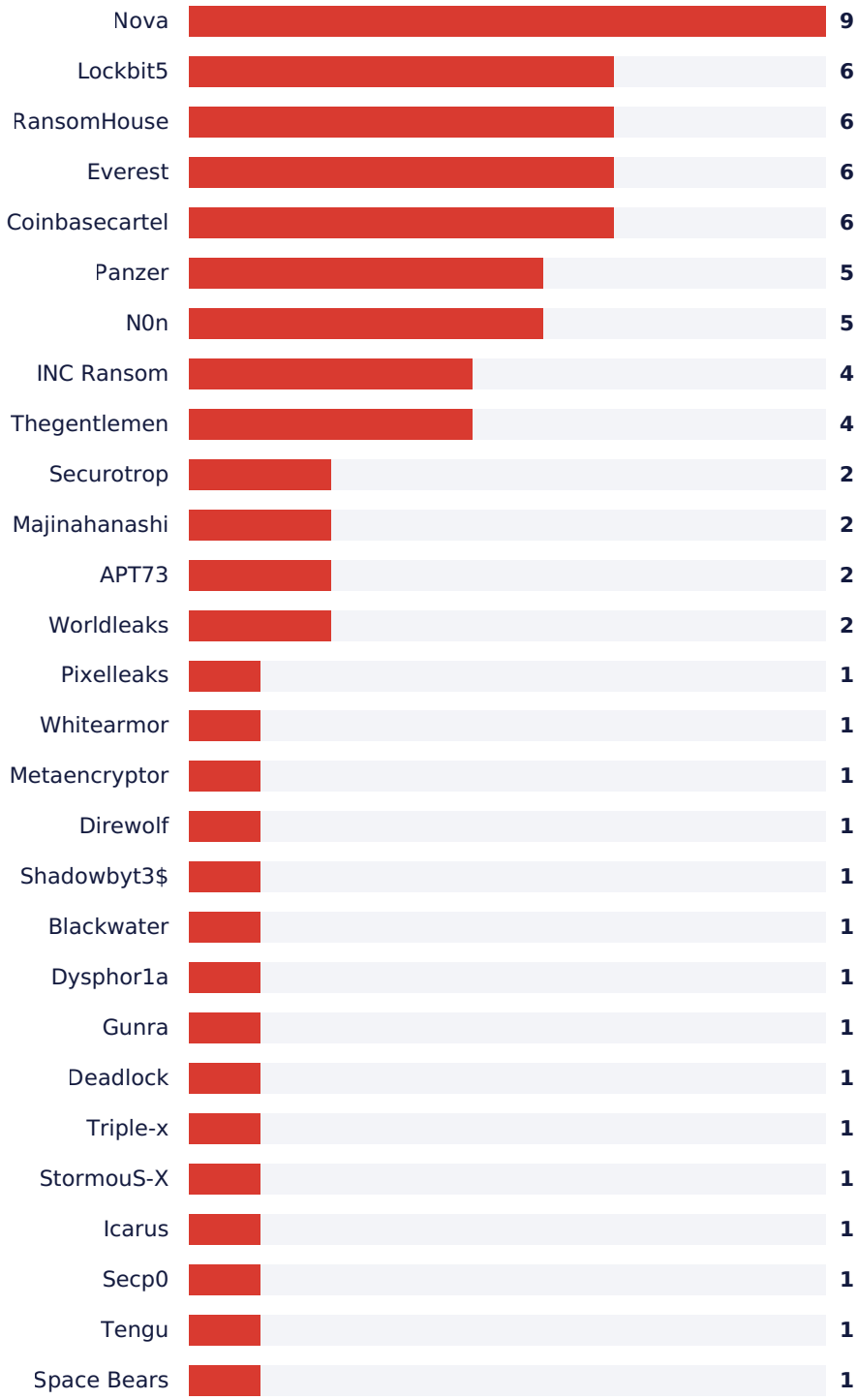
High confidence in the publication; activity date, known-group attribution and exfiltration remain unresolved.

The operational implication concerns exposed collaboration services and post-access activity. Infrastructure owners should confirm service hardening and patch status. Security operations should investigate relevant reconnaissance and credential-access evidence where an exposure or event warrants it.

7.8 Extortion labels describe a visible listing ecosystem

Ransompedia associates 28 labels with the 74 Indonesian listings. Nova accounts for nine. Lockbit5, RansomHouse, Everest and Coinbasecartel each account for six. Panzer and N0n each account for five. [S2]

Extortion listings are distributed across 28 group labels

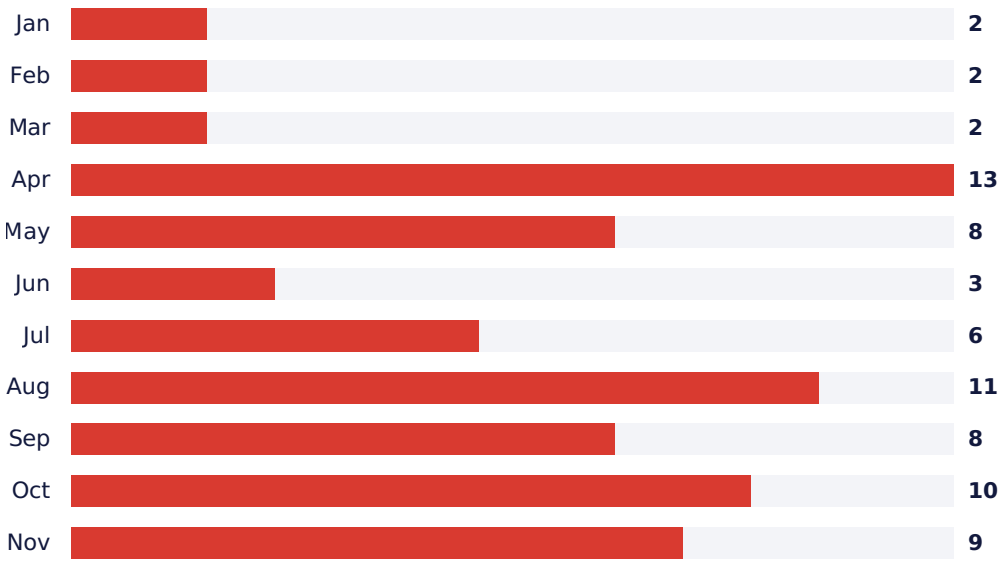


Source: Ransompedia country-tagged extortion listings, 1 January–22 November 2026; closing day partial [S2]. Listing claims are not confirmed incidents, unique victims or successful intrusions.

Those labels are not a verified count of independent operators. Brands can change, affiliations can overlap and listings can make unverified claims. The report does not infer those relationships without supporting evidence.

November has nine listings in total: three dated from 1 to 7 November and six in the recent period from 8 to 22 November. The recent six listings involve Panzer, N0n, INC Ransom and Pixelleaks. A label's recent publication can justify monitoring and continuity review. It cannot identify the initial access technique or prove that encryption occurred. [S2]

Extortion-listing dates vary across the observation window



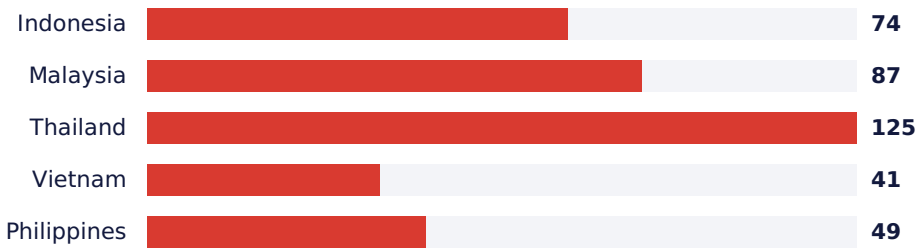
Source: Ransompedia country-tagged extortion listings, 1 January–22 November 2026; closing day partial [S2]. Listing claims are not confirmed incidents, unique victims or successful intrusions.

7.9 Regional comparisons remain listing comparisons

Country tag	Window listings	Permitted reading
Thailand	125	Largest listing count among these five country tags
Malaysia	87	More observed listings than Indonesia within the same stated window
Indonesia	74	A bounded Ransompedia listing population
Philippines	49	A smaller observed listing count
Vietnam	41	A smaller observed listing count

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

Regional country tags show different listing volumes



Source: Ransompedia country-tagged extortion listings, 1 January–22 November 2026; closing day partial [S2]. Listing claims are not confirmed incidents, unique victims or successful intrusions.

The comparison does not rank national security or incident rates. Economies, reporting visibility and organisation populations differ. A listing count should not be normalized into a risk probability without an appropriate denominator. [S2]

The action is peer-informed planning. Organisations can examine whether their recovery, supplier and notification arrangements address the consequences illustrated across the region. They should not infer that a lower listing count establishes lower exposure.

7.10 Personas remain publication identities

The corpus includes access sellers, document buyers and account advertisers. Their roles are inferred from the activity described in the retained posts. They are not legal identities or proven members of an organised group. [S1]

A recurring alias supports a publication association. Matching language or a similar asking price does not support an operator merger. The map should preserve separate nodes until concrete evidence supports a connection.

updap

Publication persona | Real identity unresolved

IN INDONESIA, 2026

17 October

Banking-related access advertisement, Case A. [B01]

12 November

Technology-service event-data claim, Case I. [B09]

CLAIMED TARGETS

Two different service-role claims are associated with the publication alias. [S1]

IN THEIR WORDS

"This is not historical data. This is live production access right now." B01

SEEN IN PUBLIC REPORTING

The cited evidence establishes retained publications, not an external attribution.

OUR ASSESSMENT

The cited evidence establishes retained publications, not an external attribution. [S1] The same publication identity does not authenticate both claims or prove the datasets share an origin.

CONFIDENCE
High confidence in alias-to-post association; claim authenticity and real identity unresolved.

sellingood

Advertisement-series persona | Real identity unresolved

IN INDONESIA, 2026

January–March
Recurring country-price menu for messaging accounts. [B07]

CLAIMED TARGETS

Indonesian-number accounts are advertised within a broader menu. [S1]

IN THEIR WORDS

"Telegram Accounts for Sale - Desktop Tdata \ Session+Json Files" B07

SEEN IN PUBLIC REPORTING

The cited evidence establishes retained publications, not an external attribution.

OUR ASSESSMENT

The cited evidence establishes retained publications, not an external attribution. [S1] Do not interpret menu repetition as additional breaches or infer that all accounts were stolen.

CONFIDENCE
High confidence in repeated advertising; account provenance and transactions unresolved.

TECHNIQUES NAMED IN THE VENDOR RESEARCH, BY TACTIC

Initial access
T1189 Drive-by Compromise
T1566.001 Spearphishing Attachment

Analytical mapping of vendor-described watering-hole and malicious-attachment behaviors [S28][S29], using MITRE definitions [S85][S86]. This does not establish either behavior at every Indonesian target. [S85]

The limited ATT&CK view maps watering-hole behavior to T1189 and malicious attachments to T1566.001 using MITRE definitions. [S85][S86]

This is an analytical mapping of vendor-described behavior. It does not establish that either technique occurred at every Indonesian target. [S28][S29]

KEY TAKEAWAYS

01
Attribute actor assessments to their publishers

02
Distinguish shared tooling from common control

03
Use capabilities and current evidence to select defensive work

CHAPTER 08

Fraud economy

08

THIS CHAPTER ANSWERS

How should defenders respond when advertisements concern accounts, identity documents or payment records?

3

Different propositions: availability, transfer and successful use

8.1 A marketplace offers different products 79
8.2 Demand-side evidence has a different meaning 79
8.3 Transferable sessions require account-security review 80
8.4 Identity-verification claims do not authenticate a platform 80
8.5 Asking prices retain their advertised unit 81
8.6 Payment-card records require a narrow scope 81
8.7 Enforcement reporting needs its own period boundary 81
8.8 Fraud operations should preserve a decision trail 82

CHAPTER 08

Fraud economy

IN SHORT

The retained corpus includes demand for identity documents, messaging-account advertisements and alleged identity-verification material. These observations describe commercial propositions. They do not establish document transfers, completed sales or successful verification. Payment-card figures have a narrower population and cannot measure national theft or loss. Fraud teams should connect each relevant offer to internal account, enrolment and transaction evidence, then document whether the advertised capability creates a current customer or business risk.

8.1 A marketplace offers different products

An identity-document request, a transferable account and a data offer create different verification tasks. The buyer may seek evidence of a real organisation. The account seller may offer newly registered accounts or reusable sessions. A data seller may advertise older material. [S1]

Those alternatives matter because price alone cannot identify provenance. A low asking price does not prove mass compromise. A high asking price does not prove privileged access or an authenticated customer population.

The corpus cases preserve the advertised unit. Records remain records, events remain events and accounts remain accounts. Their quantities do not become unique people without supporting evidence.

8.2 Demand-side evidence has a different meaning

The March document-purchase request sought Indonesian identity and business-registration documents for an active company. It specified real, unexpired material and rejected edited or fake documents. That establishes the buyer's stated demand. [S1]

It does not establish a supplier response, transfer, successful verification or corporate control. The purpose of any later use remains unresolved. The report does not infer a completed fraud from the request.

For onboarding teams, the planning implication concerns authority as well as document appearance. A document can refer to a real person or business without establishing that the applicant may represent them.

The completion test should therefore combine identity evidence with a current relationship check. The business owner should record who authorized the applicant, which independent contact confirmed that relationship and whether the request matched expected activity.

8.3 Transferable sessions require account-security review

The messaging-account series offered Indonesian-number accounts and reusable account-material formats. The same alias advertised $0.45 in January and $0.40 by late February or March. Separate July and November sellers also advertised account material. November menus described fresh and aged accounts or reusable session formats. [S1]

These are asking prices from particular posts. They do not establish a general market price or a decline in the cost of stolen accounts. The accounts could have been newly registered rather than taken from existing users.

The repeated series supports circulation over time. It does not establish additional breaches each time the same menu reappears. Nor does it link every seller that uses a similar description.

Security and fraud teams should review relevant account enrolments, automation and session behavior. The organisation should distinguish an attempted login from an authorized session and from unauthorized use.

A password change does not, by itself, describe session state. Where internal evidence establishes unauthorized access, the identity owner should determine whether session revocation, recovery changes or integration-token review are also required.

8.4 Identity-verification claims do not authenticate a platform

The recent identity-verification offer described more than one million entries, identity attributes and selfie images. It withheld the alleged platform and claimed continuing intake. Those are the seller's statements, not verified operating conditions. [S1]

A schema list can describe plausible fields without establishing authenticity. It does not identify a controller, prove the source or show that every advertised record is unique.

The appropriate defensive concern is replay and impersonation. Fraud owners should look for repeated identity use, unusual account relationships and mismatches between documents and present applicant behavior. These are recommended checks, not observed fraud outcomes.

Privacy and customer teams should avoid naming a platform from a broad field description. A wrong attribution can misdirect protective work and expose an uninvolved organisation.

8.5 Asking prices retain their advertised unit

Advertised item	Observed asking term	What remains unresolved
Agricultural remote access	$1,000	Current access, stated privilege and completed sale
Revenue-service data and access	$3,500	Authenticity, file identity, current privilege and transaction
Identity and business documents	$100 per set, with an intermediary term	Supply, transfer, purpose and successful use
Indonesian-number messaging accounts	$0.45 in January; $0.40 in later posts	Provenance, account quality and completed purchases
University remote access	984,312 satoshis	Access validity, privilege, host count and sale

The table preserves each post's currency and unit. It does not convert the satoshi amount into fiat currency or compare unlike products as a price index. [S1]

8.6 Payment-card records require a narrow scope

SCOPE OF THE CARD FIGURES

Payment-card figures cover payment-card records in the retained post corpus. They do not measure national exposure, card theft or fraud loss.

Three Indonesia-associated payment-card records appear in three retained posts. These are record and post counts. Financial teams should validate a relevant account or customer relationship through lawful internal evidence before deciding protective action. [S1]

8.7 Enforcement reporting needs its own period boundary

An April police account describes an internationally coordinated phishing-tools investigation, including 22 tools and two arrests. The public account also discusses multinational victims and losses from January 2023 to April 2024. [S57]

The 2026 enforcement announcement does not relocate those earlier victims into this year's Indonesian incident population. Arrests are also distinct from convictions. The report uses the account to illustrate the tooling market and enforcement response.

The defensive lesson is to separate acquisition, attempted use and successful harm. A tool being offered does not prove it was used against a particular organisation. A customer receiving a lure does not prove credential loss.

8.8 Fraud operations should preserve a decision trail

Fraud and security teams should share evidence without merging their outcomes. A security investigation can establish unauthorized access while a transaction review establishes whether money moved. Privacy analysis can establish a different data consequence.

The incident owner should record each conclusion and its basis. That record should distinguish attempted, blocked, unauthorized and confirmed-loss outcomes. It should also preserve the relevant time period.

This structure supports customer protection without overstating the marketplace evidence. It makes the next action clear and allows later facts to change the assessment.

KEY TAKEAWAYS

01
Preserve advertised units and asking-price status

02
Validate applicant authority beyond document appearance

03
Connect payment-record signals to current internal evidence

CHAPTER 09

Banking and financial services

09

THIS CHAPTER ANSWERS

How should financial institutions combine access claims, transaction evidence and service continuity?

2

Separate outcomes: unauthorized access and financial loss

9.1 Four questions should remain separate 84
9.2 The banking advertisement has a bounded claim 84
9.3 Transaction evidence should drive financial-loss statements 85
9.4 Customer information can create a parallel duty 85
9.5 Service restrictions require continuity planning 85
9.6 Selected financial-sector exposure 86
9.7 Sector guidance complements incident response 86
9.8 Reporting readiness should begin with applicability 87
9.9 A financial incident needs joint closure 87

CHAPTER 09

Banking and financial services

IN SHORT

Financial services face distinct questions about identity, transaction integrity, customer data and availability. The regional-bank police account describes losses and an investigation. The retained banking-related advertisement establishes a seller's claim about several systems. Neither should supply missing facts for the other. Institutions should validate current access, reconcile financial activity and preserve scoped reporting clocks. Put the incident commander, financial-crime lead, service owner and privacy lead on one factual record.

9.1 Four questions should remain separate

A financial institution should ask whether unauthorized access occurred, whether information was exposed, whether transactions changed and whether service availability degraded. Evidence for one does not establish all four.

An advertised backend is a lead concerning access. A transaction anomaly is a lead concerning financial activity. A customer complaint can concern either, while an outage can arise from protective restrictions or another cause.

The regional-bank case demonstrates why those threads must meet. Police describe a February system intrusion and account losses. Early reporting describes restricted digital access and a forensic audit. Each is a distinct case milestone. [S36][S37]

The incident commander should coordinate the threads. Financial-crime teams validate transactions. Identity owners validate accounts and sessions. Application owners determine service permissions. Privacy teams assess the information involved.

9.2 The banking advertisement has a bounded claim

The 17 October post advertised alleged mobile-banking backend access alongside a promotional API database. It claimed customer and administrator information and described the access as current. Those statements remain the seller's allegations. [S1]

The presence of banking terminology does not establish that all described systems share a trust boundary. Promotional infrastructure and core customer services can have different permissions and operators. The investigation should determine the actual relationship.

This distinction prevents an access claim from becoming a bank-wide compromise conclusion. It also avoids dismissing a promotional-system issue merely because a core system remains unaffected.

The first validation should identify an owned service and relevant authentication events. The owner should then assess permissions and any sensitive information returned. A current unauthorized session justifies a different response from an unverified service description.

9.3 Transaction evidence should drive financial-loss statements

Police reported transfers from accounts belonging to 6,609 customers and approximately Rp144 billion in losses in the regional-bank investigation. These figures describe the investigation's reported scale. The customer figure does not establish the number of affected accounts. [S36]

The same account describes assets frozen during the investigation. A frozen amount is not automatically a recovered or reimbursed amount. Leadership should require separate financial records for each outcome.

Customer operations should also distinguish a reported complaint from a validated unauthorized transaction. A complaint deserves prompt handling, but the institution should preserve the status of the underlying claim.

The finance owner should maintain a reconciliation linking the transaction, account, timestamp and case disposition. The public statement should describe only the unit and status that reconciliation supports.

9.4 Customer information can create a parallel duty

An access event can involve profile information without confirmed payment manipulation. A transaction event can also require investigation while the data scope remains unknown. The incident record should support both analyses.

The consumer-platform disclosure illustrates field-specific scoping. The controller's preliminary account population differed from the information affected for each user. Its reported exclusions should remain attributed, rather than converted into an independent forensic finding. [S44]

Financial institutions should prepare similarly bounded customer messages. The message should identify the service, known effect and official support route. It should avoid attributing unrelated offers or claiming that an absence of observed misuse guarantees no future misuse.

Privacy teams should document what was known at each notification decision. Later changes should be treated as updates to the same case where the underlying event is the same.

9.5 Service restrictions require continuity planning

Protective restrictions can reduce access while investigations continue. In the regional-bank's early account, digital access was restricted while branches remained available. That is a service-status observation, not proof that every alternative channel met every customer's need. [S37]

Continuity planning should therefore test critical customer journeys. A fallback may work for one payment or support task while failing another. The service owner should record the tested workflow and its limitations.

Communications should explain how customers can obtain authenticated assistance. Fraud teams should monitor for impersonation of the institution during the disruption. Security teams should preserve attempted abuse separately from successful transactions.

9.6 Selected financial-sector exposure

All 25 banking and finance domains had device and credential-record associations. Employee-device associations were observed for 24, and 10 had a credential listed for sale when checked. This sector's counts do not establish current bank-infrastructure access. [S4]

The banking and finance portfolio contains at least 110,475 device associations, including 2,471 employee-device associations, and 355,135 credential-record associations. It also contains 395 document associations and 5,072 lookalike observations in the preceding 30 days. These populations overlap. [S4]

Banking and finance has observations for 22 of 25 candidate domains. DMARC quarantine/reject policy was observed for 19. TLS status was valid for 18, invalid for 1 and unavailable for 3; HTTP observations covered 10. [S3]

Insurance and financial services has observations for 24 of 25 candidate domains. DMARC quarantine/reject policy was observed for 20. TLS status was valid for 20, invalid for 1 and unavailable for 3; HTTP observations covered 12. [S3]

These policy observations do not establish complete delivery enforcement. Header counts use each sector's HTTP coverage, rather than its TLS or selected-domain denominator.

The selected financial-sector portfolio is not the whole financial industry. Any reported control count should preserve its assessed denominator and observation date. No sector Atlas rating is presented.

A credential-related association does not automatically identify an employee. The identity owner should determine the relationship and current validity. A bank-domain reference in a post is also not proof that the bank's own infrastructure was accessed.

Payment-card figures retain the narrow scope in Chapter 8. They concern payment-card records in the retained post corpus. They do not measure national exposure, theft or loss.

9.7 Sector guidance complements incident response

OJK and BSSN held an April workshop for digital-finance operators covering preparedness, detection, response and recovery. A November OJK account describes cyber-resilience guidance for digital lending. These are preventive and capacity-building developments. [S52][S53]

They should not be counted as incidents affecting the participants. Their operational value lies in the functions that institutions can test: clear ownership, incident detection, controlled response and recoverability.

A financial institution should tie such guidance to its own service register. The register should identify regulated activities, external dependencies, critical information and reporting recipients.

9.8 Reporting readiness should begin with applicability

Commercial-bank cyber reporting under SEOJK 29/2022 includes initial notification within 24 hours after the bank knows of the incident. The fuller report is due within five working days after knowledge. [S15]

BI's scoped framework uses one hour after knowledge for initial cyber notification. Its fuller report is due within three calendar days after occurrence. An institution must preserve that different trigger rather than substitute one common timestamp. [S18]

Where another authority requires faster reporting, the OJK circular includes a simultaneous-reporting provision. Legal and compliance owners should identify overlapping duties before the incident. The incident commander should supply a common factual record. [S15]

9.9 A financial incident needs joint closure

Workstream	Owner	Closure question
Identity	Identity operations	Were the relevant accounts, sessions and permissions validated?
Transactions	Financial-crime and finance teams	Were disputed movements reconciled and customer outcomes recorded?
Applications	Service owner	Were the affected functions restored and the access path addressed?
Data	Privacy and data owners	Was the information scope assessed and updated?
Reporting	Legal and compliance	Were applicable recipients notified on the correct clock?
Customers	Customer operations	Were authenticated support and protective instructions available?
Recovery	Continuity owner	Was the fallback or restored service tested?

A case should not be closed because one workstream finishes first. Transaction reconciliation can continue after technical containment. Customer remediation can continue after service restoration.

The executive owner should receive separate status for those outcomes. This supports a candid account of progress without allowing a restored website or disabled account to stand in for complete recovery.

KEY TAKEAWAYS

01

Keep access, data, transaction and availability findings separate

02

Reconcile reported losses and customer outcomes with their units

03

Prepare scoped reporting routes before an incident

CHAPTER 10

Regulatory response

10

THIS CHAPTER ANSWERS

Which reporting duties apply to a personal-data failure or a cyber incident, and how do their triggers differ?

3 × 24 h

Statutory PDP written-notice period in its stated circumstances

10.1 The PDP duty is already in statute 90
10.2 Administrative sanctions are a legal ceiling 90
10.3 PP 33/2026 has a future effective date 91
10.4 Authority formation remains a dated status question 91
10.5 IIV reporting has a defined organisational route 91
10.6 Commercial-bank cyber reporting remains distinct 92
10.7 BI reporting uses a shorter initial period 92
10.8 A common record can support different clocks 93
10.9 Rehearse the evidence needed for a notification 93

CHAPTER 10

Regulatory response

IN SHORT

Indonesia's framework combines the PDP statute, IIV arrangements and sector-specific financial rules. Their deadlines have different recipients and triggers. PP 33/2026 was issued in 2026, with official accounts identifying 16 January 2027 as its effective date. Authority-formation statements remain dated and qualified. Legal and operational owners should map applicable duties to each service, preserve occurrence and discovery evidence, and rehearse notification with delivery acknowledgements.

10.1 The PDP duty is already in statute

Law 27/2022 on Personal Data Protection was enacted and promulgated on 17 October 2022. BPK's official record lists it as in force. Its 2022 origin should not obscure its relevance to 2026 incident decisions. [S5]

Article 46 requires a controller, in the event of a personal-data protection failure, to provide written notification within 3 × 24 hours. The recipients are the data subject and the institution. [S6]

The notification must include at least the personal data disclosed, when and how it was disclosed, and the controller's handling and recovery efforts. In certain circumstances, the controller must also notify the public. [S6]

The article's original wording does not expressly say "after discovery". This report preserves that statutory phrasing. Legal owners should determine the applicable trigger and any further requirements from the relevant legal text.

A cyber event and a personal-data failure are not interchangeable labels. The incident team should gather facts that allow the privacy and legal owners to assess the statutory condition. It should not delay evidence preservation while terminology is debated.

10.2 Administrative sanctions are a legal ceiling

Article 57 provides for written warnings, temporary suspension of processing, deletion or destruction of personal data, and administrative fines. It assigns imposition of those sanctions to the institution. [S6]

The fine ceiling is two percent of annual income or annual receipts, subject to violation variables. It is a statutory ceiling. This report does not describe it as an automatic fine for every incident or a measured financial loss.

The existence of the ceiling does not establish that a particular organisation has been found responsible. In the customer-platform case, the supporting November account said examination continued and responsibility or sanctions had not been determined. [S45]

Leadership should therefore separate incident response from adjudicated liability. A protective action can be necessary before a fault finding. A final legal conclusion requires its own authority and evidence.

10.3 PP 33/2026 has a future effective date

BPOM's 15 September account says PP 33/2026 was promulgated on 16 July 2026. Gianyar's official account identifies it as the implementing regulation for Law 27/2022 and describes a six-month period before effectiveness. [S7][S8]

A 12 November Bawaslu account gives the effective date as 16 January 2027. The accurate temporal statement is that the implementing regulation was issued in 2026 with a future effective date. [S9]

It would be inaccurate to describe the regulation as still absent. It would also be inaccurate to describe it as already effective at the 22 November cutoff. Organisations can prepare for a future-effective regulation without collapsing those dates.

Preparation should connect legal requirements to real data flows. The privacy owner should identify controllers, processors, data categories and high-impact services. Application owners should confirm how those relationships appear in production.

The legal team should record the applicable text and version for each obligation. Training slides and event accounts can explain developments, but they should not replace the authoritative rule when deciding detailed procedural requirements.

10.4 Authority formation remains a dated status question

Article 58 says the PDP institution is designated by the President and responsible to the President. Further institutional arrangements are to be governed by Presidential Regulation. [S6]

Komdigi's 22 July statement described formation of an independent authority as being finalized. It referred to a targeted completion period. A projected date is not evidence that formation was completed. [S10]

The 12 November Bawaslu account quotes an expert saying the supervisory institution had not been formed. An ELSAM event account also describes a Komdigi official discussing pending regulatory formalities. Those are dated statements with different source types. [S9][S56]

This report does not substitute the ministry for the Article 58 institution or assert an appointment not established by the supporting sources. Organisations should retain the relevant official reporting contacts and confirm the applicable channel when a duty arises.

Institutional uncertainty should not erase internal accountability. The controller still needs an incident owner, a privacy assessment and records supporting its actions. Sector-specific reporting routes may also apply.

10.5 IIV reporting has a defined organisational route

Perpres 82/2022 establishes the protection framework for vital information infrastructure. Its scope includes identification, protection, supervision and coordination. BSSN is the coordinator, with ministries and regulators responsible for their sectors. [S11][S12][S13]

Article 13 requires the organisational incident-response team to report an IIV cyber incident to the sectoral team. The national team receives a copy. The period is no later than 1 × 24 hours after the incident is discovered. [S12]

If the relevant sectoral team has not been formed, the report goes to the responsible ministry or agency, with a copy to the national team. The same period applies. [S12]

This is an IIV duty. It is not a universal deadline for every business website. The organisation's legal and service owners should identify the affected infrastructure and applicable designation before relying on the reporting map.

The response team should maintain a tested contact list. A plan that names a recipient but lacks a current delivery route leaves a practical gap. Rehearsals should include acknowledgement and an alternate route.

10.6 Commercial-bank cyber reporting remains distinct

SEOJK 29/SEOJK.03/2022 addresses cyber resilience and security for conventional and Islamic commercial banks. Section IX specifies initial notification and a fuller cyber-incident report. [S14][S15]

Initial notification goes to OJK within 24 hours after the bank knows of the cyber incident. It is directed electronically in writing to the bank's supervisor. The bank should ensure that OJK receives it. [S15]

The fuller report goes through OJK's reporting system within five working days after the cyber incident becomes known. Those are working days, not calendar days. [S15]

Where another authority requires faster notification or reporting, the circular provides for simultaneous submission to OJK under that timing. This requires an applicability assessment rather than a single institution-wide assumption. [S15]

OJK's official record states that PADK 1/2026 took effect on 1 March 2026 and revoked SEOJK 21/SEOJK.03/2017. [S16] Its detailed reporting scope was not independently confirmed from the original text. [S17]

A policy update should preserve that distinction. Replacing an obsolete citation is useful, but copying a non-cyber reporting paragraph into a cyber response plan can introduce a new error.

10.7 BI reporting uses a shorter initial period

PADG 24/2024 implements BI's information-security and cyber-resilience framework. Its stated scope includes payment-system operators, money-market and foreign-exchange-market actors, and other parties regulated and supervised by BI. [S18]

Article 45 requires initial cyber notification within one hour after the operator knows of the incident. The fuller incident report is due within three calendar days after occurrence. [S18]

Those trigger words differ. An incident can have an estimated occurrence time and a later discovery time. The record should preserve both rather than use the first timestamp entered into a ticket.

PADG 29/2026 took effect on 25 September 2026. It strengthened reporting sanctions and clarified BI's vital-financial-infrastructure powers. The amendment refers explicitly to the one-hour and three-calendar-day periods. [S19][S20]

The amended incidental-reporting penalty is Rp5 million for the specified late or missing reports. The existence of that provision does not establish a penalty in a particular case. [S20]

10.8 A common record can support different clocks

Framework	Condition or trigger	Recipient	Period
Law 27/2022, Article 46	In the event of a personal-data protection failure	Data subjects and the institution; public notice in certain circumstances	Written notice within 3 × 24 hours [S6]
Perpres 82/2022, Article 13	Discovery of a cyber incident affecting IIV	Sectoral team, copying national team; ministry or agency fallback where applicable	No later than 1 × 24 hours after discovery [S12]
SEOJK 29/2022, Section IX	Bank knows of cyber incident	OJK supervisor	Initial written electronic notice within 24 hours [S15]
SEOJK 29/2022, Section IX	Bank knows of cyber incident	OJK reporting system	Fuller report within five working days [S15]
PADG 24/2024, Article 45	Operator knows of cyber incident	Bank Indonesia	Initial notification within one hour [S18]
PADG 24/2024, Article 45	Cyber incident occurs	Bank Indonesia	Incident report within three calendar days [S18]

The table is an operational comparison of the cited provisions. It is not a determination that every row applies to every organisation or every incident.

Legal and compliance owners should maintain an applicability register for regulated services. The incident commander should maintain the event record. Combining those functions supports timely decisions without erasing legal differences.

10.9 Rehearse the evidence needed for a notification

The incident record should distinguish confirmed facts, estimates and unresolved propositions. It should preserve the source of each material update. A preliminary scope should remain preliminary.

The record should also retain the time at which the organisation knew each fact. A later conclusion about occurrence should not silently replace the original discovery timestamp.

A rehearsal should test preparation, authorization, delivery and acknowledgement. The legal owner should determine recipients. The communications owner should ensure that customer instructions match the current scope.

Completion means the organisation can show who made the decision, which facts informed it and how delivery was confirmed. A template alone does not establish readiness.

KEY TAKEAWAYS

01
Map each obligation to its legal scope and recipient

02
Preserve occurrence and discovery as separate timestamps

03
Rehearse notification with authorization and delivery evidence

CHAPTER 11

Conditional outlook

11

THIS CHAPTER ANSWERS

Which future observations would justify changing Indonesia's defensive priorities?

4

Planning scenarios with explicit escalation signals

11.1 Judgements have defined confidence 96
11.2 Scenario one: an access offer maps to a current account 96
11.3 Scenario two: identity material appears in a fraud workflow 97
11.4 Scenario three: a warning precedes measurable disruption 97
11.5 Scenario four: an extortion listing has corroborating evidence 97
11.6 Observations that would change the report 98

CHAPTER 11

Conditional outlook

IN SHORT

The evidence supports planning for advertised access, identity misuse, service interruption and extortion-related continuity pressure. It does not support a national attack probability or a precise loss forecast. Each scenario below states a trigger, an alternative and the observation that would change the assessment. Confidence attaches to those propositions. Use the scenarios to prepare decisions, then escalate only when current evidence supports the relevant condition.

11.1 Judgements have defined confidence

There is high confidence that the retained advertisements and Ransompedia listings existed within their stated populations. That confidence concerns publication. It does not transfer to the authenticity of every advertised dataset or permission. [S1][S2]

There is stronger support for the particular facts that controllers and authorities reported in the external dossiers. Their provisional estimates, investigative allegations and disputed conclusions remain bounded by the sources. [S35][S36][S40][S44]

Vendor reports provide supported campaign observations and publisher-specific interpretations. Their evidence does not establish a complete national picture. Historical or unknown activity dates reduce what they can say about activity within this window. [S21][S28][S29][S42][S43]

The planning assumptions below do not convert those observations into statistical forecasts. They explain which decisions should be ready and which new facts would justify using them.

11.2 Scenario one: an access offer maps to a current account

The access advertisements make current-account validation a reasonable preparedness task. The critical signal would be a credible match to an owned, enabled account or an unauthorized session. [S1]

The alternative is that the advertisement is outdated, inaccurate, brokered or unrelated to the organisation's current service boundary. A similar sector label cannot resolve that possibility.

If internal evidence confirms unauthorized access, the identity and service owners should scope permissions and contain the relevant sessions. The incident commander should determine whether broader access or information exposure occurred.

The assessment should de-escalate where an owner establishes that the account is disabled, remediated or unrelated. Closure should preserve that evidence. A low-confidence advertisement should not leave an organisation in indefinite emergency mode.

11.3 Scenario two: identity material appears in a fraud workflow

The corpus includes identity-document demand and an alleged identity-verification dataset. These observations support testing defenses against replay and impersonation. They do not prove that a particular onboarding journey has been abused. [S1]

Escalation would require a relevant internal signal. Examples include repeated identity use, an unauthorized representative or a credible match between alleged material and an owned customer relationship.

The alternative is that an advertisement concerns older, misattributed or unauthenticated material. The fraud owner should therefore preserve the evidence connecting the external signal to the internal case.

Protective action should match the validated relationship. A customer-support warning, an applicant review and a transaction restriction require different owners and completion tests.

11.4 Scenario three: a warning precedes measurable disruption

Government preparedness notices support readiness checks for relevant public services. They do not establish that every warned technique will occur or that a named actor can cause the claimed impact. [S48]

Escalation should follow measured service degradation, unauthorized changes or another validated event. The service owner should preserve the affected functions and time period.

The alternative is no corresponding impact, a protective restriction or a separate operational problem. The November blocking and global-service accounts demonstrate why those alternatives matter. [S47][S50]

A continuity response can proceed while attribution remains unresolved. Customer communication should describe service status and official recovery routes. The incident record should later distinguish the confirmed cause from earlier hypotheses.

11.5 Scenario four: an extortion listing has corroborating evidence

Ransompedia's listing population justifies extortion readiness and a defined review route. A listing alone does not establish encryption, exfiltration or a payment demand received by the organisation. [S2]

Escalation would follow corroborating telemetry, an authenticated incident report or another supported event. The incident commander should determine which services and data are involved.

The alternative is an uncorroborated allegation, repeated material or a listing whose scope differs from the seller's description. The organisation should preserve its review rather than declare an outcome based on the listing alone.

Continuity work should cover identity dependencies and restoration order. Privacy work should assess information consequences separately. A restored service does not close the data-scope question.

11.6 Observations that would change the report

New observation	Assessment it would change	Required evidence
Confirmed unauthorized privileged session	Access allegation becomes a current-access incident	Account, session and permission evidence
Controller's final data-scope notice	Preliminary account or field estimates can be updated	Dated controller account and case linkage
Official appointment or implementing instrument	Dated authority-formation status can change	Applicable official instrument
Measured service disruption matching a claim	A warning or allegation gains impact evidence	Service timeline and event correlation
Reliable new campaign activity dates	Unknown or historical chronology can be refined	Primary-source activity dates
Corroborated transaction outcome	Potential misuse can become a validated financial event	Reconciled transaction and customer case

These observations should change the specific proposition they address. An official formation instrument does not validate an unrelated breach allegation. A confirmed dataset does not establish every advertised access permission.

KEY TAKEAWAYS

01
Attach confidence to a specific proposition

02
Prepare scenario decisions before their triggers occur

03
Escalate or de-escalate with current evidence

CHAPTER 12

Accountable action plan

12

THIS CHAPTER ANSWERS

Who owns the next 30, 60 and 90 days, and what evidence demonstrates completion?

90

Days of sequenced improvement, not a delay for live threats

12.1 The first decision is whether the risk is current 100
12.2 Thirty-day lane: establish ownership and current facts 100
12.3 Sixty-day lane: test the response paths 101
12.4 Ninety-day lane: demonstrate durable closure 102
12.5 Measures that leadership can request 103
12.6 Role-specific responsibilities 104
12.7 How Brandefense supports the workflow 104

CHAPTER 12

Accountable action plan

IN SHORT

A useful plan connects an observed signal to an owner, a trigger and a closure test. Current unauthorized access warrants immediate response. The 30, 60 and 90-day lanes sequence capability improvements around that duty. Priorities are account validation, service recovery, transaction integrity and notification readiness. Leadership should require evidence of completion from the responsible owner and keep unresolved scope visible. Start with the live-risk validation queue and assign an executive sponsor.

12.1 The first decision is whether the risk is current

The schedule below is a planning horizon. It does not authorize waiting when current unauthorized access or harmful activity is established.

An external claim should enter a validation queue with an owner. The owner should record the proposition, service relationship and available current evidence. The incident commander decides escalation from that record.

Disruptive changes should follow validated risk and a service-impact assessment. This is especially important for customer-facing identities, shared administration and financial workflows.

12.2 Thirty-day lane: establish ownership and current facts

10–30 days		
Review relevant access advertisements when they plausibly match an owned service	ACCOUNTABLE OWNER Identity lead and service owner	COMPLETION EVIDENCE Account state, permissions, session review and recorded disposition
Map every critical service to its application, identity and supplier dependencies	ACCOUNTABLE OWNER Service-management lead	COMPLETION EVIDENCE Approved dependency register with named owners
Confirm reporting applicability for each regulated service	ACCOUNTABLE OWNER Legal and compliance leads	COMPLETION EVIDENCE Recipient, trigger and deadline register tied to current instruments

Preserve customer-data scope when a credible allegation or disclosure arises

ACCOUNTABLE OWNER

Privacy lead and data owner

COMPLETION EVIDENCE

Field-specific scope record with confirmed, potential and unresolved categories

Review privileged remote access after current-access evidence or unexplained changes

ACCOUNTABLE OWNER

Identity operations

COMPLETION EVIDENCE

Session disposition, privileged-group review and scoped containment record

Validate Windows archive-component inventory and apply supported vendor updates where vulnerable; priority derives from historical CVE-2025-8088 activity [S22][S25]

ACCOUNTABLE OWNER

Endpoint management lead

COMPLETION EVIDENCE

No WinRAR through 7.12 remains in the agreed scope, except owned exceptions; 7.13 is the fixed minimum, not a latest-version target [S22][S25]

The first lane should remove ambiguity about who can validate an allegation. A security mailbox without a business owner can receive a signal while leaving the underlying decision unresolved.

The incident owner should track time to ownership as well as time to closure. An unresolved case should state which fact or access is missing. It should not be closed merely because no public update appeared.

12.3 Sixty-day lane: test the response paths

31–60 days

Exercise restoration of one critical customer or operational workflow

ACCOUNTABLE OWNER

Continuity lead and service owner

COMPLETION EVIDENCE

Observed restoration result, dependencies tested and unresolved exceptions

Rehearse concurrent PDP, IIV, OJK or BI reporting where applicable

ACCOUNTABLE OWNER

Legal lead and incident commander

COMPLETION EVIDENCE

Decision times, authorized drafts, delivery rehearsal and acknowledgements

Test whether unauthorized identity use can bypass financial approval

ACCOUNTABLE OWNER
Financial-crime lead and application owner

COMPLETION EVIDENCE
Documented test scope, approval-path result and corrected exceptions

Review content-administration access for distributed websites

ACCOUNTABLE OWNER
Web-service owner

COMPLETION EVIDENCE
Named administrators, trusted deployment route and restoration check

Test applicant and representative authority checks against identity replay scenarios

ACCOUNTABLE OWNER
Fraud operations lead

COMPLETION EVIDENCE
Approved cases, escalation outcomes and exception owners

A recovery exercise should reach a business outcome. It should not end when a server starts or a backup file opens. The service owner should show that the tested workflow functions.

A notification exercise should also test a real handoff. The incident commander supplies facts. Legal determines applicability. Communications prepares customer guidance. The authorized recipient and delivery route must be known.

12.4 Ninety-day lane: demonstrate durable closure

161–90 days

Recheck completed external-control corrections in production

ACCOUNTABLE OWNER
Infrastructure lead

COMPLETION EVIDENCE
Current observation and closed change record

Validate supplier access after material service or contract changes

ACCOUNTABLE OWNER
Supplier-risk and identity leads

COMPLETION EVIDENCE
Current permissions, owner confirmation and exception disposition

Review high-volume data exports and sensitive log content

ACCOUNTABLE OWNER
Data and application owners

COMPLETION EVIDENCE
Approved export roles, monitoring review and remediated logging exceptions

Test authenticated outage communications and alternate customer support

ACCOUNTABLE OWNER
Communications and customer-operations leads

COMPLETION EVIDENCE
Exercise results, official channels and correction log

Review recurring allegations against earlier incident records

ACCOUNTABLE OWNER
Incident-management lead

COMPLETION EVIDENCE
Linked cases, current-account checks and justified closure states

The final lane should reduce repeated ambiguity. A recurring advertisement should trigger comparison with the earlier case, followed by a current-risk check. It should not automatically create a new incident or inherit an obsolete closure.

A control exception should also retain its service consequence. Technical completion is stronger when the owner can explain which access path or workflow changed and how the result was checked.

12.5 Measures that leadership can request

Measure	Target for the plan	Evidence source
Ownership of relevant external signals	Every signal in the agreed queue has an accountable owner	Incident register
Current-account validation	Every escalated access allegation has a recorded account and session disposition	Identity case record
Critical-service dependency coverage	Every service selected for the programme has an approved dependency owner	Service register
Recovery evidence	Each selected critical workflow has an observed exercise result	Continuity record
Notification readiness	Every applicable reporting route is rehearsed or has an explicit exception	Legal and incident exercise record
Data-scope discipline	Every customer-data case separates confirmed, potential and unresolved scope	Privacy case record
Financial reconciliation	Every escalated transaction case retains status and customer outcome	Financial-crime record

These are proposed completion targets, not measurements already achieved by Indonesian organisations. The executive sponsor should agree the service population and review exceptions.

A useful board discussion asks why a case remains unresolved and which decision follows next. It should not reward a falling alert count if ownership or evidence quality has deteriorated.

12.6 Role-specific responsibilities

The CISO owns coordination of security evidence and escalation. The service owner owns the business consequence and restoration acceptance. Neither should have to infer the other's decision from a dashboard.

The identity lead validates accounts, sessions and privilege. The privacy lead assesses data consequences. Financial-crime teams validate transactions. Legal and compliance determine applicable reporting duties.

Communications and customer operations should receive the same current facts. Their messages can be concise while preserving what remains unresolved. Changes in scope should be recorded and reflected consistently.

The executive sponsor resolves ownership conflicts and funds the required work. That role is particularly important where a shared supplier, distributed website estate or several reporting duties cross organisational boundaries.

12.7 How Brandefense supports the workflow

The report uses Brandefense Blackhole post observations, Ransompedia extortion listings and the selected-organisation context described in Appendix A. Each view supports a different validation decision. [S1][S2][S4]

External intelligence is useful when it reaches an accountable owner with the appropriate context. It should connect the allegation, relevant service and time period to the organisation's own evidence.

Brandefense describes cyber threat intelligence, digital risk protection and attack-surface capabilities. To discuss those capabilities against the workflows in this report, request a demo. [S82]

The organisation remains responsible for validating current access, assessing impact and deciding its response. The action plan makes those responsibilities explicit and gives each owner a completion test.

KEY TAKEAWAYS

01

Assign an owner to each relevant signal

02

Test recovery and reporting with real handoffs

03

Close work with evidence of the resulting service condition

APPENDICES

Appendices

A–D

THIS CHAPTER ANSWERS

What are the populations, evidence boundaries and source records behind the decisions?

4

Appendices for scope, evidence, sources and terms

Appendix A. Scope and evidence boundaries 106

Appendix B. Redacted evidence register 108

Appendix C. Source verification records 110

Appendix D. Glossary 113

Appendix A. Scope and evidence boundaries

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

A.1 Observation window

The post-date window is 1 January to 22 November 2026. The recent period is 8 to 22 November. Observations were captured before the end of the cutoff day. Later publications that day are outside this snapshot.

Extortion figures use listing dates. Vendor and official accounts preserve activity, discovery, notification and publication dates separately. Historical events can inform defensive context without being counted as 2026 activity.

A.2 Populations remain separate

Population	Unit	Main boundary
Country-tagged post metadata	Posts bearing the country tag within the window	A tag does not establish targeting or a distinct incident
Retained post corpus	Retained publications within its coverage	Selected evidence does not estimate population-wide relevance
Extortion listings	Ransompedia listings by listing date	Claims can repeat organisations and do not prove intrusion
Selected candidate portfolio	Primary domains in the stated portfolio	Selection does not estimate national prevalence
Passive observations	Records assessed for each condition	Coverage differs by condition; unavailable observations are not zeros
Credential or device associations	The unit stated in the result	Relationships and current validity require validation
Payment-card records	Records in the retained post corpus	Not national exposure, theft or fraud loss
Public dossiers	Cases with explicit evidence types	A dossier can contain several allegations or milestones

The country-tag metadata population and retained post corpus are distinct. A proportion observed in the retained corpus is not applied to the full tagged population. Posting volume is not an attack rate. [S1]

Passive observations cover 241 of 250 selected candidate domains; nine were unavailable. TLS statuses use a 241-domain base. Header observations use the separate 154-domain HTTP base. No composite hygiene index or sector rating is reported. [S3][S4]

Atlas provides the national headline of 59/100 for the selected 250-domain portfolio. Only that national rating is published. Anonymous sector tables report exposure counts separately. Historical records, current sale listings and passive observations retain their different time meanings and validation tasks. [S4]

A.3 Evidence language

"Advertised", "claimed" and "offered" preserve actor allegations. "Reported by police" preserves an investigative account. "The controller disclosed" preserves the controller's statement. None is silently upgraded to an independently proven outcome.

A claim can contain authentic material while overstating current access. A public disclosure can contain a provisional count. Confidence therefore attaches to the particular proposition being assessed.

"Not established" describes an unresolved proposition. It does not declare a claim fabricated or prove that no incident occurred. The report does not infer a completed sale or ransom payment from an asking price.

A.4 Relationships and redactions

Personas, posts, datasets, group labels and organisations are separate concepts. A map edge identifies its evidence type. A shared tool or a repeated title does not automatically establish a common operator.

Victims are described by roles unless a naming decision meets the publication requirements. Public quotations remove identifying or contact material. Original source references remain in the private evidence record.

Where a revealing article URL would identify a withheld victim, Appendix C uses a publisher root or withholds the URL. This preserves the distinction between a citable account and permission to expose the affected organisation.

A.5 Limits that affect decisions

The selected portfolio is not a national survey. The corpus does not establish all Indonesian cyber incidents. Listing totals do not establish loss, encryption or unique affected organisations.

An unchanged result at one observation point does not prove a control operated throughout the year. A later disclosure does not establish when the underlying activity began.

The legal comparison describes cited provisions with their scope and timing. Organisational applicability requires a current service and legal assessment. The action plan's targets are proposed completion criteria, not observed national performance.

Appendix B. Redacted evidence register

Dossier	Evidence	Date meaning	Shown in
A–I	Retained advertisements and circulation claims	Supplied post dates; current access and outcomes remain separate	Chapter 4
J	Customer-platform controller disclosure and regulatory follow-up	28 October disclosure; 5 November follow-up	Chapter 4
K	Regional-bank police account and initial complaint reporting	22 February activity; later investigation milestones	Chapters 4 and 9
L	Education-funding investigative account	December 2025 and January 2026 transactions	Chapter 4
M	Website-access-sale investigation	July publication and September update	Chapters 4 and 5
N	Disputed personnel-application account	June discovery, notification and reporting	Chapter 4
O	Local-service website account	August takedown and reporting	Chapter 4
P–R	Additional retained claim dossiers	Supplied post dates	Chapter 4

Card	Dossier	Post date	Venue	Alias	Language	Shown in
B01	A	2026-10-17	Forum advertisement	updap	English	Chapter 4
B02	B	2026-10-31	Forum advertisement	marlanwg	English	Chapter 4
B03	C	2026-10-29	Forum advertisement	CocoMel0n	English	Chapter 4
B04	D	2026-11-22	Forum advertisement	AFKForever	English	Chapter 4
B05	E	2026-11-21	Forum advertisement	SUB-ZER0	English	Chapter 4
B06	F	2026-03-04	Forum advertisement	DrBisoun0urs	English	Chapter 4
B07	G	2026-01-05	Forum advertisement	sellingood	English	Chapter 4

Card	Dossier	Post date	Venue	Alias	Language	Shown in
B08	H	2026-01-12	Forum advert-isement	Darmanboy24	English	Chapter 4
B09	I	2026-11-12	Forum advert-isement	updap	English	Chapter 4
B10	P	2026-05-05	Forum advert-isement	alwayschina	English	Chapter 4
B11	Q	2026-05-14	Forum advert-isement	Kyyzo	English	Chapter 4
B12	R	2026-06-12	Forum advert-isement	Governer	English	Chapter 4

The register links evidence to propositions. It is not an incident count. Several posts can support one circulation dossier, and several dates can describe one underlying event.

Appendix C. Source verification records

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

S1: Brandefense Blackhole, bounded Indonesia-related post observations. Own data; no public raw-data URL. Verified on 22 November 2026.

S2: Ransompedia, country-tagged extortion listings by listing date. Own data; no public raw-data URL. Verified on 22 November 2026.

S3: Selected-domain passive observations with condition-specific coverage. Own data; no public raw-data URL. Verified on 22 November 2026.

S4: Brandefense Atlas exposure snapshot and selected candidate portfolio, 250 primary domains, read 22 November 2026. Own data; no public raw-data URL. Verified on 22 November 2026.

S5: BPK, Law 27/2022 official record. Source. Verified on 23 November 2026.

S6: Law 27/2022, original statutory text. Source. Verified on 23 November 2026.

S7: BPOM, PDP implementation preparation, 15 September 2026. Source. Verified on 22 November 2026.

S8: Gianyar government, PP 33/2026 preparation, 16 September 2026. Source. Verified on 23 November 2026.

S9: Bawaslu Makassar, PP 33/2026 and authority-status event account, 12 November 2026. Source. Verified on 22 November 2026.

S10: Komdigi, authority-formation statement, 22 July 2026. Source. Verified on 22 November 2026.

S11: BPK, Perpres 82/2022 official record. Source. Verified on 23 November 2026.

S12: Perpres 82/2022, original IIV text. Source. Verified on 23 November 2026.

S13: Cabinet Secretariat, IIV framework explanation, 15 June 2022. Source. Verified on 22 November 2026.

S14: OJK, SEOJK 29/2022 official record. Source. Verified on 23 November 2026.

S15: SEOJK 29/2022, commercial-bank cyber-resilience circular. Source. Verified on 23 November 2026.

S16: OJK, PADK 1/2026 official record. Source. Verified on 23 November 2026.

S17: PADK 1/2026, commercial-bank IT regulation. Source. Host unavailable on 23 November 2026; supporting passage not independently confirmed.

S18: BI, PADG 24/2024 cyber-resilience framework. Source. Verified on 23 November 2026.

S19: BI, PADG 29/2026 official summary. Source. Verified on 23 November 2026.

S20: PADG 29/2026, original amending text. Source. Verified on 23 November 2026.

S21: Check Point Research, Amaranth-Dragon, 4 February 2026. Source. Verified on 22 November 2026.

S22: CVE Program, CVE-2025-8088 published record. Source. Verified on 22 November 2026.

S24: NVD, CVE-2025-8088 human-readable record. Source. Verified on 22 November 2026.

S25: WinRAR, 7.13 final release advisory. Source. Verified on 22 November 2026.

S26: RARLAB, version 7.13 change log. Source. Verified on 22 November 2026.

S27: ESET, WinRAR exploitation research, 11 August 2025. Source. Verified on 22 November 2026.

S28: Check Point Research, SilentDelivery and the proposed CopperDragon supplier framework, 10 November 2026. Source. Verified on 23 November 2026.

S29: Kaspersky, Silver Fox tax campaign, 30 April 2026. Source. Verified on 23 November 2026.

S35: Police, education-funding investigation, 3 April 2026. Source (article URL withheld). Verified on 22 November 2026.

S36: Police, regional-bank investigation follow-up, 15 July 2026. Source (article URL withheld). Verified on 22 November 2026.

S37: ANTARA, regional-bank complaint, 23 February 2026. Source (article URL withheld). Verified on 22 November 2026.

S38: Police, website-access-sale investigation, 30 July 2026. Source (article URL withheld). Verified on 23 November 2026.

S39: BSSN, historical website-defacement response guide, June 2023; official judiciary-hosted copy. Source. Verified on 22 November 2026.

S40: detik, disputed personnel-application account, 27 June 2026. Source (article URL withheld). Verified on 22 November 2026.

S41: Bali Tribune, local-service website account, 10 August 2026. Source (article URL withheld). Verified on 22 November 2026.

S42: Proofpoint, BlueMoon / UNK_QuietRacket, 9 September 2026. Source. Verified on 22 November 2026.

S43: Kaspersky, StrikeShark, 24 June 2026. Source. Verified on 22 November 2026.

S44: Fore Coffee, customer-platform privacy notice, 28 October 2026. Source. Verified on 23 November 2026.

S45: detik, Komdigi examination of customer-platform report, 5 November 2026. Source. Verified on 22 November 2026.

S46: Komdigi, old-data recirculation account, 2 October 2026. Source. Verified on 22 November 2026.

S47: Komdigi, blocking-related availability account, 8 November 2026. Source. Verified on 22 November 2026.

S48: Komdigi, public-system preparedness notice, 10 November 2026. Source. Verified on 22 November 2026.

S49: Komdigi, AI-agent threat coordination, 10 November 2026. Source. Verified on 22 November 2026.

S50: Kemenkes CSIRT, official relay of BSSN global-service outage advisory, 13 November 2026. Source. Verified on 23 November 2026.

S51: Police, global-attack rumour fact-check, 21 November 2026. Source. Verified on 23 November 2026.

S52: OJK, digital-finance resilience workshop, 30 April 2026. Source. Verified on 23 November 2026.

S53: OJK, digital-lending resilience guidance, 11 November 2026. Source. Host unavailable on 23 November 2026; passage last verified on 22 November 2026.

S56: ELSAM, authority-formation event account, 4 November 2026. Source. Verified on 22 November 2026.

S57: Police, phishing-tools enforcement account, 22 April 2026. Source. Verified on 22 November 2026.

S66: Police, technology-access ethics account, 18 November 2026. Source (article URL withheld). Verified on 22 November 2026.

S81: DataReportal / Kepios, Digital 2026 Indonesia; late-2025 baseline. Source. Verified on 22 November 2026.

S82: Brandefense, request-a-demo page and capability overview. Source. Verified on 22 November 2026.

S83: OSS: NIB as official business identification. Source. Verified on 22 November 2026.

S84: Jakarta civil-registration service: KTP electronic resident identity card. Source. Verified on 22 November 2026.

S85: MITRE ATT&CK, T1189 Drive-by Compromise. Source. Verified on 22 November 2026.

S86: MITRE ATT&CK, T1566.001 Spearphishing Attachment. Source. Verified on 22 November 2026.

S87: RFC Editor, RFC 7489, DMARC. Source. Verified on 22 November 2026.

S88: RFC Editor, RFC 7208, SPF. Source. Verified on 22 November 2026.

S89: RFC Editor, RFC 6376, DKIM signatures. Source. Verified on 22 November 2026.

S90: RFC Editor, RFC 4033, DNSSEC introduction and requirements. Source. Verified on 22 November 2026.

S91: RFC Editor, RFC 8446, TLS. Source. Verified on 22 November 2026.

S92: RFC Editor, RFC 6797, HSTS. Source. Verified on 22 November 2026.

S93: W3C, Content Security Policy Level 3, Working Draft, policy purpose and delivery. Source. Verified on 22 November 2026.

S94: RFC Editor, RFC 7034, HTTP Header Field X-Frame-Options. Source. Verified on 22 November 2026.

S95: WHATWG, Fetch Standard, X-Content-Type-Options. Source. Verified on 22 November 2026.

S96: BSSN, Indonesia Cyber Security Landscape 2023, published 2024; official ministry CSIRT-hosted copy. Source. Verified on 23 November 2026.

S97: BSSN, Regulation 5/2025 on the 2025-2029 Government Administration Vital Information Infrastructure Protection Roadmap, 19 February 2025. Source. Verified on 23 November 2026.

Appendix D. Glossary

Term	Meaning in this report
DMARC	Domain-based Message Authentication, Reporting, and Conformance: email policy that helps limit domain spoofing. Observed policy does not establish enforcement for every message. [S87]
SPF	Sender Policy Framework authorises servers to send email using a domain. A published record does not show whether individual messages passed validation. [S88]
DKIM	DomainKeys Identified Mail uses digital signatures to associate email with a signing domain. An unobserved record does not prove that signing is absent. [S89]
DNSSEC	Domain Name System Security Extensions help authenticate DNS data and detect tampering. Observed delegation evidence does not establish validation of every answer or provide encryption. [S90]
TLS	Transport Layer Security protects data in transit against eavesdropping and tampering. Observed certificate status does not assess the security of every service. [S91]
HSTS	HTTP Strict Transport Security directs browsers to use secure connections to a site. An observed header does not establish protection across every service or request. [S92]
CSP	Content Security Policy lets browsers restrict resources a page may load or execute. An observed header establishes policy presence for that response, not effective restrictions or protection across every page. [S93]
Frame-protection header	A header that limits whether browsers may display a page inside another page's frame, such as X-Frame-Options. Observed presence does not establish effective clickjacking protection or coverage across every page. [S94]
Content-type protection header	A header such as X-Content-Type-Options, whose nosniff value directs browsers to block scripts or styles with incompatible declared content types. Header presence does not establish a valid nosniff value or coverage across every response. [S95]
Account	An identity or login relationship; not automatically a unique person
Activity date	When the source says an action occurred
Advertisement	A publication offering or seeking material, access or a service
Asking price	A seller's or buyer's stated term; not a completed transaction value

Term	Meaning in this report
Claim	An assertion whose status is preserved until relevant evidence supports it
Controller	The role responsible for determining personal-data processing under the PDP framework [S6]
Corpus	The retained post population described in Appendix A
Discovery date	When an organisation or source says an event became known
Dossier	A bounded case analysis that can contain several publications or milestones
Event record	A recorded system or business event; not automatically a user or account
Extortion listing	A dated publication associating a label with an alleged target [S2]
IIV	Vital information infrastructure within the cited Indonesian framework [S12]
KTP	An electronic resident identity card, as described by the official civil-registration source [S84]
NIB	Offi- cial business identification, as described by the OSS service [S83]
Occurrence time	The estimated or established time an incident happened
Persona	A publication identity or alias, without a claim about its legal identity
Privilege	The permissions alleged or established for an account
Publication date	When a post, notice or report appeared
Recirculation	Later publication of an earlier allegation or material
Session	An authenticated access context whose state requires separate review
Supplier dependency	A service or permission on which an organisation relies
Validation	An owned assessment of the specific proposition that affects a response
Working day	The time unit used in the cited OJK fuller-report requirement [S15]

About this report

Odin by Brandefense prepared this public research edition from the bounded observations and read sources described above. It supports leadership, security, service, fraud and privacy decisions.

Public evidence preserves uncertainty and removes sensitive victim identifiers. The report does not claim a completed sale, verified current access or confirmed incident merely because a publication advertises it.

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