BRANDEFENSE COUNTRY REPORT · JAPAN 2026

Brandefense Japan Cyber Threat Landscape Report 2026

Identity, shared services and the boundaries of confirmed impact

Odin by Brandefense

Research window: 1 January–22 November 2026

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

85 of 250

selected organisations had a credential listed for sale when checked

6

detailed claim cases, each with a separate evidence boundary

146

Japan-labelled ransomware listings; each records a criminal assertion

30 / 60 / 90

day checkpoints for an owned response programme

CONTENTS

Contents

01	Executive summary	05
	Report map	09
02	Japan's operating context	10
03	National exposure and the selected organisation set	14
04	Underground activity and what the posts establish	23
05	Public incident accounts and sector decisions	39
06	Availability and connected-device risk	73
07	Threat actors, campaigns and supported relationships	77
08	Fraud targets workflows and delegated access	90
09	Banking and financial-service dependencies	95
10	Regulatory response and reporting	100
11	Outlook and conditional scenarios	105
12	Action plan	109
A	Appendix A. Scope and evidence boundaries	115
B	Appendix B. Evidence register	119
C	Appendix C. Sources	124
D	Appendix D. Glossary	134

Board and executives	01 05 11 12
CISO and response leads	03 04 07 12
SOC and identity teams	04 07 08 09
Operations and suppliers	02 05 06 12
Legal, privacy and fraud teams	05 08 09 10

About this edition

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

Japan's public disclosures and underground claims point to different response decisions: validate identity, preserve essential services and establish exactly which information was affected.

146

Japan-labelled ransomware listings; criminal assertions

51/100 (B)

national Atlas headline for the selected portfolio

101

assessed domains publishing DMARC quarantine or reject

85 of 250

organisations with a current credential listing

Contents and reading routes

Chapter	Question
1 Executive summary	Which decisions deserve immediate attention?
2 Operating context	Which dependencies change Japan's response priorities?
3 Organisation exposure	What does the selected portfolio support?
4 Underground activity	What do offers, demand and reposts establish?
5 Public incident accounts	Which disclosures change sector decisions?
6 Availability and devices	How do website and operational risks differ?
7 Actors and campaigns	Which relationships have source support?
8 Fraud	How do communication, consent and retained identity data create harm?
9 Banking	How should institutions separate supplier, customer and transaction risks?
10 Regulation	Which duties and reporting routes apply?
11 Outlook	Which conditional scenarios justify preparation?
12 Action plan	Who acts and what demonstrates completion?
Appendices A–D	Scope, evidence register, sources and glossary

CHAPTER 01

Executive summary

01

THIS CHAPTER ANSWERS

Which findings justify action by Japanese organisations?

4

decisions: identity, continuity, data retention and reporting

Four decisions for leaders 07

The year in numbers 07

CHAPTER 01

Executive summary

IN SHORT

Japan's evidence supports four priorities: identity validation, supplier continuity, data minimisation and precise reporting. Public disclosures show credentials crossing system boundaries, interrupted shared services and sensitive historical records. Underground offers add claims requiring validation, not a national incident total. Ransompedia records 146 Japan listings. DNS observations show 101 of 250 assessed domains requesting DMARC enforcement. Assign owners to identity alerts, test critical-service alternatives, review retained information and rehearse reporting from the first credible awareness.

This report combines Odin by Brandefense's retained underground material, Ransompedia listings, selected-domain observations and source-read public reporting. Their populations are separate. Posts, listings, public disclosures, credential records and affected people are never added into a national attack total. [S1][S2][S3][S4]

The requested window ends on 22 November. The cut-off day was still in progress during research, and source verification continued through 23 November. Publication, detection, initial access and a later scope update are different dates; the case cards preserve those distinctions.

1. A supplier incident can extend into customers' identity and continuity decisions. RIKEN's update describes 430 external-system credentials with collection or movement traces. The cloud-provider case describes 495 affected customer organisations. A payment-platform event required recipient-specific checks and selective resumption. These are different consequences, not one common intrusion chain. [S6][S8][S12]

2. Retained information can enlarge harm after its original purpose ends. The November rental-service warning concerns photo-ID images. The education-institution case describes retained supplier-held information. Other disclosures distinguish former customers, old account-opening records and retained test data. Data owners need a purpose and deletion decision, alongside access controls. [S71][S16][S31][S50]

3. Criminal offers require a narrower conclusion than their headlines suggest. A November property-themed offer lists lawyer-registration fields. Separate transport-themed offers advertise large row counts without authenticating their information. An older commerce reupload itself states a 2024 origin. These observations support provenance and account checks; they do not establish new incidents at every named service. [S1]

4. Extortion visibility supports recovery preparation, not a national attack count. Ransompedia records 146 Japan listings in the requested 2026 window, compared with 105 in all of 2025. The comparison uses different period lengths. NPA's 123 ransomware reports for January–June 2026 compare with 116 in January–June 2025 within that police-reporting population. The listing and police series cover different reporting populations and cannot be added or treated as mutual confirmation. [S2][S66][S254]

5. DNS policies provide a bounded control observation. Of 250 assessed domains, 101 request DMARC quarantine or reject, or 40.4%. Another 149 have a monitoring policy or no observed policy. The selected set is not nationally representative. [S4][S3]

6. Current credential listings require owned-account validation. In all, 85 of 250 selected organisations had a credential listed for sale when checked. The national Atlas headline is 51/100 (B). The portfolio contains at least 247,993 device associations and 17,488,907 historical credential-record associations. These overlapping observations do not establish current intrusion or national prevalence. [S3]

Four decisions for leaders

1. **Validate identity evidence across connected systems.** Route a relevant alert to the account owner, review privileges and sessions, and verify necessary revocation in every affected service (§3, §7, §12).
2. **Demonstrate critical-service continuity with suppliers.** Identify the actual product, tenant and business dependency, then test a minimum operating route while the provider is unavailable (§5–6, §9).
3. **Remove retained data and access without a current purpose.** Review test systems, migration copies, identity images and ended-contract integrations. Record the legal and business basis for what remains (§2, §8, §10).
4. **Prepare reporting before the investigation is complete.** Record awareness across departments, use current forms and keep service, information and customer-protection decisions consistent (§10, §12).

The year in numbers

1,073,099

Country-associated posts in the source view

WHAT IT DOES NOT MEASURE

Confirmed targeting, attacks or unique people

146

Japan-labelled ransomware listings in the requested 2026 window

WHAT IT DOES NOT MEASURE

Verified intrusions or unique victims

105

Japan-labelled listings in all of 2025

WHAT IT DOES NOT MEASURE

A matched-period baseline

43

Listing labels in the Japan population

WHAT IT DOES NOT MEASURE

Unique operators or their nationality

55 of 146

Listings under The Gentlemen, Qilin and Everest labels

WHAT IT DOES NOT MEASURE

A shared organisation or attack chain

73 / 122 / 110 / 169

Window listings for South Korea / Taiwan / Singapore / Australia

WHAT IT DOES NOT MEASURE

Population-adjusted national risk

123 / 116

Ransomware reports to NPA during January–June 2026 and January–June 2025

WHAT IT DOES NOT MEASURE

Full-window reports or a complete national census

51/100 (B)

National Atlas headline for the selected portfolio

WHAT IT DOES NOT MEASURE

A breach percentage or sector ranking

85 of 250

Organisations with a credential listed for sale when checked

WHAT IT DOES NOT MEASURE

Tested credentials, completed sales or confirmed intrusions

250

Selected organisation entries represented by primary domains

WHAT IT DOES NOT MEASURE

Independent corporate groups or national prevalence

101 of 250

Assessed domains requesting DMARC enforcement

WHAT IT DOES NOT MEASURE

Effective phishing prevention or receiver compliance

26 + 11

Case cards plus additional detailed public accounts

WHAT IT DOES NOT MEASURE

A combined count of independent intrusions

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

The public evidence includes 6 unverified underground claim cases and 31 detailed public-source accounts. Some accounts describe campaign research or revised scope rather than a newly discovered intrusion. Section 5.5 adds 137 chronological short accounts. Neither presentation count measures independent incidents. Disclosure and update dates are not necessarily attack dates.

KEY TAKEAWAYS

01

Validate the owned identity and service before choosing containment.

02

Test supplier fallbacks and review unnecessary historical information.

03

Keep criminal claims, official disclosures and reporting populations separate.

Report map

Twelve chapters connect evidence to decisions. Follow the route matching your responsibility and retain each finding's limits.

Board and executives	Fund continuity, retention and recovery decisions	01 05 11 12
CISO and response leads	Scope alerts and coordinate owners	03 04 07 12
SOC and identity teams	Validate access, sessions and suspicious delivery chains	04 07 08 09
Operations and suppliers	Preserve essential services and safe processes	02 05 06 12
Legal, privacy and fraud teams	Assess affected information and applicable reporting	05 08 09 10

01 Executive summary
What the findings justify now

02 Japan's operating context
Why services, information and physical processes need different evidence

03 National exposure and the selected organisation set
Which domain observations are available and which conclusions remain unsupported

04 Underground activity and what the posts establish
Why demand, alleged possession and recirculation differ

05 Public incident accounts and sector decisions
How official disclosures and later updates change a response

06 Availability and connected-device risk
Why website disruption is not operational-system access

07 Threat actors, campaigns and supported relationships
What supports each label, campaign and map edge

08 Fraud targets workflows and delegated access
How payment authority, remote control and application grants can be misused

09 Banking and financial-service dependencies
How banks separate transaction, information and service questions

10 Regulatory response and reporting
How reporting scope, awareness and dates affect decisions

11 Outlook and conditional scenarios
Which signals activate or change a planning scenario

12 Action plan
What an accountable owner must demonstrate

CHAPTER 02

Japan's operating context

02

THIS CHAPTER ANSWERS

Which features of Japan's digital economy change incident decisions?

3

continuity questions: identity, suppliers and physical operations

2.1 Interdependence is an operating condition 11

2.2 Three evidence questions 11

2.3 Institutional changes need precise dates 12

2.4 Geography does not establish attribution 12

2.5 Information retention is part of security 12

CHAPTER 02

Japan's operating context

IN SHORT

Japan's incident response depends on connected services: customer identity, hosted business systems, logistics and research access. A supplier disruption can stop a service without establishing an intrusion at every customer. A stolen account can expose information without proving access to a physical process. Regulatory reporting and customer protection need separate decisions. Map these dependencies, identify an alternate operating route and give each evidence question an owner.

2.1 Interdependence is an operating condition

The practical unit of response is often a service shared across several organisations. Public disclosures in Chapter 5 describe hosting, customer engagement, mobility and research services. Their users can face different consequences from the same upstream event. A customer may lose access, need to rotate a credential, or require a personal-data assessment. Those outcomes should be recorded separately.

This matters for procurement. A contract that promises an availability percentage does not necessarily identify who can supply incident logs, revoke a privileged integration or tell customers what information was accessed. Ask those questions before a supplier incident. Establish an internal service owner who can make a continuity decision while the supplier is still investigating.

A dependency register should cover the business function, the supplier's access, the information shared and the fallback. Its purpose is to support a decision during disruption. A long supplier list without those relationships does not show whether orders, payments or public enquiries can continue.

2.2 Three evidence questions

Use the following questions when a notice or criminal claim reaches the response team.

Question	Evidence to seek	Responsible owner
Is the service available?	User transactions, service status and a tested fallback	Business operations
Was information accessed or disclosed?	Relevant account, application and export records	Incident response and data owner
Did a physical process change?	Operator readings, change history and engineering assessment	Plant operations and safety

One answer cannot substitute for another. A public website outage does not establish operational-technology access. A successful login does not establish access to every record. An absence of confirmed extraction during an investigation does not establish that extraction was impossible.

These distinctions guide the case cards. Each card separates the organisation's statement, what remains unresolved and the first response the evidence supports. Publication dates describe when information became public. They do not automatically identify when activity began.

2.3 Institutional changes need precise dates

The National Cybersecurity Office (NCO) is the current official source used for national coordination and cross-sector advisories. Older material can still carry the NISC name. An institution's current name does not make a historical advisory a new incident.

An official Cabinet Office account identifies 1 October 2026 as commencement of specified public-private cooperation and access/neutralization provisions of the cyber response capability laws. This is a limited commencement statement. It is not presented as the enactment date or the commencement of every provision. [S88]

The business decision is to maintain a current reporting and coordination map. Identify the applicable regulator, incident-response contact, police route and personal-data authority. A new reporting form or coordination arrangement should be reflected in the response plan without assuming that it replaces other duties.

2.4 Geography does not establish attribution

This report takes no position on territorial disputes, historical controversies, elections or government decisions. A country label attached to a post, account or listing does not establish its operator's nationality or a state's involvement. A campaign name is a source's label for activity.

State-linked assessments appear only as the cited source's attribution, with its scope and uncertainty retained. Matching language, shared political slogans or the same public target do not establish a common operator. Defender actions follow the reported technique and the organisation's own evidence.

Regional comparisons use South Korea, Taiwan, Singapore and Australia as four peers with relevant industrial, financial, logistics or service dependencies. Their listing counts describe the observed listing population. They do not rank national security capability, political status or the likelihood that any particular organisation will be attacked.

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

2.5 Information retention is part of security

PPC's November warning about rental-service identity images connects data minimisation to incident harm. Keeping an image after its verification purpose ends leaves material available to be disclosed later. A legally required record and a convenient image copy are different things. [S71]

Data owners should distinguish information needed to deliver a service, information required by law and information retained without a current purpose. Set a retention decision for each category. Test deletion in both production and supplier-held copies, allowing for applicable preservation duties.

The same principle applies to ended customer contracts, old integration keys and former staff accounts. Their current business value may be low while their ability to expose another system remains high. Include them in access and retention reviews rather than treating the end of a contract as proof of removal.

KEY TAKEAWAYS

01

Map suppliers to the services, information and privileges they control.

02

Keep service availability, information access and physical-process evidence separate.

03

Review historical records and ended-contract access before they become a new response problem.

CHAPTER 03

National exposure and the selected organisation set

THIS CHAPTER ANSWERS

What can the organisation sample support, and which exposure decisions still require owned evidence?

85 of 250

selected organisations had a credential listed for sale when checked

3.1 Universe card 15
3.2 Exposure signals by sector 16
3.3 Device and credential populations 17
3.4 Current credential offers 20
3.5 Public email and web observations 20
3.6 The national headline and its decision boundary 21

CHAPTER 03

National exposure and the selected organisation set

IN SHORT

In all, 85 of 250 selected organisations had a credential listed for sale when checked. The national Atlas headline is 51/100 (B). The portfolio contains at least 247,993 device associations and 17,488,907 historical credential-record associations. These overlapping observations do not establish current intrusion or national prevalence. Validate current accounts, investigate relevant employee-device evidence and review email authentication.

3.1 Universe card

The selected set is a working portfolio of important organisations, not a published league table of Japan's largest companies. One primary domain represents each entry. Selection reflects public-service responsibilities or a major role in the sector. [S3]

Item	Scope
Population	250 selected primary domains in ten sector groups
Sector size	25 entries in each group
Selection	Purposive public bodies, financial institutions, infrastructure operators and major service, industry and research organisations
Unit	A selected organisation entry represented by a primary domain
Exposure snapshot	22 November 2026; 250 selected domains assessed
Time scope	Device and credential records are cumulative; current listings describe the snapshot
Context windows	Mentions: 23 November 2025–22 November 2026; similar-domain observations: 19 October 2026–18 November 2026
Representativeness	The set does not estimate national exposure prevalence

The domains are analytical reference points. A primary domain does not establish every subsidiary, customer service, hosted application or independent legal entity within a group. Corporate restructuring, shared infrastructure and separate customer brands can change the relevant response boundary.

The sample also differs from the public incident register. An organisation can appear in an official incident notice without being selected here. A selected organisation can have no relevant public incident disclosure. Neither fact establishes the presence or absence of an intrusion.

3.2 Exposure signals by sector

85 of 250 organisations had a credential listed for sale when checked. The snapshot also contains device associations for 209 domains and historical credential records for 241. These populations overlap. [S3]

Every sector contains 25 selected entries. The table shows observed signal counts and their denominators. A current listing is an advertisement, not a completed sale, tested credential or confirmed intrusion.

Current credential listings concern 85 of the 250 selected organisations

	Current listing	Device associations	Employee devices	Credential records	Documents
Public administration	13/25	21/25	16/25	24/25	14/25
Banking	12/25	22/25	10/25	25/25	13/25
Insurance and capital markets	6/25	24/25	14/25	23/25	17/25
Universities and research	14/25	25/25	22/25	25/25	14/25
Health and life sciences	2/25	14/25	9/25	25/25	16/25
Industrial manufacturing	4/25	22/25	17/25	25/25	17/25
Technology and communications	17/25	24/25	21/25	24/25	23/25
Energy and utilities	4/25	20/25	12/25	25/25	17/25
Transport and logistics	8/25	22/25	12/25	23/25	11/25
Retail trade and services	5/25	15/25	11/25	22/25	12/25

Current credential listings by sector (coral). Cells show organisations with the signal / selected organisations; categories overlap. Source: selected Japan organisation exposure observations, 22 November 2026 [S3]. 250 selected organisations; associations can overlap and include historical material. Not current intrusions or national prevalence.

Sector	Domains	Current listings	Listing history (period unspecified)	Employee-device signals	Document signals
Public administration	25	13	13	16	14
Banking	25	12	12	10	13
Insurance and capital markets	25	6	6	14	17

Sector	Domains	Current listings	Listing history (period unspecified)	Employee-device signals	Document signals
Universities and research	25	14	14	22	14
Health and life sciences	25	2	2	9	16
Industrial manufacturing	25	4	4	17	17
Technology and communications	25	17	16	21	23
Energy and utilities	25	4	4	12	17
Transport and logistics	25	8	8	12	11
Retail trade and services	25	5	5	11	12
Total	250	85	84	144	154

The period and overlap with current listings are unspecified for the 84-domain listing-history measure. It cannot be read as an inclusive all-time total or a count excluding current listings. The two figures do not establish a change over time. [S3]

Employee-device associations concern 144 domains, and document associations concern 154. A document can be public, repeated or unrelated to a security incident; validate its content and intended audience. [S3]

Similar-domain observations concern 223 selected domains in the 19 October 2026–18 November 2026 window. Annual chat mentions concern 46, and web mentions concern 37. Similarity and discussion do not establish impersonation or unauthorised access. Validate ownership and actual use before alleging abuse. [S3]

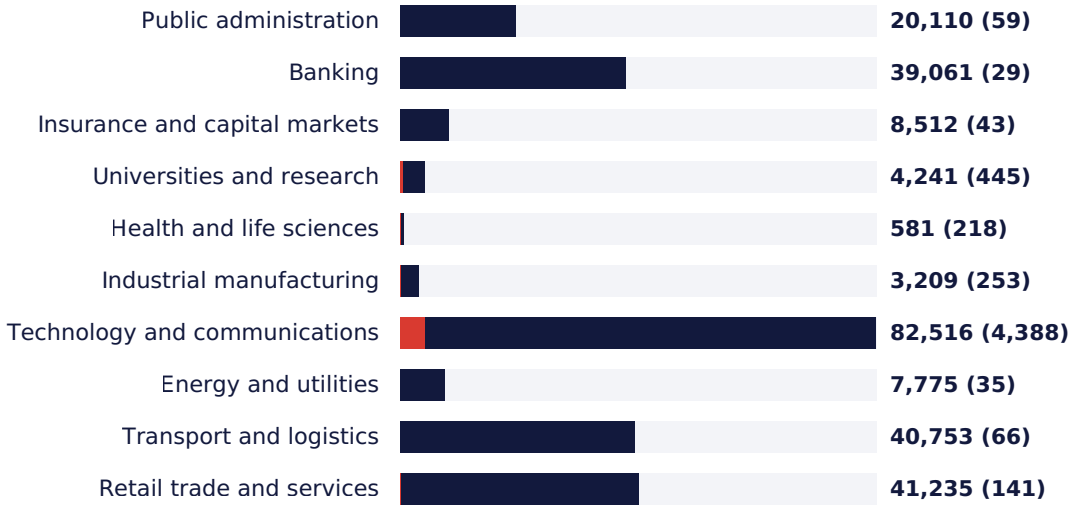
3.3 Device and credential populations

The selected portfolio contains at least 247,993 device associations, including 5,677 employee-device associations. It contains 17,488,907 historical credential-record associations and 1,025 document associations. These are separate populations and can overlap across domains. [S3]

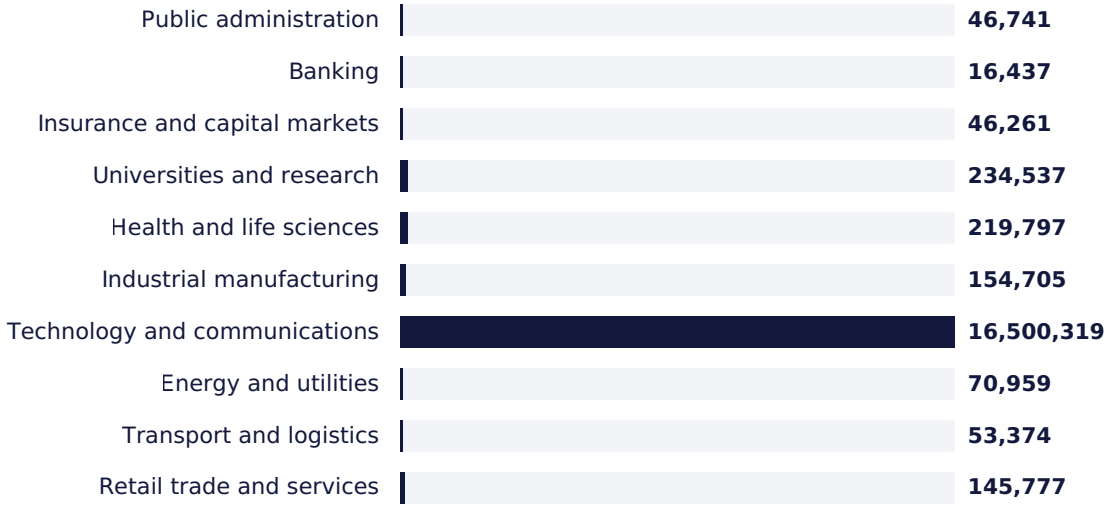
Technology and communications has the largest device and credential association totals



Device associations, at least (employee associations in parentheses)



Historical credential-record associations (separate scale)



Source: selected Japan organisation exposure observations, 22 November 2026 [S3]. 250 selected organisations; associations can overlap and include historical material. Not current intrusions or national prevalence.

Sector	Devices, at least	Employee devices	Credential records	Documents
Public administration	20,110	59	46,741	187
Banking	39,061	29	16,437	44
Insurance and capital markets	8,512	43	46,261	38
Universities and research	4,241	445	234,537	33
Health and life sciences	581	218	219,797	50
Industrial manufacturing	3,209	253	154,705	78

Sector	Devices, at least	Employee devices	Credential records	Documents
Technology and communications	82,516	4,388	16,500,319	351
Energy and utilities	7,775	35	70,959	40
Transport and logistics	40,753	66	53,374	31
Retail trade and services	41,235	141	145,777	173
Total	247,993	5,677	17,488,907	1,025

Technology and communications accounts for 16,500,319 credential-record associations, or 94.3% of the portfolio total. Its device total is at least 82,516. These concentrations describe the observed records, not a sector compromise rate. [S3]

Employee-device associations are included within the device view and must not be added to it. The remaining 242,316 associations are not labelled as employee-associated; this does not establish who owns those devices.

Reading exposure signals precisely

The following distinctions should accompany an organisation-level alert and its aggregate context.

Signal	Proposition supported	Question still requiring validation
Credential offered for sale	A monitored offer associates a credential with a domain	Does an active owned account exist, and what can it access?
Device association	Captured information associates a device with a service or domain	Who owns the device, when was information captured and is access still usable?
Historical credential record	An account reference appears in retained historical material	Is it current, reused or already remediated?
Document reference	A document mentions an organisation or domain	Is it sensitive, authentic and intentionally public?
Lookalike-domain candidate	A domain resembles a protected brand	Is it related, legitimate or being used for deception?
Underground mention	A post refers to the organisation	Is it a specific claim, ordinary discussion or a repeated advertisement?

One person can have several accounts, appear in several historical sources and use multiple organisations' services. Device and credential associations can overlap across those services. Adding them together does not produce a count of unique people or affected organisations.

Employee-associated material should receive prompt attention because a validated employee account may have internal privileges. The label alone does not establish a managed corporate device, an active infection or an intrusion into the employer's environment. Universities and shared-service organisations can have particularly varied account populations.

3.4 Current credential offers

A current offer is a reason to investigate the relevant account. It is not evidence that a sale occurred, that the credential works or that the organisation's own systems were the source. The response should establish ownership and scope before disruptive containment.

Begin with the exact owned identity, if available through an authorised alert. Check whether the account still exists, its last legitimate use, its privileges and any previous reset or revocation. Review the relevant session, application and remote-access activity. Preserve the result even when the account is obsolete.

Escalate when an active privileged account, suspicious session or unauthorised action is confirmed. Containment may include revoking sessions, rotating an integration secret or restricting an access path. The appropriate action depends on the validated evidence and business impact.

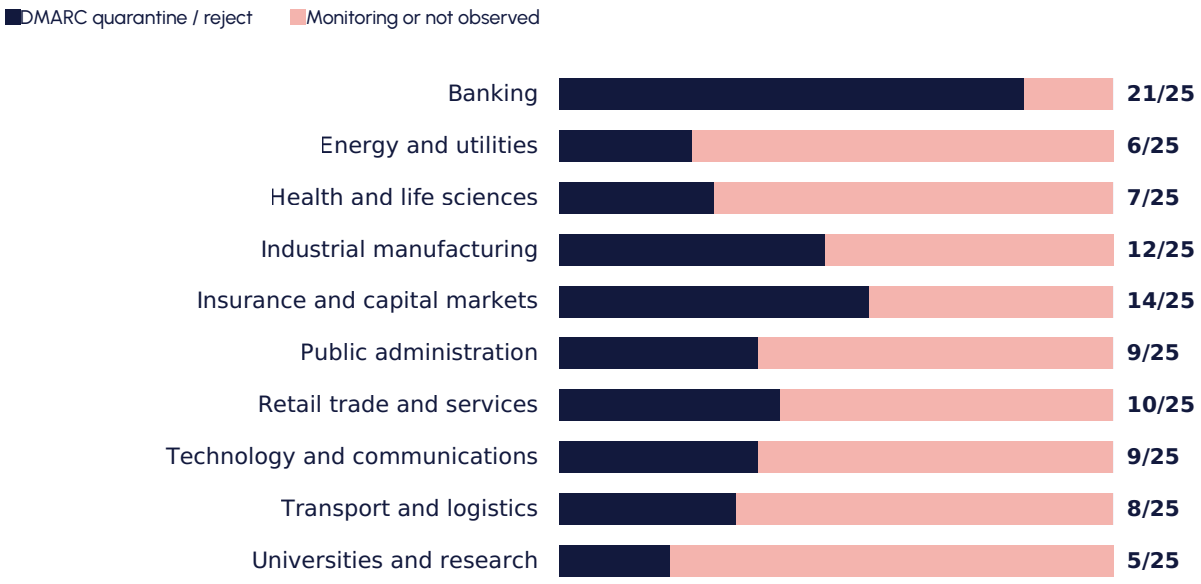
Do not use the absence of a visible offer to close an unrelated investigation. Public and monitored markets cover only part of the activity. Material can be private, mislabelled, historical or never advertised.

3.5 Public email and web observations

The DNS-only dataset contains interpretable responses for all 250 selected domains. It records 101 domains with DMARC quarantine or reject policies, or 40.4% of that assessed population. The other 149 have a monitoring policy or no observed policy. [S4]

Figure c05 describes the assessed domains. It is not a phishing-delivery or fraud-success measure.

101 of 250 assessed domains publish a DMARC enforcement policy



Source: public DNS policy observations, 250 assessed domains, 22 November 2026 [S4]. A published policy does not establish receiver compliance or effective phishing prevention.

Sector	Assessed domains	Quarantine or reject	Monitoring or missing
Banking	25	21	4
Energy and utilities	25	6	19
Health and life sciences	25	7	18
Industrial manufacturing	25	12	13
Insurance and capital markets	25	14	11
Public administration	25	9	16
Retail trade and services	25	10	15
Technology and communications	25	9	16
Transport and logistics	25	8	17
Universities and research	25	5	20
Total	250	101	149

Across the assessed set, 58 policies request reject and 43 request quarantine. Another 109 request monitoring and 40 have no observed policy. These are policy observations, not proof of effective delivery controls. [S4]

The edition has no complete TLS, homepage-header or combined hygiene-index dataset. No such prevalence or index is inferred. DNS observations do not substitute for those missing results.

A mail policy describes how receiving systems are asked to handle authentication results. It does not establish that every receiver complies or that all legitimate senders are correctly configured. Review the sending inventory before changing enforcement, then monitor legitimate delivery.

A certificate or homepage observation applies to the service checked. It does not describe every application or guarantee secure application behaviour. A missing observation remains unknown. It should not be counted as either a secure result or a confirmed weakness.

3.6 The national headline and its decision boundary

The national Atlas headline is 51/100 (B). The figure supports prioritisation; it is not a breach percentage, incident probability or certification of control effectiveness. [S3]

Only the national headline is published. Sector tables show anonymous signal counts, without sector or organisation ratings. The rating belongs to the dated snapshot; cumulative historical records do not establish that every signal first appeared during 2026.

Historical associations remain separate from current offers and from the incident window. Public disclosures, criminal advertisements and passive controls answer different questions. Remediation of a specific account requires organisation-side evidence, even when historical observations persist.

The useful decision is still concrete. Maintain a route from an external alert to the responsible identity, application or business owner. Record whether the alert was validated, which service was involved and what action resolved the evidence. A national headline cannot replace that organisation-specific work.

KEY TAKEAWAYS

01

The 250-entry set defines scope and does not estimate Japanese national prevalence.

02

Device, credential, document and mention populations require separate interpretation.

03

Validate the owned identity and access path before choosing containment.

CHAPTER 04

Underground activity and what the posts establish

04

THIS CHAPTER ANSWERS

Which offers deserve investigation, and which conclusions would exceed the evidence?

6

detailed claim cases, each with a separate evidence boundary

4.1 Universe card 24

4.2 The retained view and its limits 25

4.3 Recent activity: 8–22 November 27

4.4 Detailed claim cases 29

4.5 Demand, old information and international offers 35

4.6 Prices, file sizes and actor relationships 37

4.7 From an alert to a proportionate action 38

CHAPTER 04

Underground activity and what the posts establish

IN SHORT

Retained underground posts show demand for Japanese information, specific data offers, an alleged bank vulnerability and recirculated material. They do not establish a national incident total. One recent offer describes property data while listing lawyer-registration fields. Another global travel offer does not quantify its Japanese share. Separate possession from demand, current access from an advertised capability, and a new post from an old incident. Validate relevant alerts against owned information and access records.

4.1 Universe card

The source population is material retained by Odin by Brandefense from underground posts. The main window is based on posting time, 1 January–22 November 2026. A post date is not an intrusion, acquisition or execution date. [S1]

Item	Scope
Evidence	Retained forum, messaging and related underground posts
Country relationship	Japan-associated discussion, offers or demand; some posts mention several places
Time	Posting time within the requested window
Country-associated count	1,073,099 posts in the source view; not confirmed targeting
Retained population	17,529 distinct posts in the report's narrative corpus
Meaning	Observed messages and assertions, not confirmed incidents or unique victims
Limits	Uneven source visibility; private and unpublished activity remains outside the view

The retained population is not a census of Japanese underground activity. Its volume cannot establish an annual attack rate. Repeated advertising, international offers and ordinary discussion can produce many messages without a new Japanese intrusion.

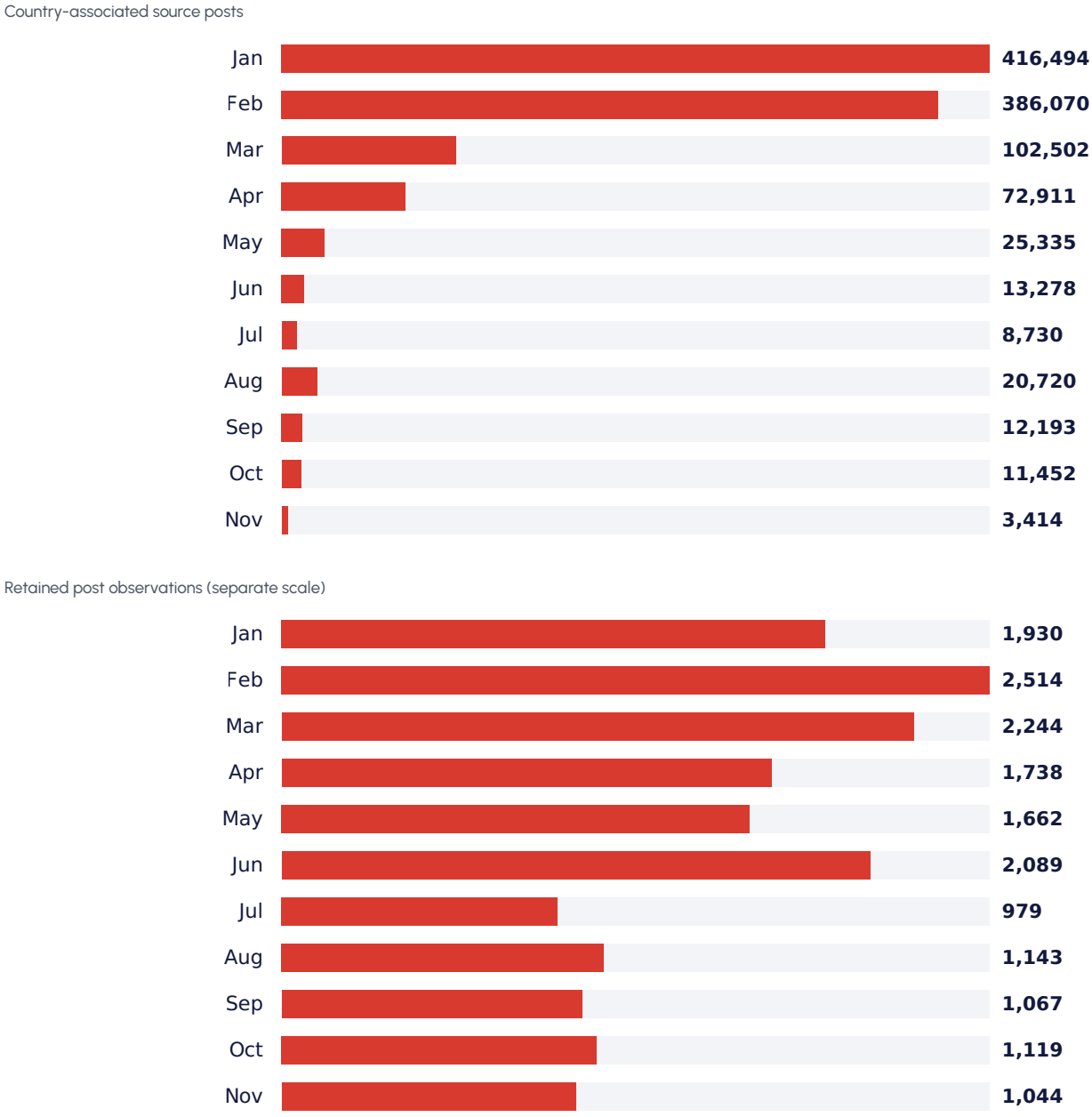
The public case cards preserve short authentic excerpts and state what remains unresolved. Sensitive identifiers and contact details are withheld. Claims of file size, row count, price or access remain attributed to the post unless separately confirmed.

4.2 The retained view and its limits

The retained view contains 17,529 posts. This is the retained population, not an annual total for Japan. [S1]

The country-associated source view contains 1,073,099 posts. Country-tagged counts and the retained narrative corpus are different coverage views. Neither is assumed to be a complete subset of the other. One post can discuss several places. [S1]

Country-associated post volume is uneven and does not measure attack frequency



Source: Odin by Brandefense, Japan-related post observations, 1 January–22 November 2026; closing day partial. Country-tagged and retained posts are separate populations, not attack counts [S1].

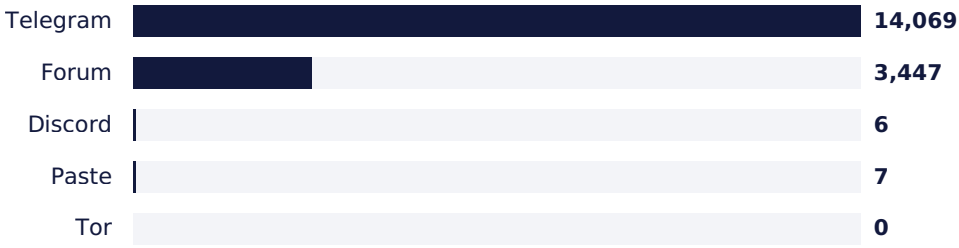
Figure c01 shows monthly country-associated counts. The following platform and language tables describe the retained narrative corpus. Changes in source volume are not interpreted as changes in national threat frequency.

Source type	Posts	Share of retained posts
telegram	14,069	80.3%
forum	3,447	19.7%
paste	7	0.0%
discord	6	0.0%

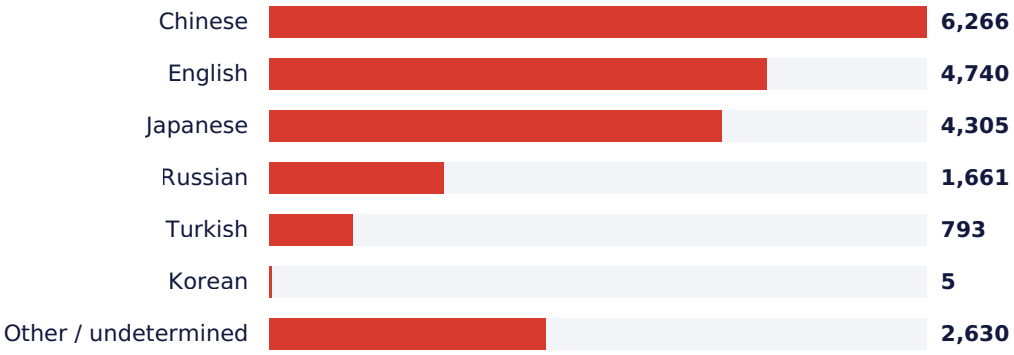
The table shows clearly named language categories and other/undetermined labels. The latter includes unknown, geographic and unresolved labels. Counts represent label occurrences; the other/undetermined total does not represent unique posts. Shares use 17,529 retained posts as the denominator, and labels can overlap. [S1]

Language and platform visibility do not identify nationality or incident counts

Retained posts by platform



Language associations (can overlap; separate scale)



Source: Odin by Brandefense, Japan-related post observations, 1 January–22 November 2026; closing day partial. Country-tagged and retained posts are separate populations, not attack counts [S1].

Language category	Label occurrences	Share of retained posts
Chinese	6,266	35.7%
English	4,740	27.0%
Japanese	4,305	24.6%

Language category	Label occurrences	Share of retained posts
Russian	1,661	9.5%
Turkish	793	4.5%
Korean	5	0.0%
Other/undetermined labels	2,630	15.0%

Do not infer actor nationality from a post's language. A Japanese-language field list can be copied from a dataset, while a Chinese or English advertisement can discuss Japan among many markets. Language describes the retained message and may not identify its author or intended buyer.

The same caution applies to a venue. A forum can carry a specific data offer, a request for an old upload or a global sales list. It is the assertion and supporting evidence that determine the response, not the platform name alone.

4.3 Recent activity: 8–22 November

The closing-period examples below illustrate two distinct propositions. A buyer solicits material on 18 November. A seller advertises a dataset with an inconsistent sector description on 16 November. Neither post establishes a newly affected Japanese organisation. [S1]

Date	Observed assertion	Evidence boundary	Card
2026-11-18	Demand for high-value government and technology information, including Japan	Demand does not establish possession or delivery	B01
2026-11-16	An offer of 48,000 records with a property description and lawyer-related schema	Authenticity, provenance and even sector identity remain unresolved	B02
2026-11-15	Travel-loyalty themed offer advertising 48,000,000 records for $550	Claimed rows, ownership, authenticity and current access are unverified	B12
2026-11-14	Transport-themed offer advertising approximately 19,210,000 records for $400	The declared total is not a validated Japanese affected-person count	B11

The specific mismatch matters more than the advertised volume. A label can be inaccurate without proving that the entire offer is fabricated. Equally, a detailed schema does not authenticate a file. A response team should record the contradiction and seek owned evidence before naming an affected service.

Evidence card B01 18 Nov 2026

[alias withheld] Forum Forum English

ORIGINAL

I am looking to obtain high-value intelligence and data

Note. Japan is one of several sought countries; this is demand rather than a data-holding claim.

Held
The author seeks government, military, semiconductor and other high-value material, with Japan one of several countries.

Not established
This is a solicitation. No possession, seller relationship, delivery or Japanese compromise is demonstrated.

Evidence card B02 16 Nov 2026

[alias withheld] Forum Forum Japanese

ORIGINAL

弁護士登録番号 氏名 氏名カナ 氏名ローマ字 生年月日

TRANSLATION

Lawyer registration number; name; name in kana; name in Latin letters; date of birth.

Note. The contradiction is the finding; no property-sector incident is established.

Held
The 16 November offer advertises 48,000 records under a property-related description, while its Japanese schema lists lawyer registration, bar membership and law-office fields.

Not established
The corpus does not validate the file, row count, origin, data freshness, or whether the stated property sector is correct.

Evidence card B11 14 Nov 2026

[alias withheld] Forum Forum English

ORIGINAL

records: 19.21M

Note. Separate from the 16 November 48,000-record offer. The total is advertised, not independently confirmed.

Held
The author advertises a dataset attributed to a Japanese transport operator, with 19.21M records at $400.

Not established
No file authentication, unique-person count, date of original compromise, successful sale, or continuing access was established. Source-sample identities and values are withheld.

Evidence card B12 15 Nov 2026

[alias withheld] Forum Forum English

ORIGINAL

Records - 48M

Note. Separate from the 16 November 48,000-record offer. The total is advertised, not independently confirmed.

Held
The author advertises a dataset attributed to a Japanese travel loyalty programme, with 48M records at $550.

Not established
No file authentication, unique-person count, date of original compromise, successful sale, or continuing access was established. Source-sample identities and values are withheld.

The two transport-themed offers add a customer-safety question. If a relevant owned match is corroborated, review booking, loyalty and recovery workflows for impersonation using genuine-looking information. The advertisements alone do not justify a national affected-person total.

Chapter 5 treats official November disclosures separately. The timing of a post and a public notice does not establish that they describe the same information. No matching file, account or independently supported connection is established between these examples and those disclosures.

4.4 Detailed claim cases

Each case distinguishes the observed assertion, chronology, established proposition, alternatives and a proportionate response. None is presented as a verified intrusion. The cases are not added to police reports, ransomware listings or public-disclosure populations.

CASE A

A

The title and schema point to different sectors

Evidence card B02 | 16 Nov 2026 | Forum | unresolved / professional services

Claim unverified

CLAIM	A 16 November forum offer advertises 48,000 records under a property-related description. Its Japanese schema instead includes lawyer registration, bar membership and law-office fields.
CHRONOLOGY	The date establishes when this offer appeared in the retained material. It does not establish when information was collected or whether an earlier offer existed elsewhere.
ESTABLISHED	The post contains an internal inconsistency between its description and declared fields. That supports uncertainty about its identity, rather than a confirmed property-sector incident.
ALTERNATIVES	A mistaken label, recycled advertising, combined information or a genuine file described inaccurately could explain the mismatch. The post does not resolve those possibilities.
LIMITS	File authenticity, the claimed rows, provenance and freshness remain unverified. A registration field can also refer to information already available through a legitimate directory.
RESPONSE	A relevant data owner should compare the declared fields with authorised exports and public information. Investigate a credible owned match before choosing containment or an incident notice.

Bottom line

Compare the declared schema with authorised exports and public information before identifying an affected service.

CASE B

B

A staged disclosure narrative uses pressure and uncertain counts

Claim unverified

Evidence card B03 | 6 Nov 2026 | Forum | personal services

CLAIM	A 6 November post says a disclosure site and a first wave concerning 50 practitioners are ready. It promises further practitioner and customer material.
CHRONOLOGY	The text refers to an earlier report in its own narrative. That reference is not independent evidence of the earlier material, an intrusion sequence or completed publication.
ESTABLISHED	An account made an extortion-style disclosure assertion. The post alone does not establish possession, the people represented, a completed release or a payment.
ALTERNATIVES	It could reflect genuine information, copied material, recycled pressure or an unsupported demand. References to earlier reports do not identify which alternative is correct.
LIMITS	The scope, acquisition route and underlying identities were not independently established. A claim that all users are covered remains the poster's assertion.
RESPONSE	The service owner should preserve a relevant alert, verify any authorised information match and coordinate customer-protection planning. Communications should distinguish the demand from the facts established.

Bottom line

Preserve a relevant alert, verify an owned information match and coordinate customer protection on the facts established.

Evidence card B03 6 Nov 2026

[alias withheld] Forum Forum English

ORIGINAL

full disclosure of all users since September 2026 is ready

Note. An unverified extortion narrative, not an independently confirmed breach.

Held

The author claims a new disclosure site, a first wave covering 50 practitioners, and further release of practitioner and customer records.

Not established

The author's possession, counts, disclosure completion, identities, and compromise mechanism were not independently verified. A settlement demand does not prove payment.

C

CASE C

A vulnerability offer is not an access sale

Evidence card B04 | 2 Mar 2026 | Forum | banking / finance

Claim unverified

CLAIM	On 2 March, a forum post offers an unspecified vulnerability affecting a Japanese bank for $5,000. Its wording says the buyer would need to exploit it.
CHRONOLOGY	The observed event is an advertisement on that date. No discovery date, affected software version or earlier exploitation history is supplied in the retained assertion.
ESTABLISHED	The account advertised a purported capability. The wording does not establish that it held an active account, controlled a system or had already used the alleged issue.
ALTERNATIVES	A real vulnerability, exaggerated weakness, copied offer or fabricated capability remains possible. The price does not authenticate the technical claim.
LIMITS	No technical proof, confirmed affected product or bank intrusion is established. The seller's financial description of the target is also unverified.
RESPONSE	A bank receiving a relevant authorised alert should route it to its application-security owner. Review owned evidence and test within authorised scope before assigning severity or taking disruptive action.

Bottom line

Route a relevant alert to application security and validate the alleged weakness within authorised scope.

Evidence card B04 — 2 Mar 2026

[alias withheld] | Forum | Forum | English

ORIGINAL

Selling a critical vulnerability on a bank from Japan

Note. Offer of a purported capability; no access or bank breach is established.

Held

The post offers an unspecified bank vulnerability for $5,000 and says the buyer must exploit it.

Not established

No technical proof, affected product, access, exploitation, or bank compromise is demonstrated. The claimed bank profit is not independently checked.

CASE D

D

Registration records could enable believable impersonation

Evidence card B05 | 3 Feb 2026 | Forum | leisure / events

Claim unverified

CLAIM	A 3 February offer advertises 457,000 sports-event registration and attendance records. Its declared fields include event identifiers, names, contact information, birth dates and entry status.
CHRONOLOGY	The post date establishes advertising during the report window. It does not establish a current registration-system intrusion or the period covered by the records.
ESTABLISHED	The advertised field set describes a plausible event-registration workflow. It does not authenticate the contents or establish that the rows represent distinct people.
ALTERNATIVES	A genuine export, older registration information, aggregation or a misleading offer could produce the same description. A detailed field list cannot settle provenance.
LIMITS	The full information, seller's acquisition role, claimed count and freshness remain unverified. No affected organisation is named here.
RESPONSE	Event and service owners should examine a credible owned match against export records and supplier access. If disclosure is corroborated, consider impersonation that quotes real event or attendance information.

Bottom line

Review owned exports and supplier access if the claimed registration information can be corroborated.

Evidence card B05 — 3 Feb 2026

[alias withheld] | Forum | Forum | English

ORIGINAL

Data contents: id, registration_date, event_id, event_name, user_id, first_name, last_name, email, phone, birthday, gender, postal_code, address, entry_category, status, attendance_flag.

Note. Specific data-sale claim; show declared fields and claimed rows without turning them into a verified impact count.

Held

The seller advertises 457,000 sports-event registration and attendance records with 16 listed fields, including Japanese contact details.

Not established

The content was not authenticated. No distinct people count, source compromise date, seller authorship, or complete file is established.

CASE E

E

Claimed redistribution does not identify the original intruder

Claim unverified

Evidence card B06 | 22 Aug 2026 | Forum | technology / software

CLAIM	An account on 22 August claims to release 74 GB of source code and other material from a Japanese software business. It credits other aliases for the alleged original acquisition.
CHRONOLOGY	The post describes redistribution. Its date does not establish when any original access occurred or whether the credited accounts participated in it.
ESTABLISHED	The account asserted that it was sharing material and attributed an earlier role to others. That is a claimed association, not a verified transfer or common operator.
ALTERNATIVES	The material could be authentic, partial, previously public, historical or misrepresented. An alias credit could be accurate or promotional.
LIMITS	Source-code authenticity, completeness, acquisition date and customer consequences remain unresolved. No product vulnerability or exposed integration is established from the description alone.
RESPONSE	A relevant owner should identify an authorised artifact match and assess its actual sensitivity. Review credentials or integrations only where the validated material makes them relevant.

Bottom line

Identify a genuine owned artifact before assessing sensitive code, credentials or integrations.

Evidence card B06 — 22 Aug 2026

[alias withheld] | Forum | Forum | English

ORIGINAL

74GB of source codes, and other stuff

Note. Alleged redistribution rather than proof that the posting account conducted the intrusion.

Held

The author claims to release 74 GB of source code and other material from a Japanese software business, crediting other aliases for the alleged original acquisition.

Not established

No authenticated source code, completeness, compromise date, original actor relationship, or customer impact is established.

CASE F

F

Insurance rows remain an advertised population

Evidence card B09 | 13 May 2026 | Forum | insurance

Claim unverified

CLAIM	A 13 May forum offer advertises 10,000,000 Japanese insurance records in CSV form. Its description lists identity, contact and policy-related fields.
CHRONOLOGY	The offer predates some later public disclosures in this report. No file or independently supported relationship connects them, so it is not attributed to those incidents.
ESTABLISHED	The post advertises an insurance-themed dataset with a claimed count and field categories. It does not establish an insurer's intrusion or the number of affected people.
ALTERNATIVES	Historical information, aggregated lead data, an inaccurately labelled file or a new disclosure could explain the offer. The retained text does not distinguish them.
LIMITS	The contents, rows, uniqueness, provenance and acquisition date were not independently established. CSV describes a format, not an authenticity test.
RESPONSE	An insurer should investigate a credible owned match and review policy-change and recovery workflows. Corroborate disclosure before choosing customer notices or population-wide account actions.

Bottom line

Validate any owned information match and review policy-change, recovery and customer-notification decisions.

Evidence card B09 — 13 May 2026

[alias withheld] | Forum | Forum | English

ORIGINAL

Type: Japan Insurance Format: CSV Records: 10M

Note. Specific Japanese sale claim; rows must remain an advertised count.

Held

The seller advertises a Japanese insurance dataset with 10 million CSV records and lists identity, contact and policy-related fields.

Not established

The dataset, size, provenance, date, uniqueness and any insurer compromise are not independently established.

4.5 Demand, old information and international offers

The additional cards show why counting posts as incidents fails. They remain useful to defenders, but each supports a narrower proposition. [S1]

Observed post	What it establishes	What it does not establish	Card
January reupload stating an original 22 February 2024 acquisition and 18,653,758 lines	Recirculation was advertised during 2026	A new 2026 intrusion or current password validity	B07
November hotel-reservation offer claiming 16,000,000 global rows, including Japanese guest origins	An international offer mentions Japan	The Japanese share or a Japanese service-provider intrusion	B08
January Chinese-language solicitation for government information from several places	Stated buying interest	Possession, successful acquisition or a Japanese government intrusion	B10

Evidence card B07 — 13 Jan 2026

[alias withheld] | Forum | Forum | English

ORIGINAL

contains 18,653,758 lines

Note. Recirculation observed in 2026; not a new 2026 incident.

Held

The January 2026 post describes itself as a reupload and states that the original acquisition occurred on 22 February 2024.

Not established

The 2026 post date does not establish a 2026 intrusion, new victims, unique people, or password validity.

Evidence card B08 — 5 Nov 2026

[alias withheld] | Forum | Forum | English

ORIGINAL

database consisting of 16 million rows

Note. Global, multi-country offer; neither the 16 million records nor the hotels are attributable to Japan.

Held

The seller advertises a hotel-reservation dataset, alleges ongoing new records, and lists Japan among several customer-origin countries.

Not established

The 16 million figure is a global claim. The Japanese share, affected hotels, data authenticity and alleged continuing access are unverified.

Evidence card B10 — 1 Jan 2026

[alias withheld] | Forum | Forum | Chinese

ORIGINAL

政府的内部情报，包括政策、报告、机密文件、军事情报

TRANSLATION

Internal government intelligence, including policies, reports, classified documents and military intelligence.

Note. Multi-country demand, not an offer to sell government data.

Held

The Chinese-language advertisement seeks internal government, policy, classified and military information from several countries, including Japan.

Not established

The post establishes a stated buying interest only. It does not establish possession, a successful acquisition or a Japanese government compromise.

Old information can still support identity fraud if genuine. Its continued value does not make its acquisition recent. A response team should record both the observed advertising date and the claimed underlying period, keeping any unverified age statement attributed to the poster.

International offers require a country boundary. A Japanese customer, a Japanese brand overseas and a system operated in Japan are different relationships. A global row total should not be assigned to Japan merely because the advertisement lists it among many guest or customer origins.

Demand also has a separate meaning. A buyer's interest can justify attention to sensitive information and insider-reporting routes. It does not establish an existing seller, access path, acquisition or successful transaction.

Other sector-specific assertions appear below. Their dates are post dates and their contents remain unverified. They are not added to a national incident count. [S1]

Date	Advertised theme	Evidence boundary
2026-01-01	Radio or music-service data; 3,016,221 records claimed	No authenticated file or verified disclosure
2026-01-02	Hotel data; approximately 720,000 records claimed	An offer, despite a request-style title
2026-01 to 2026-10	Education-themed data; approximately 98,000 rows	Similar advertising across dates is not a new incident each time
2026-02 to 2026-04	Administration or support data; approximately 468,000 rows	A separate buyer dispute alleges generated identifiers; neither assertion authenticates the data
2026-04-02	Employee or payroll material; approximately 672,000 records	Claimed contents and affected population remain unverified
2026-04-02 to 2026-04-22	User or contact material; approximately 437,000 records	Repeated descriptions do not establish distinct incidents
2026-04-07	Housing-search material; approximately 2,400,000 records	No verified origin, uniqueness or current access
2026-04-07	Communications-service accounts and activity; more than 250 GB claimed	Volume is an assertion, not a person count
2026-04-18	Retail or order information; approximately 1,700,000 records	No authenticated dataset or confirmed current intrusion
2026-09-17	Pharmaceutical-business files; approximately 4 TB claimed	A referenced owner statement is not independently established by the post
2026-09-18	Older leisure-related material; 2,137,062 lines and a stated 2022 leak date	Redistribution observed in 2026; original date and file remain assertions
2026-01-11	Sale dispute over approximately 850,000 Japanese phone entries	A buyer alleges false information; the dispute does not resolve authenticity

4.6 Prices, file sizes and actor relationships

The $5,000 vulnerability price is an advertised asking price. The 74 GB code description is an asserted volume. Neither shows a completed exchange, commercial value or verified possession. The report therefore does not infer market revenue from these offers. [S1]

Similar wording can support a finding that advertisements resemble one another. It cannot establish identical files, original authorship or a transfer between accounts. An alias credited in a post also remains a claimed relationship until a concrete shared element supports a narrower conclusion.

For response teams, the first question is whether information or access belongs to the organisation. The next is whether it remains relevant and usable. The identity owner, application owner and data custodian may need different evidence before reaching those decisions.

4.7 From an alert to a proportionate action

Use an explicit decision record for a relevant alert. Preserve the assertion, the observed date and the claimed scope. Add the owned evidence used to validate or reject it, the decision owner and the next review point.

If an active account is confirmed, inspect its privileges and relevant activity. If an information match is corroborated, assess affected categories and protective steps. If the alert describes old or unrelated material, retain the reason for closing it without turning uncertainty into a declaration of safety.

The same discipline applies to public communications. Describe an advertisement as an advertisement, a request as a request and an official disclosure within its stated scope. A cautious label in the appendix cannot repair an overconfident headline.

KEY TAKEAWAYS

01

The six cases establish observed assertions and do not count verified intrusions.

02

Keep demand, redistribution, international scope and claimed access separate.

03

Use an owned evidence match to choose identity, data-protection or service-response actions.

CHAPTER 05

Public incident accounts and sector decisions

THIS CHAPTER ANSWERS

Which incidents change operating decisions?

2026

Public disclosures and campaign research

5.1 Public incident accounts 41
5.2 Additional public accounts 54
5.3 Sector decisions 58
5.4 Anonymous incidents and the wider leak wave 58
5.5 Further original-notice accounts 59

CHAPTER 05

Public incident accounts and sector decisions

IN SHORT

The cases separate service interruption, confirmed extraction and possible exposure. November notices show why sensitive test data, supplier-held records and stored credentials require different responses. Later revisions can change scope without establishing another attack. Finance needs session and onboarding controls; manufacturers need tested recovery; customer platforms need export restrictions and communication alternatives. Verify the affected fields and dependencies before choosing containment or customer guidance.

Service restoration and data-loss decisions require separate evidence. A restored application can leave unresolved questions about copied records or credentials. Conversely, a large possible population does not establish extraction from every account. The accounts below preserve those distinctions and identify the latest substantive revisions.

Sector	Decision raised by the cases	Priority action
Banking, securities and insurance	Sensitive data can persist in test, query and onboarding environments	Minimise retained data, restrict exports and revoke active sessions where appropriate
Telecom, hosting and digital services	One supplier's controls can affect many downstream services	Map tenant scope, shared administration and alternative customer communication
Manufacturing and research	Encryption and exposed credentials create different recovery boundaries	Test restoration and investigate access to connected environments
Healthcare and education	Supporting systems and old supplier copies can contain sensitive histories	Review peripheral systems, contractor access and obsolete records
Transport, retail and food services	Identity images, purchase histories and payment pages create different risks	Tailor retention and customer guidance to the actual data category

5.1 Public incident accounts

G

CASE G

RIKEN: external credentials widened the response

Research

Official update

ACCOUNT	RIKEN reported unauthorized access to the computing environment supporting Fugaku. Its November 20 update materially expanded the response beyond the information available when national reporting began. [S7] [S6]
CHRONOLOGY	Suspicious traffic appeared on November 12, intrusion was confirmed on November 13, and services stopped on November 14. The first notice was November 16; the detailed revision followed November 20. [S6]
ESTABLISHED	The revision identified access traces involving 4,222 users' information and collection or movement of 430 external-system credentials, including private keys. Among these, 233 lacked passphrases and 197 had them. [S6]
LIMITS	Some credentials showed external connection traces, while wider misuse remained unestablished. Concrete evidence of research-result extraction had not been found. Credential movement and successful access to every external system are different outcomes. [S6]
RESPONSE	Defenders should replace affected credentials, examine authentication at connected institutions, and validate key use before restoring trust. A research platform's incident response must include systems reachable through its users' stored secrets.

Bottom line

Revoke research credentials showing traces of collection or movement and review authentication in every connected environment.

H

CASE H

IDC Frontier: encryption disrupted shared cloud capacity

Cloud services

Ransomware confirmed

ACCOUNT	IDC Frontier confirmed a ransomware incident affecting customer virtual machines in IDCF Cloud. Contemporary reporting described disruption across corporate and municipal customers, illustrating the operational reach of a shared infrastructure provider. [S9]

CHRONOLOGY	The outage began around 03:40 Japan time on October 7. The provider's October 27 seventh report consolidated investigation findings and subsequent response. Four zones in East Japan Region 1 were affected. [S8]
ESTABLISHED	The provider identified an open-source software weakness in portal authentication as the intrusion route. Attackers encrypted or stopped virtual machines, and the affected service population comprised 495 customer organizations. [S8]
LIMITS	The 495 figure describes affected customer organizations. It is not a count of people or confirmed data-theft victims. The October 27 report did not identify external extraction of customer virtual-machine data. [S8]
RESPONSE	Defenders should test cloud isolation, independent recovery copies and provider outage alternatives together. Procurement teams should require explicit distinctions between control-plane intrusion, guest-system encryption and confirmed extraction when requesting incident updates.

Bottom line

Test recovery outside the affected provider's control plane.

CASE I

PLAID: a customer platform faced an extended interruption

Digital services

Official findings

ACCOUNT	PLAID's KARTE incident affected a customer engagement platform used by multiple organizations. Its November 20 findings and restart outlook made the supplier's interruption an immediate continuity issue for downstream customers. [S11]
CHRONOLOGY	The company dates the attack to November 13, when it stopped all services. It completed its provider-side scope investigation on November 19 and published the consolidated account on November 20. [S10]
ESTABLISHED	A flaw in internal processing exposed a public data-access route. Information and credentials obtained through that route enabled access to the administrative console. The confirmed scope included current and former customer relationships. [S10]
LIMITS	The provider separately reported 79,249 account-email records and 45,816 sales or support contact records. These categories do not establish a single total of downstream affected people or prove identical fields across customers. [S10]

RESPONSE	The published restart target was mid-January 2027. Defenders should prepare alternate customer communications and remove unnecessary historical data from engagement platforms. Restart schedules need business-owner review alongside technical remediation and tenant-specific notification.

Bottom line

Plan customer communications around a prolonged supplier interruption.

J

CASE J

A payments provider: recovery required separate decisions

Finance

Official disclosure

ACCOUNT	A payments provider confirmed unauthorized access involving customer information. [S12] [S13]
SCOPE	The provider distinguished affected environments from those eligible for resumption after checks. [S12]
ESTABLISHED	The disclosed scope concerned personal information. Record populations do not necessarily identify unique people. [S12]
LIMITS	Partial resumption did not establish full recovery or closure of every investigation. [S12]
RESPONSE	Use customer-specific evidence to govern restart decisions and explain the current service status.

Bottom line

Use customer-specific evidence to govern restart decisions and explain the current service status.

K

CASE K

Nitori: a large possible exposure remained qualified

Retail

Possible exposure

ACCOUNT	Nitori disclosed possible personal-information leakage following unauthorized access to its systems. National business reporting amplified the notice, but the company's qualification remained central to interpreting the announced scale. [S15]
CHRONOLOGY	The company detected the issue on November 6 and published its notice on November 9. It considered unauthorized access during the middle to latter part of October possible. [S14]

ESTABLISHED	The potential scope reached approximately 37.62 million records. This made customer-data retention and the handling of former customer records important questions for organizations reviewing similar retail systems. The notice excluded passwords and card information. [S14]
LIMITS	The figure is a maximum possible record scope. It should not be restated as a confirmed number of stolen records, a count of unique customers or proof of subsequent misuse. [S14]
RESPONSE	Defenders should reconcile retained customer datasets with current business needs and investigate application access across the stated period. Customer messaging should retain the distinction between a possible exposure and established extraction while setting out concrete protective steps.

Bottom line

Preserve the possible-exposure qualifier and reduce unnecessary customer-data retention.

L

CASE L

An education institution: supplier exposure and disruption differed

Official update

Education

ACCOUNT	An education institution reported a supplier-related information leak and disruption of its own systems. [S16]
SCOPE	The investigation treated supplier-held information and the institution's operational systems separately. [S16]
ESTABLISHED	Retained information and privileged access required review across the service relationship. [S16]
LIMITS	The institution had not found concrete evidence of direct personal-information extraction from its own systems. [S16]
RESPONSE	Remove obsolete supplier-held copies and restrict administrative access by task and time.

Bottom line

Remove obsolete supplier-held copies and restrict administrative access by task and time.

CASE M

M Times Car: identity-image findings changed the response

Transport

Revised scope

ACCOUNT	Times Car's incident combined customer-account information with identity-document images. Reporting on the October 23 fifth update highlighted revised image counts, customer assistance and a substantial change in retention practice. [S18]
CHRONOLOGY	Abnormal access was detected on September 25. The September 28 notice described the initial customer scope; the October 23 update replaced the earlier estimate for identity images with more specific findings. [S17]
ESTABLISHED	The latest account scope was approximately 6.6 million. Around 1.46 million encrypted identity-document images showed traces of access and external transmission. A separate image category showed access traces without observed external transmission. [S17]
LIMITS	An image record is not an additional unique person. External transmission of encrypted images did not mean immediate readability, although decryption risk could not be entirely excluded. Access and transmission were reported as separate categories. [S17]
RESPONSE	The operator changed its identity-image retention approach. Defenders should revisit whether verification requires keeping full documents after onboarding, and ensure investigation reports separate account records, encrypted objects, access traces and observed data movement.

Bottom line

Keep identity documents only for the period needed to complete verification.

CASE N

N KDDI: corrected mail-platform figures superseded the first estimate

Telecommunications

Corrected disclosure

ACCOUNT	KDDI's shared internet-provider mail platform incident reached multiple service operators. Subsequent reporting on administrative guidance reinforced the importance of distinguishing the platform's customers from the provider's other consumer services. [S20]

CHRONOLOGY	Unauthorized activity began in May for some affected providers. KDDI detected the issue on June 17, first disclosed it in June, and corrected its July 6 report on July 21. [S19]
ESTABLISHED	The corrected scope identified 12,231,954 users' email addresses and 7,616,173 passwords. The password group belongs within the wider affected population and must not be added as another population of people. [S19] PPC separately confirmed this shared-platform credential disclosure and issued remedial directions. [S83]
LIMITS	The correction superseded a larger early estimate. KDDI stated that specified major consumer services were unaffected. The incident does not justify extending the exposure to every service carrying the same corporate brand. [S19]
RESPONSE	Defenders should coordinate credential replacement across participating providers, check reused passwords and validate which mail platform each account actually uses. Communications teams should replace obsolete numbers consistently across notices, support scripts and downstream customer updates.

Bottom line

Use the corrected scope and coordinate password response across affected providers.

CASE O

Aflac Japan: bulk queries required a separate detection response

Latest official scope

Insurance

ACCOUNT	Aflac Japan disclosed customer-information leakage through its application environment. Wider reporting confirmed the Japanese subsidiary event, while later company updates refined both the activity period and the affected information. [S22]
CHRONOLOGY	The current account dates unauthorized access to June 10–25, with detection on June 25. The first public notice appeared on June 30. The incident FAQ was updated again on November 13. [S21]
ESTABLISHED	The revised scope was approximately 4.4 million customers, including an approximately 220,000-person bank-account subset. The company described inadequate data-query controls and requests that could resemble ordinary use. These findings support attention to bulk-query monitoring. [S21]

LIMITS	Earlier customer and bank-account estimates were superseded. The company excluded several other sensitive fields, including card information and website passwords. Reporting on a separate overseas Aflac incident does not attribute this Japanese event. [S21]
RESPONSE	Defenders should review query authorization and alerts for unusual extraction volume, even when requests use legitimate application functions. Insurance response plans should separately address identity exposure, bank-account information and customer-service impersonation.

Bottom line

Detect abnormal query volume as well as abnormal login behavior.

P

CASE P

Nippon Medical School Musashikosugi Hospital: a nurse-call system carried sensitive information

Ransomware and leak

Healthcare

ACCOUNT	Nippon Medical School Musashikosugi Hospital reported a ransomware incident affecting a nurse-call environment. Initial national coverage used a smaller preliminary patient figure that later hospital findings materially revised. [S24]
CHRONOLOGY	The hospital identified entry through a VPN weakness on January 26 and theft from the nurse-call database on January 29. Disruption was detected on February 9. Its February 27 fifth report updated the investigation. [S23]
ESTABLISHED	The revised potential scope was approximately 130,000 patients and 1,700 staff or students. The hospital confirmed that stolen nurse-call data was subsequently published. The information existed outside the central electronic medical-record environment. [S23]
LIMITS	The initial approximately 10,000-patient figure was obsolete. The hospital reported continued normal care and did not confirm leakage from its electronic medical-record system. A peripheral clinical system can still contain substantial sensitive information. [S23]
RESPONSE	Defenders should inventory data in bedside, communications and facilities systems, then segment remote maintenance access. Clinical continuity exercises should include the loss of supporting systems and the disclosure of data copied into them.

Bottom line

Treat supporting clinical systems as sensitive-data stores during access reviews.

CASE Q

Q Advantest: later notification confirmed extraction

Manufacturing

Ransomware confirmed

ACCOUNT	Advantest's initial ransomware response and later individual notification describe different stages of the same incident. Subsequent reporting made the later confirmation of personal-information theft explicit. [S27]
CHRONOLOGY	The company detected suspicious activity on February 15 and published its initial notice on February 19. An October 6 individual notification filed with California's attorney general supplied more specific findings. [S26] [S25]
ESTABLISHED	The later notice confirmed that information had been extracted during the February event and that the recipient's personal information was involved. It therefore strengthened the early public account rather than establishing a second October intrusion. [S25]
LIMITS	The notification template lists categories that can differ among recipients. Those categories should not be presented as fields stolen from every individual, and the reviewed notices do not establish a complete affected-person total. [S25]
RESPONSE	Defenders should maintain an incident chronology through later regulatory and individual notices. Manufacturing response plans should preserve evidence of extraction alongside encryption recovery, so delayed findings can update customer and employee communications accurately.

Bottom line

Update the original incident record when later notices confirm extraction.

CASE R

R Money Forward: copied repositories differed from production access

Financial technology

Investigation complete

ACCOUNT	Money Forward disclosed unauthorized copying of GitHub repositories. Public reporting and the company's investigation distinguished exposure within development materials from compromise of the live production database. [S29]

CHRONOLOGY	The company first announced the incident on May 1. Its June 23 fourth report completed the detailed investigation and identified additional information within the copied material. Temporary disruption also affected bank-linking functions. [S28]
ESTABLISHED	The final update identified additional customer names and email addresses, business contacts and employee information. The company also reported internal identifiers relating to 60,449 customers. These identifiers alone did not directly identify individuals and contained neither names nor email addresses; they differed from login IDs. [S28]
LIMITS	The company did not confirm unauthorized access to its production database. Repository copying, secret exposure and access to systems reachable with those secrets require distinct findings. The published categories should not be combined into an unsupported total. [S28]
RESPONSE	Defenders should scan development materials for production-derived data, revoke exposed secrets and test access with replacement credentials. Service interruption decisions should reflect the dependency being contained and the evidence required for safe reconnection.

Bottom line

Remove production-derived data from repositories and validate replacement credentials before reconnection.

S

CASE S

An online platform: incomplete logs constrained the conclusion

Digital services

Potential exposure

ACCOUNT	An online platform reported unauthorized access involving development and cloud environments. [S30]
SCOPE	Exposed credentials required investigation beyond the initially reviewed environment. [S30]
ESTABLISHED	Personal information was within the potential scope of access. [S30]
LIMITS	Incomplete logs prevented a categorical no-leak conclusion but did not confirm complete database theft. [S30]
RESPONSE	Revoke exposed credentials and retain query-level evidence for sensitive cloud data.

Bottom line

Revoke exposed credentials and retain query-level evidence for sensitive cloud data.

T

CASE T

A financial services operator: retained test data created exposure

Financial services

Official findings

ACCOUNT	A financial services operator confirmed unauthorized access to a test environment. [S31]
SCOPE	The investigation identified misuse of account credentials. [S31]
ESTABLISHED	Retained business information was within the affected scope. [S31]
LIMITS	The findings did not establish compromise of transaction processing. [S31]
RESPONSE	Retire unnecessary test environments and remove copied business data when testing ends.

Bottom line

Retire unnecessary test environments and remove copied business data when testing ends.

U

CASE U

A manufacturer: external transmission did not resolve file scope

Manufacturing

Final investigation

ACCOUNT	A manufacturer reported an intrusion involving remote-access credentials. [S32]
SCOPE	Later findings confirmed external data transmission. [S32]
ESTABLISHED	The specific files sent externally remained unidentified. [S32]
LIMITS	Confirmed transmission did not establish the contents of every exposed file or subsequent public release. [S32]
RESPONSE	Review remote-access authentication and preserve outbound-transfer logs.

Bottom line

Review remote-access authentication and preserve outbound-transfer logs.

CASE V

V

Nihon Kotsu: operational and historical records had different scopes

Transport

Revised official scope

ACCOUNT	Nihon Kotsu reported malware intrusion and suspension of hired-car systems. Later reporting and corporate notices distinguished the service interruption from the affected historical personal-information holdings. [S35]
CHRONOLOGY	The intrusion was detected on July 11 and first disclosed on July 13. The October 30 sixth notice refined affected groups after earlier investigation updates. The chronology describes one evolving incident. [S34] [S33]
ESTABLISHED	Affected groups included private-car customers, staff, applicants, relatives, business contacts and accident counterparties. Their approximate category counts differed substantially. Some records included identity, financial or health-related fields, depending on the group. [S33]
LIMITS	The categories may overlap and should not be summed as unique people. The operator excluded taxi ride and dispatch customer data from this scope. Hired-car disruption does not establish compromise of all taxi operations. [S33]
RESPONSE	Defenders should separate recruitment and accident records from current dispatch operations, reduce retention and exercise telephone alternatives. Transport continuity plans should identify exactly which booking or dispatch workflow can continue while affected environments remain isolated.

Bottom line

Separate retained personnel and accident records from active dispatch systems.

CASE W

W

A transport operator: business applications held personal information

Transport

Official disclosure

ACCOUNT	A transport operator confirmed information extraction from a business application. [S36]
SCOPE	Application recovery and assessment of the stored information were separate response tasks. [S36]
ESTABLISHED	The affected information included personnel and business-contact data. [S36]

LIMITS	The reviewed notice did not establish ransomware or an actor attribution. [S36]
RESPONSE	Inventory personal information in supporting applications and preserve access logs during recovery.

Bottom line

Inventory personal information in supporting applications and preserve access logs during recovery.

X

CASE X

A technology provider: investigate environments separately

Technology services

Potential exposure

ACCOUNT	A technology provider investigated unauthorized access across separate environments. [S37]
SCOPE	The investigations had different access histories and information scopes. [S37]
ESTABLISHED	Potential exposure included account information and stored credentials. [S37]
LIMITS	External extraction across the entire potential population was not established. A single attack chain was not established. [S37]
RESPONSE	Rotate potentially exposed secrets and assess each environment on its own evidence.

Bottom line

Rotate potentially exposed secrets and assess each environment on its own evidence.

Y

CASE Y

BOOKOFF: a confirmed leak and corrected field list

Retail

Official findings

ACCOUNT	BOOKOFF disclosed unauthorized access to its membership-management system and began individual notification. Subsequent corporate findings provided a precise distinction between membership records and affected people. [S39]
CHRONOLOGY	The company confirmed access on October 6, with information obtained from October 4–6. It first disclosed the incident on October 9. The November 6 third notice consolidated findings and current response. [S38]

ESTABLISHED	The announced scope was 6,427,735 membership records relating to 6,383,279 people, including former members. An access-control problem in part of the system was exploited. The published information categories included hashed passwords and customer contact fields. [S38]
LIMITS	An October correction added fields omitted from the earlier list without changing the person count. The latest notice did not confirm public release, point misuse or alteration of member information. Payment and bank details were outside scope. [S38]
RESPONSE	Defenders should validate field-level scope before notification and distinguish account records from people. Retail response plans should support direct contact and customer self-checking while tracking revisions consistently across frequently asked questions and support channels.

Bottom line

Reconcile affected people, membership records and field lists before issuing customer notices.

Z

CASE Z

ANA: provider records included different passenger-data tiers

Official disclosure

Aviation

ACCOUNT	ANA confirmed a passenger-data incident involving its reservation-system provider. National reporting described the carrier's affected population, while the company notice separated basic booking data from additional information held for a smaller group. [S41]
CHRONOLOGY	The reviewed company notice was dated October 30, following reporting on October 29. It identified reservation records dating from August 2023 through September 2026. Those booking dates did not establish the intrusion period. [S40]
ESTABLISHED	Approximately 37,800 customers were affected. Around 36,100 were associated with basic reservation information, while approximately 1,700 had additional fields, potentially including passport or contact information. The categories reflected different passenger-data holdings. [S40]
LIMITS	The company excluded card details and passwords. The notice did not establish that every passenger had the more sensitive additional fields exposed. The supplier event should not be presented as direct intrusion into every airline application. [S40]

RESPONSE

Defenders should map passenger information by provider and field sensitivity, then prepare tailored notices for each population. Aviation exercises should include reservation-themed impersonation while keeping flight operations, booking availability and confidentiality findings separate.

Bottom line

Tailor passenger notices to the fields actually present in each provider-held record.

5.2 Additional public accounts

Additional account AA: OpJapan: attack claims remained different from proven outages

- **Account.** Security researchers described renewed campaigns using the OpJapan label. The reviewed research supports analysis of actor claims and targeting patterns, while leaving the operational effect on each claimed target unresolved. [S42] [S43]
- **Chronology.** S2W reported a February 14–16 claim wave. Check Point's September 7 research examined renewed activity during August 24–30. Publication dates and the claimed activity windows are separate parts of the chronology. [S42] [S43]
- **Established.** Check Point recorded 66 claims concerning 26 organizations in the later wave. The research primarily described distributed denial-of-service activity and included a surveillance-access claim. These are the researcher's counts of claims and named targets. [S42]
- **Limits.** The research did not establish backend compromise or data leakage across the claimed targets. Claim totals are not confirmed incident totals, and an actor's screenshot or service-error observation does not establish a sustained nationwide outage. [S42]
- **Response.** Defenders should compare claims with availability telemetry, provider logs and customer impact before escalation. Maintain denial-of-service capacity and communications plans, while assessing any alleged access or stolen data through a separate evidence review.

Additional account AB: CoGUI: disruption targeted a phishing ecosystem focused on Japan

- **Account.** Proofpoint described an October disruption effort against Chinese-language phishing kits with a strong Japanese focus. Microsoft's related civil-action notice supplied a separate record of the disruption proceedings. [S44] [S45]
- **Chronology.** Both reviewed sources were published on October 14. The research connects the intervention to an existing phishing ecosystem rather than identifying a single new breach at a Japanese bank or retailer. [S44]
- **Established.** Proofpoint assessed relationships among CoGUI, CoAceV and CoFish_ws, including common roots and affiliate activity. The kits supported high-volume impersonation of consumer-facing brands. Those relationships remain the researchers' assessment, rather than independently established ownership findings here. [S44]

- **Limits.** Large message-volume figures in the research cover broader campaign activity and should not be restated as Japanese victims or successful fraud. The disruption does not establish permanent elimination of the kits or their operators. [S44]
- **Response.** Defenders should combine brand monitoring with payment-fraud signals and customer reporting. Disruption should prompt checks for replacement domains and revised lures, while account protection continues through stronger authentication and rapid handling of suspected credential theft.

Additional account AC: A manufacturer: ransomware halted production

- **Account.** A manufacturer reported ransomware that halted production. [S46]
- **Scope.** Investigation and recovery planning continued after the disclosure. [S46]
- **Established.** Remote-access authentication and backup protection required review. [S46]
- **Limits.** A production interruption did not establish compromise of deployed customer products. [S46]
- **Response.** Enforce multifactor authentication and test isolated recovery before accepting a restart plan.

Additional account AD: Rakuten Securities: test-system scope involved two account categories

- **Account.** Rakuten Securities disclosed unauthorized access involving a test system. National business coverage reported the possible information exposure; a subsequent corporate notice confirmed a Financial Services Agency reporting order. [S49] [S48]
- **Chronology.** The broker detected suspected unauthorized access on November 16. Its investigation found that information may have leaked on November 11. The first public notice followed on November 17. The reporting-order notice followed on November 19. [S47] [S48]
- **Established.** One category covered detailed personal and financial fields for up to 4.47 million accounts. A separate category covered customer codes and login identifiers for up to 11.25 million accounts. Former accounts were included. [S47]
- **Limits.** The release did not establish overlap between those categories, so they must not be summed. Password or trading-PIN leakage and related unauthorized trades were not confirmed. Possible test-data exposure differs from established fraudulent account trading. [S47]
- **Response.** Defenders should remove unnecessary production-derived information from test environments and apply equivalent access governance where sensitive fields remain. Incident response should assess identity exposure and trading-secret compromise separately, using evidence appropriate to each risk.

Additional account AE: Monex: onboarding documents remained a supplier-side concern

- **Account.** Monex's November 13 interim corporate report detailed possible leakage from an account-opening contractor. National television coverage reported the revised scope, including information retained for incomplete applications. [S51]
- **Chronology.** The supplier detected the event on October 18 and blocked unauthorized access on October 19. November 13 was a scope update concerning that earlier incident, rather than evidence of a new November attack. [S50]

- **Established.** The maximum scope included approximately 1.13 million email-address entries, with duplicates and unfinished applications. A further 1,592 identity-document images were potentially involved. The company was still establishing the corresponding number of individuals. [S50]
- **Limits.** Email entries and document images cannot be added as people. Login and trading credentials were held in a different database and were not leaked. Some account-opening functions remained suspended while the contractor investigation continued. [S50]
- **Response.** Defenders should minimise abandoned application data and identity-image retention, then verify contractor segmentation. Broker continuity plans should allow customer support to distinguish interrupted onboarding from trading availability and explain why different information categories require different protective steps.

Additional account AF: SBC Medical: customer history and staff records had overlapping scope

- **Account.** SBC Medical Group reported unauthorized access affecting Japan-based systems. Its Japanese corporate release and subsequent reporting described customer information and staff records, while identifying a separate clinic-management service incident. [S52] [S54]
- **Chronology.** The group detected the events on November 16. Its investor notice was dated November 18 in the United States, followed by the November 19 Japanese announcement. These publication dates describe the same disclosure cycle. [S53]
- **Established.** The basic-information category covered 1,624,000 people. Reservation, consultation, review and monitoring-related metadata categories overlapped. The corporate release also identified staff accounts and personnel documents, and stated that historical customer passwords had been stored without encryption. [S52]
- **Limits.** The monitoring category involved metadata and filenames rather than leaked photographs. Electronic medical records and MySBC were not confirmed stolen. Separate access to a clinic-management service does not establish a common attacker or identical affected populations. [S52] [S53]
- **Response.** Defenders should separate clinical, booking, marketing and personnel systems, then address password reuse where plaintext secrets are confirmed. Notices should describe overlapping categories without creating a misleading combined customer total.

Additional account AG: Rokkatei: a payment page exposed data without storing cards

- **Account.** Rokkatei disclosed tampering affecting its online-shop payment page. Reporting on the initial notice was followed by a November 21 corporate update that expanded the possible information scope and described a reported misuse case. [S56]
- **Chronology.** The affected input window ran from October 21 at 21:00 to November 18 at 11:00. The first notice appeared on November 18. A reported unauthorized card-use case was confirmed on November 20. [S55]
- **Established.** Altered payment-page software could extract information entered by customers even though the shop did not retain a card-number database. The second notice added possible exposure of names, addresses and contact details. [S55]
- **Limits.** The current findings did not establish that every potentially affected entry was extracted or misused. One confirmed misuse report should not be described as the outcome for the entire possible exposure population. [S55]

- **Response.** The retailer requested card reissue. Defenders should monitor checkout scripts and browser-side changes, validate third-party payment integrations and prepare customer guidance covering both payment-card risk and the personal information entered during checkout.

Additional account AH: Arara: an address count required careful interpretation

- **Account.** Arara confirmed unauthorized access affecting its email-distribution platform. National reporting covered the announced address count. [S58]
- **Chronology.** The third report dates reconnaissance to October 27 and activity to October 28–31. All services stopped on October 31. The latest reviewed provider update was November 6, before the recent fortnight. [S57]
- **Established.** Arara reported confirmed extraction of 81,329,467 email addresses. This figure does not represent unique people. Some customer-specific attributes were also involved. The provider investigated up to 380 customer companies and abuse of the platform's sending functions. [S57]
- **Limits.** Addresses are not unique people. An additional cloud dataset identified during the same period did not establish a new attack. This event is separate from the other messaging-provider and payment-platform incidents discussed here. [S57]
- **Response.** Defenders should review tenant-specific fields, restrict message-sending privileges and monitor unexpected outbound campaigns. Supplier notices should state whether figures represent addresses, messages, records or people, and distinguish confirmed findings from unresolved details.

Additional account AI: A messaging provider: shared-platform exposure reached customers

- **Account.** A messaging provider revised a shared-platform incident; a customer later reported downstream exposure. [S59] [S60] [S61]
- **Scope.** Provider and customer disclosures described different scopes of the service relationship. [S59]
- **Established.** Information leakage affected provider-held customer records. [S59]
- **Limits.** Provider and customer populations may overlap and must not be added as unique people. [S59]
- **Response.** Constrain bulk exports and prepare alternatives for customer communications.

Additional account AJ: GMO Internet: hosted desktops carried trading-session risk

- **Account.** GMO Internet confirmed malware on customer hosted desktops used by trading-tool customers. Reporting described the company's response to extortion threats and possible effects on customers' own devices. [S64]
- **Chronology.** A customer inquiry arrived on October 19, malware was confirmed on October 20 and potentially affected servers were stopped on October 21. Later notices described publication of customer information on October 27. [S62] [S63]
- **Established.** The possible scope comprised 26,739 servers. Credentials stored in trading tools might have been taken and misused, and customers reported unrecognized transactions. Corporate guidance addressed ending existing trading sessions alongside changing credentials. [S62] [S63]
- **Limits.** The possible server population is not a confirmed compromise or affected-person count. Actor threats concerning customer devices do not prove that every endpoint was encrypted. The notices do not establish a single outcome for all customers. [S63]

- **Response.** Defenders should inspect automation hosts, revoke active sessions and rotate stored trading credentials together. Financial response teams should compare transaction records with host findings before attributing individual unauthorized trades to the platform incident.

Additional account AK: A consumer app: usage information required protection

- **Account.** A consumer application operator confirmed unauthorized access to customer-related data. [S65]
- **Scope.** The disclosure did not establish when the unauthorized activity began or ended. [S65]
- **Established.** Usage-related information was within the affected scope. [S65]
- **Limits.** The notice did not confirm external extraction or provide an affected-person total. [S65]
- **Response.** Protect usage datasets and distinguish confirmed access from extraction in customer advice.

5.3 Sector decisions

The common operational requirement is to identify the exact dependency being contained. A booking service, refund form, contractor account or stored research key can extend the response beyond the system where the incident was detected. Affected organizations need both technical owners and business owners for those dependencies.

The information category should govern customer action. Identity-document images, unencrypted passwords, encrypted objects, customer identifiers and purchase histories carry different implications. Notices should preserve those distinctions when counts change and when downstream customers publish later updates.

5.4 Anonymous incidents and the wider leak wave

NPA's first-half report describes a January 2026 ransomware incident at an unnamed beverage manufacturer. Police identified LockBit and restored more than 1 TB. The recovery date is not specified. This official example supports preserving evidence and seeking recovery assistance without inventing a named victim or a restoration deadline. [S66]

JPCERT/CC's October advisory distinguishes several patterns behind recent domestic data leaks, including API abuse, application-server shells, known vulnerabilities and administration weaknesses. Its later update does not establish that every case shared one actor, flaw or access path. An organisation should investigate its actual exposed application and access evidence. [S73]

On 6 November, NPA announced joint investigations into large personal-information leaks confirmed during 2026. A shared investigation does not establish a shared perpetrator across every disclosure in this chapter. Preserve each account's individual chronology and scope. [S82]

5.5 Further original-notice accounts

The following 137 short accounts extend the detailed cases above. Identifying dates, figures and service details are withheld. Supplier and customer notices can concern overlapping populations. The rows do not form a national incident or victim total.

N001

An organisation reported loss of backup media. External leakage was not confirmed. Secure and inventory backup media. [S163]

N002

An organisation confirmed information leakage through application access. Test authorization and constrain bulk retrieval. [S167]

N003

A public-sector body reported possible exposure of personnel and contractor records after unauthorized access through a remote-access device. Review remote-access controls and revoke affected maintenance accounts. [S114]

N004

An organisation confirmed information leakage after unauthorized access. Review affected data and restrict access before restoring service. [S169]

N005

An organisation confirmed information leakage after unauthorized access. Review affected data and restrict access before restoring service. [S173]

N006

An organisation confirmed information leakage after unauthorized access. Review affected data and restrict access before restoring service. [S164]

N007

An organisation reported possible information exposure. Confirmed extraction was not established for the entire potential scope. Review access and retained information. [S122]

N008

An organisation confirmed unauthorized viewing of information. Viewing alone does not establish external copying. Test authorization and review access logs. [S120]

N009

An organisation confirmed information leakage after unauthorized access. Review affected data and restrict access before restoring service. [S168]

N010

An organisation confirmed information leakage after unauthorized access. Review affected data and restrict access before restoring service. [S176]

N011

An organisation reported ransomware disruption. Service interruption alone does not establish data theft. Test isolated recovery and maintain alternative service channels. [S166]

N012

An organisation reported possible information exposure. Confirmed extraction was not established for the entire potential scope. Review access and retained information. [S193]

N013

An organisation reported possible information exposure involving a supplier. Validate the affected customer scope and review supplier access. [S177]

N014

An organisation confirmed information leakage after unauthorized access. Review affected data and restrict access before restoring service. [S121]

N015

An organisation confirmed information leakage after unauthorized access. Review affected data and restrict access before restoring service. [S175]

N016

An organisation confirmed information leakage after unauthorized access. Review affected data and restrict access before restoring service. [S165]

N017

An organisation confirmed information leakage after unauthorized access. Review affected data and restrict access before restoring service. [S201]

N018

An organisation reported ransomware disruption. Service interruption alone does not establish data theft. Test isolated recovery and maintain alternative service channels. [S95] [S96]

N019

An organisation confirmed information leakage after unauthorized access. Review affected data and restrict access before restoring service. [S191]

N020

An organisation reported possible information acquisition through application access. Test authorization and investigate unusual bulk retrieval. [S179]

N021

An organisation reported possible information exposure. Confirmed extraction was not established for the entire potential scope. Review access and retained information. [S186]

N022

An organisation confirmed leakage involving authentication information. Revoke affected credentials and investigate access to dependent services. [S195]

N023

An organisation confirmed information leakage after unauthorized access. Review affected data and restrict access before restoring service. [S196]

N024

An organisation reported possible information exposure. Confirmed extraction was not established for the entire potential scope. Review access and retained information. [S178]

N025

An organisation reported possible information exposure. Confirmed extraction was not established for the entire potential scope. Review access and retained information. [S185]

N026

An organisation confirmed leakage involving authentication information. Revoke affected credentials and investigate access to dependent services. [S184]

N027

An organisation confirmed leakage involving authentication information. Revoke affected credentials and investigate access to dependent services. [S183]

N028

An organisation confirmed unauthorized downloading of files containing personal information. Restrict sensitive-file access and preserve download logs. [S119]

N029

An organisation reported possible information exposure. Confirmed extraction was not established for the entire potential scope. Review access and retained information. [S188]

N030

An organisation confirmed information leakage involving a supplier. Review supplier-held copies and coordinate affected-customer notifications. [S194]

N031

An organisation confirmed information leakage after unauthorized access. Review affected data and restrict access before restoring service. [S204]

N032

An organisation reported possible information exposure. Confirmed extraction was not established for the entire potential scope. Review access and retained information. [S198]

N033

An organisation reported possible information exposure. Confirmed extraction was not established for the entire potential scope. Review access and retained information. [S172]

N034

An organisation confirmed information leakage involving a supplier. Review supplier-held copies and coordinate affected-customer notifications. [S180]

N035

An organisation confirmed information leakage after unauthorized access. Review affected data and restrict access before restoring service. [S199]

N036

An organisation confirmed information leakage after unauthorized access. Review affected data and restrict access before restoring service. [S187]

N037

An organisation reported possible information exposure. Confirmed extraction was not established for the entire potential scope. Review access and retained information. [S117]

N038

An organisation reported possible information exposure. Confirmed extraction was not established for the entire potential scope. Review access and retained information. [S118]

N039

An organisation confirmed information leakage after unauthorized access. Review affected data and restrict access before restoring service. [S132]

N040

An organisation reported possible information exposure involving a supplier. Validate the affected customer scope and review supplier access. [S182]

N041

An organisation confirmed leakage involving authentication information. Revoke affected credentials and investigate access to dependent services. [S102] [S103] [S104]

N042

An organisation reported possible information exposure. Confirmed extraction was not established for the entire potential scope. Review access and retained information. [S150]

N043

An organisation confirmed information leakage through application access. Test authorization and constrain bulk retrieval. [S151]

N044

An organisation confirmed information leakage after unauthorized access. Review affected data and restrict access before restoring service. [S152]

N045

An organisation confirmed information leakage after unauthorized access. Review affected data and restrict access before restoring service. [S153]

N046

An organisation confirmed leakage involving authentication information. Revoke affected credentials and investigate access to dependent services. [S154]

N047

An organisation confirmed unauthorized downloading of files containing personal information. Restrict sensitive-file access and preserve download logs. [S155]

N048

An organisation confirmed unauthorized account access. Account misuse does not by itself establish server intrusion. Strengthen authentication and revoke affected sessions. [S156]

N049

An organisation confirmed unauthorized use of cloud credentials. Revoke affected keys and constrain service permissions. [S157]

N050

An organisation reported possible information exposure. Confirmed extraction was not established for the entire potential scope. Review access and retained information. [S158]

N051

An organisation confirmed information leakage involving a supplier. Review supplier-held copies and coordinate affected-customer notifications. [S243]

N052

An organisation reported possible information exposure. Confirmed extraction was not established for the entire potential scope. Review access and retained information. [S171]

N053

An organisation confirmed information leakage after unauthorized access. Review affected data and restrict access before restoring service. [S181]

N054

An organisation reported possible information exposure. Confirmed extraction was not established for the entire potential scope. Review access and retained information. [S197]

N055

An organisation reported possible information exposure involving a supplier. Validate the affected customer scope and review supplier access. [S130]

N056

An organisation reported payment-page tampering and possible exposure of payment information. Inspect payment scripts and coordinate response with payment partners. [S146]

N057

An organisation reported possible information exposure. Confirmed extraction was not established for the entire potential scope. Review access and retained information. [S147]

N058

An organisation confirmed information leakage after unauthorized access. Review affected data and restrict access before restoring service. [S148]

N059

An organisation reported possible information exposure. Confirmed extraction was not established for the entire potential scope. Review access and retained information. [S149]

N060

An organisation reported possible information exposure. Confirmed extraction was not established for the entire potential scope. Review access and retained information. [S189]

N061

An organisation confirmed information leakage after unauthorized access. Review affected data and restrict access before restoring service. [S128]

N062

An organisation confirmed information leakage after unauthorized access. Review affected data and restrict access before restoring service. [S144]

N063

An organisation confirmed leakage involving authentication information. Revoke affected credentials and investigate access to dependent services. [S145]

N064

An organisation reported possible information exposure. Confirmed extraction was not established for the entire potential scope. Review access and retained information. [S244]

N065

An organisation reported possible information exposure. Confirmed extraction was not established for the entire potential scope. Review access and retained information. [S99]

N066

An organisation reported possible information exposure. Confirmed extraction was not established for the entire potential scope. Review access and retained information. [S115]

N067

An organisation reported possible exposure involving authentication information. Revoke potentially exposed credentials and review dependent access. [S116]

N068

An organisation confirmed unauthorized viewing of information. Viewing alone does not establish external copying. Test authorization and review access logs. [S140]

N069

An organisation confirmed leakage involving authentication information. Revoke affected credentials and investigate access to dependent services. [S141]

N070

An organisation confirmed unauthorized account access. Account misuse does not by itself establish server intrusion. Strengthen authentication and revoke affected sessions. [S142]

N071

An organisation confirmed information leakage through application access. Test authorization and constrain bulk retrieval. [S143]

N072

An organisation confirmed information leakage after unauthorized access. Review affected data and restrict access before restoring service. [S170]

N073

An organisation reported possible information exposure. Confirmed extraction was not established for the entire potential scope. Review access and retained information. [S134]

N074

An organisation confirmed unauthorized account access. Account misuse does not by itself establish server intrusion. Strengthen authentication and revoke affected sessions. [S135]

N075

An organisation confirmed leakage involving authentication information. Revoke affected credentials and investigate access to dependent services. [S136]

N076

An organisation confirmed unauthorized account access. Account misuse does not by itself establish server intrusion. Strengthen authentication and revoke affected sessions. [S137]

N077

An organisation confirmed information leakage after unauthorized access. Review affected data and restrict access before restoring service. [S138]

N078

An organisation confirmed information leakage after unauthorized access. Review affected data and restrict access before restoring service. [S139]

N079

An organisation confirmed information leakage after unauthorized access. Review affected data and restrict access before restoring service. [S229] [S230]

N080

An organisation reported possible information exposure. Confirmed extraction was not established for the entire potential scope. Review access and retained information. [S240]

N081

An organisation reported possible information exposure. Confirmed extraction was not established for the entire potential scope. Review access and retained information. [S245]

N082

An organisation confirmed information leakage after unauthorized access. Review affected data and restrict access before restoring service. [S247]

N083

An organisation reported unauthorized reward activity. Review access controls and investigate account misuse. [S248]

N084

An organisation reported possible information acquisition through application access. Test authorization and investigate unusual bulk retrieval. [S174]

N085

An organisation confirmed information leakage after unauthorized access. Review affected data and restrict access before restoring service. [S190]

N086

An organisation confirmed information leakage after unauthorized access. Review affected data and restrict access before restoring service. [S100] [S101]

N087

An organisation reported possible information exposure. Confirmed extraction was not established for the entire potential scope. Review access and retained information. [S94]

N088

An organisation reported possible information exposure. Confirmed extraction was not established for the entire potential scope. Review access and retained information. [S98]

N089

An organisation confirmed information leakage involving a supplier. Review supplier-held copies and coordinate affected-customer notifications. [S111]

N090

An organisation reported possible information exposure. Confirmed extraction was not established for the entire potential scope. Review access and retained information. [S123]

N091

An organisation confirmed information leakage after unauthorized access. Review affected data and restrict access before restoring service. [S228]

N092

An organisation reported possible information exposure. Confirmed extraction was not established for the entire potential scope. Review access and retained information. [S112]

N093

An organisation confirmed unauthorized access and changes to stored information. Review authorization and validate data integrity before restoring access. [S131]

N094

An organisation reported possible information exposure. Confirmed extraction was not established for the entire potential scope. Review access and retained information. [S219] [S220]

N095

A local government reported ransomware disruption of a resident-notification system. Restoration was targeted rather than confirmed; test alternative emergency-message channels. [S246]

N096

An organisation reported possible information exposure involving a supplier. Validate the affected customer scope and review supplier access. [S105] [S106] [S107]

N097

An organisation reported no evidence of customer-system data extraction in the reviewed investigation. This does not resolve every supplier-side exposure. Validate the affected environment separately. [S161]

N098

An organisation confirmed unauthorized viewing of information. Viewing alone does not establish external copying. Test authorization and review access logs. [S108]

N099

An organisation reported possible exposure involving authentication information. Revoke potentially exposed credentials and review dependent access. [S110]

N100

An organisation reported possible information exposure. Confirmed extraction was not established for the entire potential scope. Review access and retained information. [S129]

N101

An organisation confirmed unauthorized access to business documents. Restrict document access and preserve audit logs. [S160]

N102

An organisation reported possible information exposure involving a supplier. Validate the affected customer scope and review supplier access. [S223] [S224]

N103

An organisation reported possible exposure involving authentication information. Revoke potentially exposed credentials and review dependent access. [S227]

N104

An organisation confirmed information leakage after unauthorized access. Review affected data and restrict access before restoring service. [S231] [S232] [S233]

N105

An organisation confirmed information leakage involving a supplier. Review supplier-held copies and coordinate affected-customer notifications. [S241]

N106

An organisation reported possible information exposure involving a supplier. Validate the affected customer scope and review supplier access. [S242]

N107

An organisation reported possible information exposure. Confirmed extraction was not established for the entire potential scope. Review access and retained information. [S202]

N108

An organisation confirmed information leakage after unauthorized access. Review affected data and restrict access before restoring service. [S205]

N109

A notification-service provider confirmed leakage involving authentication information. Reset affected credentials, terminate sessions and test stored-password protection. [S109]

N110

An organisation reported payment-page tampering and possible exposure of payment information. Inspect payment scripts and coordinate response with payment partners. [S125]

N111

An organisation confirmed information leakage after unauthorized access. Review affected data and restrict access before restoring service. [S126]

N112

An organisation reported possible information exposure. Confirmed extraction was not established for the entire potential scope. Review access and retained information. [S127]

N113

An organisation reported possible information exposure involving a supplier. Validate the affected customer scope and review supplier access. [S206]

N114

An organisation confirmed information leakage after unauthorized access. Review affected data and restrict access before restoring service. [S216]

N115

An organisation confirmed leakage involving authentication information. Revoke affected credentials and investigate access to dependent services. [S217]

N116

An organisation reported possible information exposure. Confirmed extraction was not established for the entire potential scope. Review access and retained information. [S218]

N117

An organisation confirmed information leakage after unauthorized access. Review affected data and restrict access before restoring service. [S221]

N118

An organisation confirmed unauthorized account access. Account misuse does not by itself establish server intrusion. Strengthen authentication and revoke affected sessions. [S222]

N119

An organisation confirmed information leakage after unauthorized access. Review affected data and restrict access before restoring service. [S225] [S226]

N120

An organisation reported possible information exposure involving a supplier. Validate the affected customer scope and review supplier access. [S238]

N121

An organisation confirmed information leakage after unauthorized access. Review affected data and restrict access before restoring service. [S239]

N122

A notification-service provider reported unauthorized sending and misuse of integration access. Revoke integration secrets and validate sending controls. [S200]

N123

A public-sector body reported access outside intended file-sharing recipients and possible information leakage. Review sharing permissions, revoke exposed links and prepare a secure alternative. [S97]

N124

An organisation confirmed information leakage after unauthorized access. Review affected data and restrict access before restoring service. [S113]

N125

An organisation confirmed unauthorized account access. Account misuse does not by itself establish server intrusion. Strengthen authentication and revoke affected sessions. [S124]

N126

An organisation confirmed information leakage after unauthorized access. Review affected data and restrict access before restoring service. [S207]

N127

An organisation confirmed information leakage involving a supplier. Review supplier-held copies and coordinate affected-customer notifications. [S208] [S209] [S210]

N128

An organisation confirmed information leakage after unauthorized access. Review affected data and restrict access before restoring service. [S211] [S212]

N129

An organisation reported highly likely information leakage involving a supplier. Review integration credentials and minimise information available to external tools. [S213] [S214]

N130

An organisation confirmed external data transmission. The specific transmitted records remained unidentified. Rotate potentially exposed credentials and reduce retained copies. [S215]

N131

An organisation confirmed unauthorized access and changes to stored information. Review authorization and validate data integrity before restoring access. [S234]

N132

An organisation reported possible information exposure involving a supplier. Validate the affected customer scope and review supplier access. [S235]

N133

An organisation confirmed information leakage after unauthorized access. Review affected data and restrict access before restoring service. [S236]

N134

An organisation confirmed unauthorized access and changes to stored information. Review authorization and validate data integrity before restoring access. [S237]

N135

An organisation reported possible exposure involving authentication information. Revoke potentially exposed credentials and review dependent access. [S162]

N136

An organisation confirmed information leakage after unauthorized access. Review affected data and restrict access before restoring service. [S192]

N137

An organisation reported possible information exposure. Confirmed extraction was not established for the entire potential scope. Review access and retained information. [S203]

KEY TAKEAWAYS

01

Remove unnecessary sensitive data from test systems, supplier stores and historical copies.

02

Revoke exposed credentials and sessions across connected environments before restoring trust.

03

Base recovery and customer guidance on confirmed fields, current scope and the actual service dependency.

CHAPTER 06

Availability and connected-device risk

THIS CHAPTER ANSWERS

What do official accounts establish about disruption and connected devices, and which operational decisions follow?

4

official publication milestones, each with a distinct scope

6.1 Website disruption requires a precise impact statement 74

6.2 Domestic-looking traffic can conceal a remote attacker 74

6.3 Keep operational scenarios separate from observed incidents 75

6.4 Official developments through the cutoff 75

6.5 Claims and official evidence boundaries 76

CHAPTER 06

Availability and connected-device risk

IN SHORT

Japan's police documented February DDoS attacks that disrupted websites across government, transport and finance. Connected devices also helped criminals disguise attack origins. These observations support separate decisions about public-service availability and trusted access. A website outage does not establish data theft or disruption of an industrial process. Assign service owners, test recovery arrangements and remove unnecessary paths into operational networks.

6.1 Website disruption requires a precise impact statement

Confirmed disruption needs a defined service and period.

The National Police Agency's September report describes February 2026 DDoS attacks against several critical-infrastructure organizations. It records website-access problems and attributes the activity to groups believed to be pro-Russian hacktivists. [S66]

That account establishes an availability impact. It does not, by itself, establish interference with transport operations, settlement systems or plant controls. A public website and the underlying service can have different dependencies.

For a CISO, the practical question is which customer journey depends on each exposed service. A short interruption to a marketing page differs from an outage affecting passenger information, supplier ordering or incident communications.

Define the consequences before selecting controls. Service owners should identify which requests can be delayed, which transactions require reconciliation, and which users need an alternative route. These are operational decisions requiring business participation.

An external outage claim should enter the response queue with a time, affected function and evidence of actual customer impact. Actor statements can direct attention, but the incident statement should follow the organization's observations.

A response team should also preserve the distinction between a failed request, a degraded application and an unavailable service. Each can require a different decision. Avoid describing every error as a complete shutdown.

6.2 Domestic-looking traffic can conceal a remote attacker

A domestic address is a weak trust signal.

In July, the NPA, communications ministry and NICT explained how household devices can relay third-party traffic as residential proxies. The destination may see a household address while the originating attacker remains elsewhere. [S72]

This matters to organizations that treat local network origins as reassuring. A familiar country or consumer connection cannot substitute for account controls, transaction checks or evidence that a request matches a user's expected activity.

The same advisory recommends preventing unapproved devices from joining business networks and separating IoT networks from work systems. Those measures address the risk that an organization supplies infrastructure criminals can abuse. [S72]

The distinction between device owner and attacker remains important. A person whose equipment relays traffic may be unaware of the activity. Investigation should establish the role of the device before assigning responsibility.

For managed environments, inventory should connect each device to an accountable owner and business purpose. Unmanaged media boxes, cameras and routers deserve attention alongside servers because their network access can outlast their operational usefulness.

Where a device cannot be maintained, the decision should be explicit: replace it, isolate it or remove it. A permanent exception without an owner turns a temporary limitation into an enduring route through the network.

6.3 Keep operational scenarios separate from observed incidents

The accessible official evidence used here documents website disruption and connected-device abuse. It does not establish a Japanese refrigeration failure or industrial-process shutdown within this chapter's evidence base.

The following is an analytical scenario, not a reported Japanese incident. An industrial controller shares connectivity with general office devices and receives remote maintenance from a supplier. An unauthorized session changes its operating state.

The scenario creates a different consequence from a public website outage. Availability controls must account for the process, its safe state and the people who can recover it. A generic internet-blocking decision may have operational consequences.

A joint IT and operations review should identify who can approve remote access, who can terminate it, and how the process remains safe when connectivity is lost. The supplier's responsibilities should be agreed before an incident.

Test recovery with operations personnel present. A backup is useful only when the organization can restore the relevant configuration and verify safe behavior. The acceptance decision belongs to the service or process owner.

6.4 Official developments through the cutoff

Timeline dates are official publication dates. The September report describes February activity; its publication date is not the attack date.

21 Jul 2026 **NPA, MIC and NICT**

Published guidance on household IoT devices abused as residential proxies; this concerns attack origins and device controls. [S72]

10 Sep 2026 **National Police Agency**
Its January–June report described February DDoS website disruptions affecting government, transport and financial services; physical-service disruption was not established here. [S66]

15 Oct 2026 **National Police Agency**
Announced Japan-targeting phishing-infrastructure disruption following a US court order issued on 8 October; this was a separate law-enforcement response. [S74]

16 Nov 2026 **National Police Agency**
Emphasized asset management, exposure reduction, API controls and supplier oversight; the notice is guidance rather than an additional victim case. [S75]

6.5 Claims and official evidence boundaries

Point	Actor claim	Official account	Interpretation
Website disruption	No actor claim is used as evidence in this assessment.	Police reported February website-access problems during DDoS activity. [S66]	Availability impact is supported; data theft requires separate evidence.
Data theft	No actor's campaign-wide data-theft claim is adopted here.	JPCERT/CC describes a separate wave of unauthorized access and data leaks with multiple mechanisms. [S73]	Do not merge that wave with DDoS without evidence linking the incidents.
Physical effect	No actor claim of a Japanese industrial shutdown is adopted here.	The cited accounts cover website disruption and residential-proxy abuse. [S66] [S72]	The example in §6.3 is an analytical scenario, not an observed Japanese incident.

These boundaries help incident leaders communicate accurately while evidence develops. They also prevent unrelated claims from collapsing into a single campaign narrative.

KEY TAKEAWAYS

01
Give each exposed service a business owner, an impact threshold and a tested alternative communication route.

02
Treat residential network origins as context and keep unmanaged connected devices away from business systems.

03
For operational technology, agree access termination, safe-state and recovery decisions with the people responsible for the process.

CHAPTER 07

Threat actors, campaigns and supported relationships

THIS CHAPTER ANSWERS

Which actor and campaign associations are supported by the evidence?

146

Japan-labelled ransomware listings; each records a criminal assertion

7.1 Relationship map 78
7.2 APT-C-60 and legitimate-service delivery 79
7.3 WaterPlum and recruitment as an access route 80
7.4 DDoS and phishing labels 81
7.5 Ransomware listings and regional peers 83
7.6 Listing sectors and monthly distribution 86
7.7 Behaviour matrix for the documented delivery chain 87
7.8 Recent technical advisories require product-specific decisions 88

CHAPTER 07

Threat actors, campaigns and supported relationships

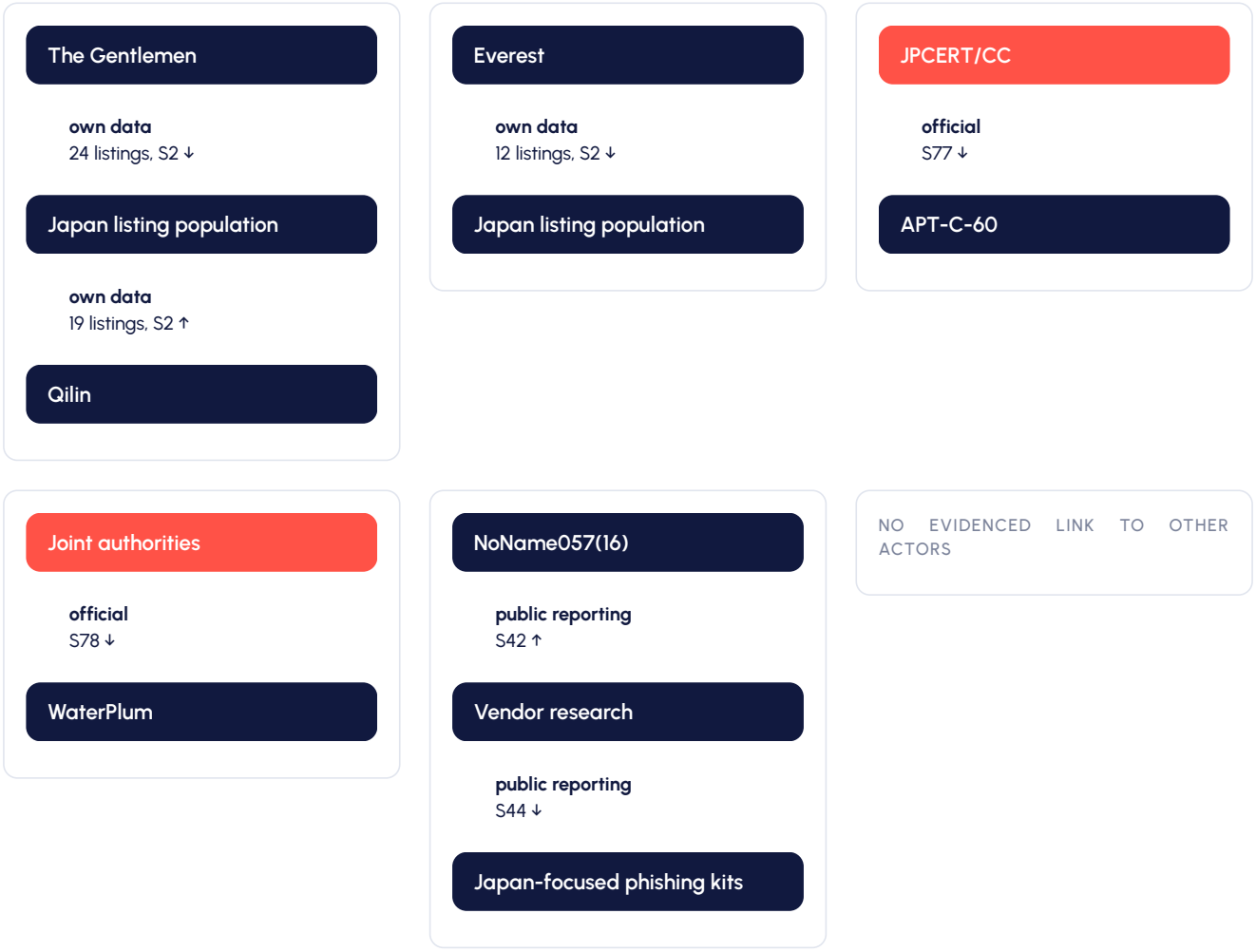
IN SHORT

Japan's evidence contains extortion labels, vendor-described DDoS claims and officially documented malware campaigns. These are different populations. Ransompedia records 146 Japan listings in the requested window, spread across 43 labels. JPCERT/CC describes APT-C-60 delivery through legitimate services. A joint advisory describes WaterPlum recruitment lures. Follow each source's evidence and attribution, then test the corresponding access and recovery controls in your own environment.

7.1 Relationship map

The map connects a source to the label or activity it supports. An edge does not identify a shared operator across different campaigns. The ransomware edges describe Brandefense's own listing data. Official and vendor reporting have their own edge types. [S2][S77][S78][S42][S44]

Own post Relay Official statement Public reporting Our observation



No operational connection between the extortion labels, recruitment campaign, DDoS claims and forum offers is established here. Treating them as a single criminal ecosystem would be an analytical model. The report instead uses separate response questions: restore a service, validate identity, contain malware or assess an availability claim.

7.2 APT-C-60 and legitimate-service delivery

JPCERT/CC's 13 July research describes continued attacks against Japanese organisations during 2026. Its examples begin with spearphishing links to cloud-hosted archives or malicious attachments. Archive contents include a shortcut that starts a further delivery chain. JPCERT/CC identifies the resulting malware as SpyGlace. [S77]

The source describes use of legitimate development and content-delivery services during later stages. It also describes JavaScript started through a standard Windows program. These observations explain why a permitted destination or signed utility is insufficient evidence that a sequence is safe. The service providers are not identified as the campaign operators. [S77]

For defenders, preserve the sequence around a suspicious download: originating message, downloaded archive, user interaction, child processes and subsequent network activity. Investigate an unusual shortcut-to-script chain even when a later request goes to a legitimate service. Apply proportionate restrictions and review legitimate business needs before changing application policy.

APT-C-60

JPCERT/CC campaign label | Attribution only as stated by the cited source

IN JAPAN, 2026

2026-07-13

Spearphishing, archives, shortcuts and legitimate-service delivery leading to SpyGlace

CLAIMED TARGETS

Only within the cited source scope

SEEN IN PUBLIC REPORTING

[S77] Spearphishing, archives, shortcuts and legitimate-service delivery leading to SpyGlace

OUR ASSESSMENT

Campaign identification belongs to JPCERT/CC; no independent state attribution is made here.

CONFIDENCE

High that source reports the stated activity; its unresolved limits remain

7.3 WaterPlum and recruitment as an access route

The 18 September joint advisory describes WaterPlum targeting IT professionals, including people in Japan, through recruitment and coding-task lures. The participating authorities attribute the activity to North Korea. That attribution is theirs; the report makes no independent state-attribution finding. [S78]

The advisory also discusses fraudulent remote-worker activity and a Japanese laptop-farm disruption. The described activity spans December 2025–July 2026. Its international device, wallet or cryptocurrency figures are not Japanese victim totals. Do not convert the publication into a claim that every recruitment approach or remote worker is malicious. [S78]

Recruitment and engineering teams should agree on how unfamiliar code is evaluated. Use an isolated environment without production access or reusable work credentials. Verify recruiter and applicant identity through established channels. If a coding task is suspected to be malicious, preserve the relevant endpoint and account evidence and review exposed integrations.

WaterPlum

Campaign attributed by the joint authorities | Attribution only as stated by the cited source

IN JAPAN, 2026

2026-09-18

Recruitment and coding-task lures targeting IT professionals, including Japan

CLAIMED TARGETS

Only within the cited source scope

SEEN IN PUBLIC REPORTING

[S78] Recruitment and coding-task lures targeting IT professionals, including Japan

OUR ASSESSMENT

The authorities attribute the activity to North Korea. International figures are not Japanese victim totals.

CONFIDENCE

High that source reports the stated activity; its unresolved limits remain

Earlier official espionage advisories provide historical baseline context outside the 2026 observation window. In February 2025, NPA and NISC documented campaigns observed from about 2019 to the time of that advisory against Japanese government, think-tank, academic, semiconductor and manufacturing targets. [S256] The authorities attributed those campaigns to MirrorFace and assessed suspected Chinese involvement. [S256] The advisory describes emails with malicious attachments or download links and exploitation of vulnerabilities in Internet-connected devices; it predates the 2026 window and is excluded from the 2026 profiles. [S256]

7.4 DDoS and phishing labels

Check Point's September research reports 66 claims against 26 Japanese organisations during 24–30 August under NoName057(16)'s renewed campaign. Its account mainly concerns DDoS assertions and one surveillance-access claim. These are not 66 independently confirmed outages or 26 proven intrusions. [S42]

Proofpoint's October research describes three Japan-focused phishing kits and their shared roots and overlapping affiliates. Its language and ecosystem assessments belong to the vendor. They do not establish nationality, state direction or a common operator for every message using a kit. NPA separately reports participation in the infrastructure disruption. [S44][S74]

An impersonated brand is not thereby the source of a breach. The first response is to protect the actual sign-in or payment workflow and give users an authenticated reporting route. A disruption announcement does not establish permanent elimination of the activity.

NoName057(16)

Vendor-described DDoS claimant label | Attribution only as stated by the cited source

IN JAPAN, 2026

2026-09-07

Renewed Japan-focused claims concerning 24–30 August

CLAIMED TARGETS

Only within the cited source scope

SEEN IN PUBLIC REPORTING

[S42] Renewed Japan-focused claims concerning 24–30 August

OUR ASSESSMENT

Vendor-reported claim counts do not establish confirmed downtime, data theft or physical-process access.

CONFIDENCE

High that source reports the stated activity; its unresolved limits remain

Japan-focused phishing kits

Vendor-described kit relationships | Attribution only as stated by the cited source

IN JAPAN, 2026

2026-10-14

Consumer and financial-brand impersonation; an infrastructure disruption

CLAIMED TARGETS

Only within the cited source scope

SEEN IN PUBLIC REPORTING

[S44] Consumer and financial-brand impersonation; an infrastructure disruption

OUR ASSESSMENT

Kit ancestry, affiliates and language assessments belong to the cited vendor. They do not establish nationality or state direction.

CONFIDENCE

High that source reports the stated activity; its unresolved limits remain

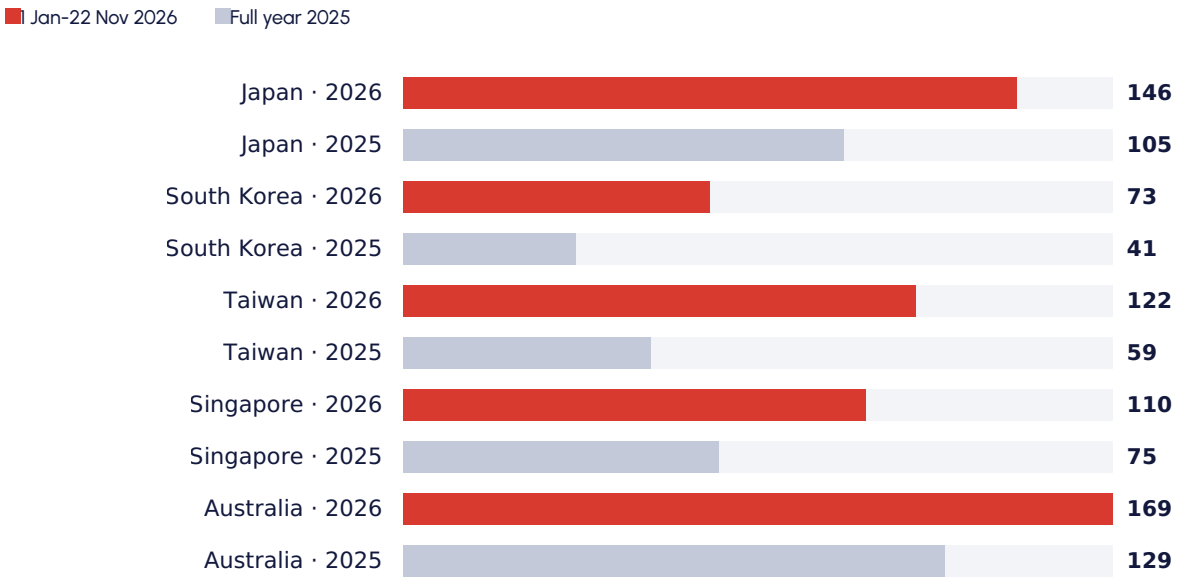
7.5 Ransomware listings and regional peers

Ransompedia records 146 Japan-labelled listings dated within 1 January–22 November 2026, compared with 105 for all of 2025. This compares a partial year with a full year. It is not a matched-period growth rate. Listings are public criminal assertions and may repeat an organisation. [S2]

Figure c08 places the Japan population beside the selected peers. Differences can reflect publication practices, country labels and source visibility as well as criminal activity. They do not measure national control effectiveness.

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

Japan has 146 observed listings; the regional comparison describes claims, not attack probability



Source: Ransompedia country-labelled listing claims [S2]. 2026: 1 January–22 November, closing day partial; 2025: full year. Unequal periods and source visibility; not a national risk ranking.

Peer	Requested window	All of 2025	Reason for comparison
Japan	146	105	Report focus
South Korea	73	41	Nearby technology and industrial dependencies
Taiwan	122	59	Semiconductor and manufacturing supply chains
Singapore	110	75	Regional finance and logistics services
Australia	169	129	Regional service and critical-infrastructure dependencies

The Japanese listing population has 43 labels. The Gentlemen, Qilin and Everest account for 55 listings, or 37.7%. The remaining labels account for 91. A label's frequency does not identify unique operators, entry methods or a success rate. [S2]

Listing label	Listings	Share
The Gentlemen	24	16.4%
Qilin	19	13.0%
Everest	12	8.2%
SafePay	8	5.5%
NightSpire	7	4.8%
Other labels	76	52.1%
Total	146	100.0%

No claim about a label's intrusion method is inferred from the listing count. A defender should examine its own initial-access evidence, restoration readiness and information scope. Buying a product associated with one published technique does not resolve every scenario represented by these labels.

The Gentlemen

Extortion listing label | No state attribution assessed

IN JAPAN, 2026

2026

24 Japan-labelled listings in the requested window

CLAIMED TARGETS

Listing population; victims not named here

SEEN IN PUBLIC REPORTING

[S2] Retained listing count: 24.

OUR ASSESSMENT

The listing count establishes observed criminal assertions. It does not establish unique operators, a successful intrusion, encryption, theft or payment.

CONFIDENCE

High for retained listings; underlying claims unverified

Qilin

Extortion listing label | No state attribution assessed

IN JAPAN, 2026

2026

19 Japan-labelled listings in the requested window

CLAIMED TARGETS

Listing population; victims not named here

SEEN IN PUBLIC REPORTING

[S2] Retained listing count: 19.

OUR ASSESSMENT

The listing count establishes observed criminal assertions. It does not establish unique operators, a successful intrusion, encryption, theft or payment.

CONFIDENCE

High for retained listings; underlying claims unverified

Everest

Extortion listing label | No state attribution assessed

IN JAPAN, 2026

2026

12 Japan-labelled listings in the requested window

CLAIMED TARGETS

Listing population; victims not named here

SEEN IN PUBLIC REPORTING

[S2] Retained listing count: 12.

OUR ASSESSMENT

The listing count establishes observed criminal assertions. It does not establish unique operators, a successful intrusion, encryption, theft or payment.

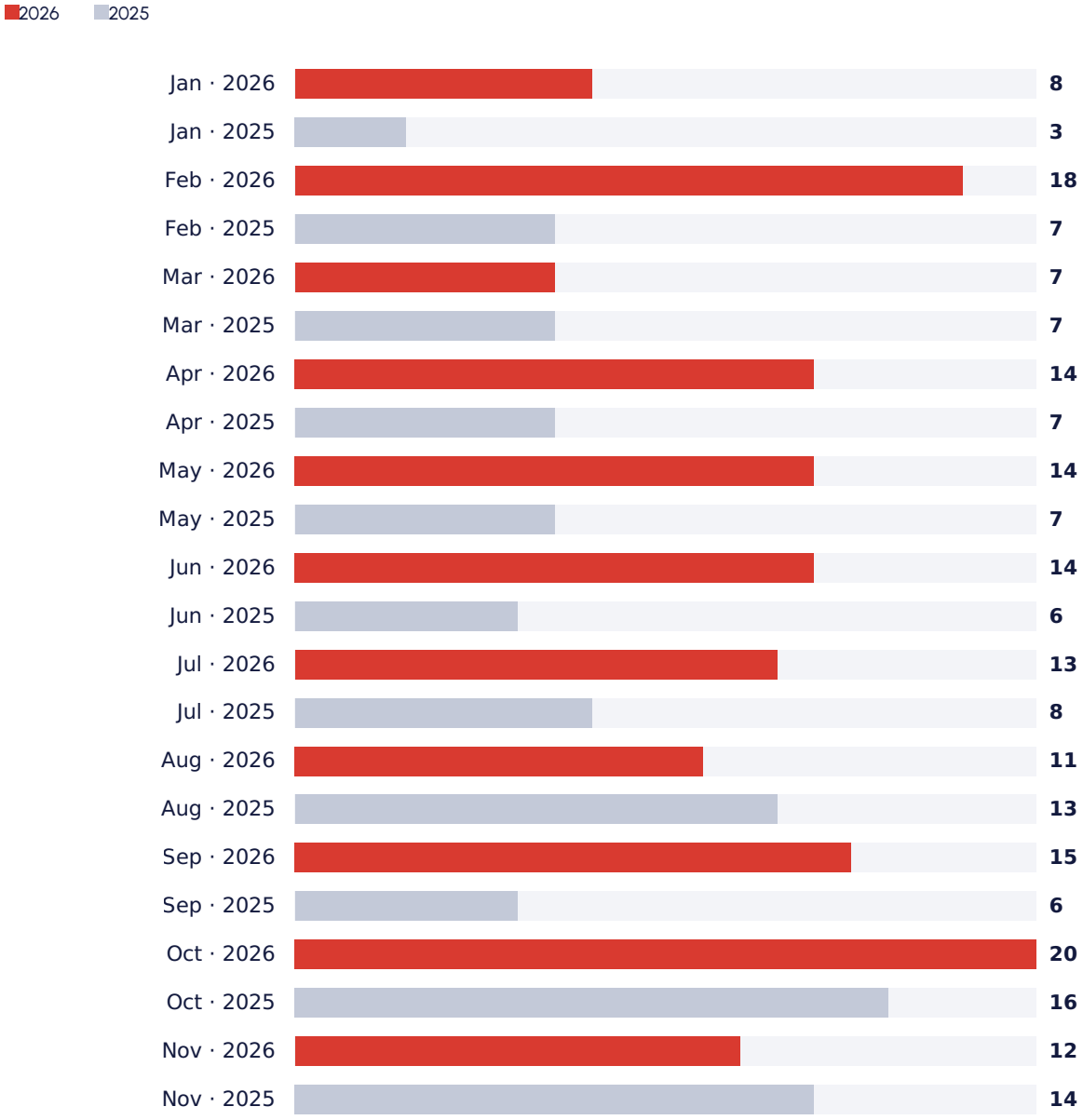
CONFIDENCE

High for retained listings; underlying claims unverified

7.6 Listing sectors and monthly distribution

Figure c10 shows the listing dates. October contributes 20 and the partial November window 12. These dates describe publication in the listing population. They do not establish intrusion dates or a measured month-to-month change in attack frequency. [S2]

Listings appear throughout the year; October has 20 and November is partial



Source: Ransompedia Japan-labelled criminal claims [S2]. January–November in each year; November 2026 covers 1–22 November (closing day partial), while November 2025 is the full month. Not a matched-period growth rate.

The 2025 bars cover full corresponding months. November 2026 is partial.

The broad sector groups below keep smaller categories together. Industry labels remain source descriptions. They do not independently validate the precise activities or corporate boundaries of each listed subject.

Broad sector	Listings	Share
Manufacturing, construction and production	40	27.4%
Other and mixed activity	27	18.5%
Technology and communications	21	14.4%
Transport and travel	19	13.0%
Health	14	9.6%
Education	12	8.2%
Professional services	7	4.8%
Retail and commerce	6	4.1%
Total	146	100.0%

Use the sector view to test relevant continuity needs. Manufacturing and logistics require business and plant involvement. Healthcare needs safe clinical fallbacks. Education and technology organisations should review privileged research and development access. A listing alone does not establish which of those systems was affected.

7.7 Behaviour matrix for the documented delivery chain

This matrix is an analyst mapping of behaviours described by JPCERT/CC to ATT&CK terminology. It is not the source's attribution method or proof that the technique occurred at every Japanese organisation. The source examples support the named behaviours. [S77][S90][S91][S92]

TECHNIQUES NAMED IN THE VENDOR RESEARCH, BY TACTIC

Initial access	Execution	Stealth
T1566.002 Spearphishing link; analyst mapping from JPCERT/CC	T1204.002 Malicious shortcut; analyst mapping from JPCERT/CC	T1218.005 Mshta script activity; analyst mapping from JPCERT/CC

Analyst mapping of source-described behaviour; not a source attribution method or proof at every target. [S77]

Tactic or stage	Behaviour in the source	Defender evidence
Initial access	Spearphishing link to a hosted archive	Original message and download history
Execution	User opens a malicious shortcut from an archive	File-origin and process-creation evidence
Stealth	A standard Windows utility starts embedded script activity	Parent-child process chain and script telemetry
Later-stage delivery (not an ATT&CK tactic)	Later material arrives through legitimate developer services	Destination, process and requested-content context together

Avoid blanket trust in a provider's domain. Also avoid blocking an entire legitimate platform solely because a report describes its abuse. Investigate the account, content and process sequence relevant to the organisation.

7.8 Recent technical advisories require product-specific decisions

JPCERT/CC's 18 November advisory identifies CVE-2026-114938 in accelerated Base64 decoding, including vulnerable OpenJDK builds from 17.0.6 onward. Exploitation requires x86-64 AVX-512 VBMI support and crafted data reaching the vulnerable accelerated path. ARM64 is reported unaffected. [S89]

JPCERT/CC had not confirmed exploitation as of 18 November. This advisory does not establish a Japanese incident. Include bundled runtimes when checking the deployed distribution, full build and operating conditions. [S89]

The table gives affected upstream reference builds and Ubuntu correction examples. Fixed examples separate the base version, patch, build and Ubuntu revision. Verify the deployed distribution and full package revision; bundled runtimes require the application vendor's supported fix. [S249] [S250] [S251]

Branch	Vulnerable reference	Fixed Ubuntu example
OpenJDK 17	17.0.21.0.3	Ubuntu 24.04: openjdk-17 base 17.0.21, patch 1, build 2, revision 1~24.04.1
OpenJDK 21	21.0.13.0.3	Ubuntu 24.04: openjdk-21 base 21.0.13, patch 1, build 2, revision 1~24.04.1
OpenJDK 25	25.0.5.0.3	Ubuntu 24.04: openjdk-25 base 25.0.5, patch 1, build 2, revision 1~24.04.1
OpenJDK 27	27.0.1.0.3	Ubuntu 26.10: openjdk-27 base 27.0.1, patch 1, build 4, revision 1~26.10.1

The application owner should verify the running service after updating. Record its build and configuration, then test service operation before retiring any supported interim measure.

IPA's 20 November PHP notice covers several vulnerabilities with different version, feature and configuration conditions. Its branch-level guidance follows; individual advisories determine applicability. The PHP Group confirms the listed November security releases. [S80] [S252]

PHP branch	Versions requiring review	Fixed release or action
8.1	8.1.34 and earlier in this branch	Migrate to a supported branch or obtain a vendor-supported fix
8.2	Before 8.2.36 in this branch	8.2.36
8.3	Before 8.3.37 in this branch	8.3.37
8.4	Before 8.4.28 in this branch	8.4.28
8.5	Before 8.5.13 in this branch	8.5.13

These branch entries do not mean that every vulnerability affects every listed version. Check vendor backports and embedded products separately. Default settings alone do not establish safety; verify each advisory's conditions and the running application after correction. [S80]

KEY TAKEAWAYS

01

Keep listing labels and source-attributed campaigns separate.

02

Investigate suspicious process and account sequences even when legitimate services are involved.

03

Validate the affected product, build and configuration before declaring a technical advisory resolved.

CHAPTER 08

Fraud targets workflows and delegated access

THIS CHAPTER ANSWERS

How do fraud attempts cross communication channels and delegated access, and where should an organisation interrupt them?

3

control decisions: payment authority, remote access and application consent

8.1 Executive impersonation moves the conversation 91
8.2 A phone call can turn an employee into an access path 91
8.3 Application consent creates another recovery problem 92
8.4 Consumer channels can lead to organizational exposure 93
8.5 Identity retention changes the consequence of a breach 93
8.6 Payment-card observations and their limits 93

CHAPTER 08

Fraud targets workflows and delegated access

IN SHORT

Official Japanese notices describe executive impersonation, bank and tax-service calls, malicious payment apps and cloud consent abuse. These routes cross communication channels and can enlist employees in granting access. The response must cover payment authority, remote-control sessions, application permissions and retained identity records. Require independent verification for payment and access changes, and give employees a fast route to stop suspicious activity.

8.1 Executive impersonation moves the conversation

A familiar name can conceal an unauthorized instruction.

IPA's March warning describes messages using executive or company names. Employees were told to create a LINE group and return its invitation code. Subsequent messages could request transfers while presenting them as business instructions. [S68]

The warning's consultation interval began in December 2025. Its 106 consultations are therefore not a count of 2026 victims. Separately, police recognized 127 executive-impersonation fraud cases with approximately ¥3,880,000,000 in losses during January–June 2026. [S66]

The operational weakness is the transfer of authority between channels. A message arrives through email, creates urgency, then moves discussion into a smaller group where ordinary checks may disappear.

Changing channels should not change the approval requirement. The finance team needs an established route for confirming an unusual instruction with an authorized person. A reply inside the suspicious conversation does not provide that independence.

An organization should also clarify who can authorize a new payment destination, disclose an account balance or create a work group involving finance staff. A senior display name should not waive those rules.

Employees need a practical interruption mechanism. They should be able to pause a transfer, contact a known colleague and report a suspicious request without first resolving whether it is fraudulent.

8.2 A phone call can turn an employee into an access path

The NPA's June notice warns of corporate-bank vishing that combines telephone contact, remote-control software and stolen banking credentials. Criminals can operate the organization's own device while presenting an apparent update. [S67]

IPA's second-quarter report describes a similar consultation involving a supposed tax-service update. A caller obtained an email address, supplied a link and induced installation. Another employee became suspicious and interrupted the interaction. [S69]

These cases show why the incident boundary extends beyond the original call. The organization must consider what the session could access and which accounts were usable from the device. A reassuring update screen is not evidence that activity was benign.

Treat unsolicited requests to install software as changes requiring authorization. Staff should verify the request through a contact already held by the organization. The caller's supplied number or link should not become the verification channel.

If remote control has already occurred, give responders a clear escalation route. Decisions about isolation, evidence preservation, account protection and payment recall need coordination. Staff should not improvise a complete recovery while the session remains active.

The recovery plan should distinguish an observed action from a possible consequence. A remote session establishes an access opportunity. It does not automatically prove that every document, browser secret or financial account was taken.

8.3 Application consent creates another recovery problem

Recovery must include delegated application permissions.

IPA's third-quarter report describes mass mail sent from an employee's Microsoft account after consent was granted to an application. The organization was still investigating the access route and whether information had leaked. [S70]

The case warrants attention because a cloud application can operate through granted permissions. An incident review should therefore examine consent and application activity alongside the account's sign-ins and mail behavior.

IPA recommends reviewing audit and sign-in records, granted permissions, message traces, forwarding and mailbox rules. Its guidance also discusses limiting user consent and using administrative approval for applications. [S70]

For the CISO, this requires a named owner for application access. A service desk may handle account recovery, while a separate administrator controls enterprise applications. The response procedure must connect those responsibilities.

Review whether the application was approved, what it could do and whether its access remains necessary. Closing a user ticket should not leave an unexplained grant active.

This principle also applies to normal administration. Periodic review of delegated access can expose permissions that outlast the project, employee or supplier relationship that justified them. Exceptions should have an owner and a review date.

8.4 Consumer channels can lead to organizational exposure

In September, police warned that malicious smartphone applications could enable remote control and unauthorized transfers through cashless-payment services. Delivery routes included social advertisements, message links and online contacts. [S81]

An organization should consider which business activities depend on employee phones. Payment approvals, account recovery and work communications can share a device with personal applications. The resulting exposure needs a proportionate policy.

The policy should explain permitted installation sources, reporting routes and the treatment of a device suspected of malicious control. Staff should know how to preserve access to essential work without continuing to trust the affected device.

8.5 Identity retention changes the consequence of a breach

PPC's 18 November warning followed an incident at an unnamed rental-car operator where unauthorized access exposed retained photo-ID images. It urged deletion after identity-check use ends and distinguished those images from required licence-number records. [S71]

That distinction gives data owners a concrete review question: does the organization still need the document image, or only a verified attribute and transaction record?

Retention decisions should connect purpose, legal requirements and deletion responsibility. Keeping additional copies for convenience can enlarge the consequences of later unauthorized access.

Avoid treating identity-document possession as proof of a legitimate applicant. The September joint WaterPlum advisory warns that stolen identity images can assist impersonation during fraudulent technology-work recruitment. Authorities attributed that campaign to North Korean actors. [S78]

8.6 Payment-card observations and their limits

SCOPE OF THE CARD FIGURES

This limited population does not establish current validity, unique cardholders, national theft prevalence or fraud losses.

The report contains 303 Japan-associated payment-card observations. Their presence does not establish that a card remains valid, belongs to a current customer or was used in a completed transaction. The observations do not identify a bank intrusion. [S5]

For a relevant authorised alert, the issuer should validate the actual card and account evidence through its normal fraud process. An observation count alone does not justify mass reissuance. Review actual misuse, account status and customer-protection needs before choosing action.

KEY TAKEAWAYS

01

Preserve payment approval and independent verification when a conversation moves between email, telephone and chat.

02

Include remote-control activity and cloud application grants in account-recovery decisions.

03

Remove identity-document images when their purpose ends, using the retention obligations applicable to the organization.

CHAPTER 09

Banking and financial-service dependencies

09

THIS CHAPTER ANSWERS

How should financial institutions distinguish customer fraud, supplier exposure and their own systems?

3

response tracks: transactions, information and service continuity

9.1 Scope of the banking view 96

9.2 Nonproduction systems can retain production harm 96

9.3 Repository access differs from database access 97

9.4 Shared payment services require recipient-specific scope 97

9.5 Customer fraud and account recovery 98

9.6 Supervision and shared exercises 98

CHAPTER 09

Banking and financial-service dependencies

IN SHORT

Financial-sector evidence spans several different events: a retained test environment, development repositories, supplier-hosted payments and customer-facing fraud. A supplier incident does not establish access to every customer's core systems. A data record does not establish an unauthorised transfer. Keep transaction integrity, information disclosure and service availability under separate owners, then connect them when owned evidence supports a common cause.

9.1 Scope of the banking view

The selected banking portfolio contains 25 primary domains. The exposure view has at least 39,061 device associations, including 29 employee-device associations, and 16,437 historical credential-record associations. Current credential listings concern 12 domains. These observations do not establish bank-infrastructure intrusions. [S3]

The banking portfolio covers 25 primary domains. Of these, 22 have device associations not labelled as employee-associated, and 10 have employee-device associations. The former population totals 39,032 associations. It does not establish that the devices belong to customers. [S3]

A small number of the 303 Japan-associated payment-card observations relate to banks in this portfolio. They do not establish a common origin with the credential or device observations. No bank-sector rating is published. [S3] [S5]

The public cases answer different questions. A financial services operator reported exposure in a test environment. A software group's repository disclosure affected development information. A payments-platform incident affected service recipients and required customer-specific checks. None should be relabelled as the same type of bank intrusion. [S31][S28][S12]

The payment-card observations in §8 describe a separate, limited population. They do not count bank customer accounts, corporate credentials or completed fraudulent transactions.

9.2 Nonproduction systems can retain production harm

A financial services operator confirmed unauthorized access to a retained test environment. The findings did not establish compromise of transaction processing. Review retained business data and account access. [S31]

The control lesson is wider than a single environment. A test system can retain real contact, shareholder or customer information and a valid access route long after a project ends. Its lower operational importance does not make its contents low risk.

Require an owner, purpose and end date for nonproduction environments containing real information. Review authentication and access records with the same attention given to the information's sensitivity. Demonstrate deletion or de-identification when the original purpose ends, subject to applicable obligations.

The completion evidence should identify the environment, the retained categories and the access decision. A statement that development is finished does not show that the server, copies or accounts were removed.

9.3 Repository access differs from database access

The financial-software disclosure restricted its personal-information leak assessment to repository contents and stated that production databases were not accessed or leaked. It also distinguished personal information from internal user identifiers. These boundaries must remain in the response account. [S28]

A repository can nevertheless contain information useful for a second step: configuration, integration references, deployment details or secrets. An organisation receiving a relevant supplier alert should determine which of its own integrations could be affected. Rotate only the relevant credentials and verify the result in the receiving service.

Do not turn a supplier's repository incident into an unsupported claim about the institution's transaction database. Ask for the affected repository, information categories and integration scope through authorised channels. Keep any unresolved question visible to the application and supplier owners.

9.4 Shared payment services require recipient-specific scope

A payments provider distinguished affected environments from those eligible for resumption after checks. Recovery decisions require customer-specific evidence. [S12]

A customer should establish its actual product, environment and information flow before copying a platform-wide number into its own notice. Service suspension can be a protective action while facts remain incomplete. Resumption of one recipient does not establish that every recipient has the same status.

Response track	Initial evidence	Completion evidence
Transaction integrity	Authorised payment records, settlement exceptions and relevant access	Reconciled transactions and resolved exceptions
Information disclosure	Applicable product, tenant and data categories	Documented scope and reporting assessment
Service availability	Suspended functions, recipient status and fallback	Business-tested operation and accepted residual limits

The same person or record can appear in several notices concerning a shared service. Downstream disclosures should not be summed into a national total without evidence that their populations are separate. Keep a shared incident reference while retaining each institution's independent duty assessment.

9.5 Customer fraud and account recovery

Customer information can make a fraudulent caller or message more convincing even when it cannot authorise a transaction by itself. Fraud teams should examine the affected workflow: password recovery, contact changes, remote-support requests or payment redirection. The response should address the route actually being abused.

Confirm payment changes through an existing trusted channel. Review recovery decisions that rely on information potentially available in a disclosure. Provide a clear way for customers to verify a warning without following a link supplied by the suspicious message.

Avoid assuming that every transfer reported after a disclosure was caused by that disclosure. Preserve timing, contact details, account actions and other relevant evidence in the institution's authorised case records. Causal claims need more than proximity in time.

FSA's online-trading fraud alert page, initially published in April 2025 and updated on 13 November 2026, emphasises stronger authentication and prompt contact with the relevant institution. [S79]

FSA's 13 November 2026 monthly table tracks provisional broker reports for January 2025–October 2026 and counts unauthorized-access cases and the subset that progressed to unauthorized trading. [S255] Monthly reports peaked in April 2025 at 5,490 unauthorized-access cases and 3,033 cases with unauthorized trading. During January–October 2026, monthly unauthorized-access cases ranged between 18 and 340, with 168 cases and 139 cases with unauthorized trading in October. Cumulative totals across the series reached 19,427 unauthorized-access cases, including 10,782 cases that progressed to trading, while gross transaction values do not represent net customer losses. [S255]

9.6 Supervision and shared exercises

Financial institutions should keep the reporting procedures in §10 current. FSA's 2026 reporting-form change is distinct from the personal-data reporting assessment. A single exercise should test how operations, fraud, privacy and technical response maintain a consistent account while filing through the applicable routes. [S87]

Use a scenario involving a shared platform and uncertain data scope. Require the team to decide whether transactions continue, whether customer information is affected and when an initial report is due. Introduce a later supplier update that changes only one answer.

The exercise succeeds when the owners can explain the distinction and update their decisions. A single status label, such as restored or contained, is insufficient if the customer-information and transaction questions remain unresolved.

KEY TAKEAWAYS

01

Treat retained test data and supplier repositories as separate exposure surfaces.

02

Resolve payment integrity, customer information and continuity through distinct evidence.

03

Keep recipient-specific notices and reporting duties aligned with the actual shared-service scope.

CHAPTER 10

Regulatory response and reporting

10

THIS CHAPTER ANSWERS

Which duties and reporting routes should a Japanese response team prepare?

30 / 60

days for the APPI final report, depending on the reportable event

10.1 Personal-data reporting under APPI 101
10.2 Financial-sector supervision 102
10.3 Cyber-response capability legislation 102
10.4 Retention and the identity-image warning 103
10.5 A reporting pack that can be used early 103

CHAPTER 10

Regulatory response and reporting

IN SHORT

Reporting begins with facts and awareness, not with the end of an investigation. PPC guidance describes reportable personal-data events, prompt initial reporting, final-report deadlines and affected-person notification. Financial institutions also need current supervisory procedures. Specified cyber-response provisions commenced in October, separately from enactment. Prepare a reporting matrix with legal counsel, record awareness times and keep customer protection active while the technical investigation continues.

This is an operational summary, not legal advice.

10.1 Personal-data reporting under APPI

The following table summarises current PPC guidance for private-sector businesses. It describes applicable duties rather than a new 2026 law. The response team must confirm its own legal position and any sector-specific arrangements. [S84]

Requirement	Scope or timing	Response implication
Reportable event	Actual or suspected leakage, loss or damage in the specified categories	Escalate a credible suspected event before final attribution
Specified categories	Sensitive information; likely financial harm; suspected malicious purpose; or more than 1,000 people	Determine information type, risk and affected population separately
Initial regulator report	Promptly; guidance generally indicates about 3–5 days after awareness	Prepare an initial account with known facts and open questions
Final regulator report	Within 30 days; 60 days for suspected malicious acts	Assign an owner for updates and deadline calculation
Affected-person notice	Promptly according to circumstances	Explain relevant facts and protective steps without waiting for every detail

Administrative bodies must assess reporting under PPC's public-sector guidance. Its numerical trigger covers actual or suspected leakage, loss or damage involving more than 100 people. Other reportable categories can apply below that figure. [S253]

For a corporation, PPC guidance uses awareness in any department as the reference point. The initial clock does not wait for the central security team to receive a completed forensic report. Train customer support, fraud, operations and supplier managers to escalate credible evidence promptly. Record what the receiving department knew and when it knew it. [S84]

The reporting categories have qualifications. Relevant security protections can remove an event from the reporting requirement. The applicable authority may be PPC or a delegated competent minister. Where direct affected-person notice is difficult, protective alternative measures can be permitted. These points require a documented assessment rather than an automatic public announcement. [S84]

An outsourced provider may be exempt from direct regulator and affected-person reporting after promptly notifying the responsible client in the circumstances described by the guidance. That does not remove the client's duty. Contracts should establish who supplies the facts and how the client learns about suspected disclosure. [S84]

The indicative 3–5-day guidance is not a safe period in which to postpone internal escalation. Legal and privacy owners should also calculate the final deadline under the actual rules, including applicable calendar treatment. The table is a response aid, not a substitute for that assessment.

10.2 Financial-sector supervision

FSA's cybersecurity guidelines and associated supervisory amendments applied from 4 October 2024. The report treats these as the baseline already in force during 2026. FSA's February 2026 notice states that its further supervisory amendments applied on 27 February, the day of publication. [S85][S86]

FSA announced a further reporting-procedure change on 18 September. The amended supervisory guidance applied from 1 October 2026. Its common forms cover other cyber incidents alongside the existing DDoS and ransomware forms. This procedural change is separate from APPI's reporting triggers and deadlines. [S87]

Item	Date distinction	Preparation
Cybersecurity guideline baseline	Applied 4 October 2024	Check the current applicable guideline and supervisory text
Further supervisory amendments	Published and applied 27 February 2026	Confirm the provisions relevant to the institution
Common reporting forms	Announced 18 September; applied 1 October 2026	Replace superseded templates in the response playbook

The announcement establishes dates and procedural scope. It does not, by itself, support prescribing a particular control as mandatory for every Japanese business. Financial institutions should map the detailed applicable guidance to their services, outsourced operations and management responsibilities.

10.3 Cyber-response capability legislation

The Cabinet Office account confirms commencement of specified provisions on 1 October 2026. The provisions concern stronger public-private cooperation and access/neutralization measures. Other dates and legal provisions should not be inferred from that statement. [S88]

For a business, the immediate task is an applicability review. Identify whether its services fall within relevant designated or sector arrangements. Confirm the correct authority route and information-sharing contact. Maintain a separate privacy analysis when personal information may be involved.

The report describes the official framework without endorsing or opposing government policy. It does not infer that the legislation authorises a private organisation to investigate or interfere with systems it does not own. Defensive testing should remain within the organisation's authorised environment.

10.4 Retention and the identity-image warning

PPC's 18 November advisory reports a rental-car operator's stored photo-ID images being leaked following external unauthorised access. It urges deletion after the verification purpose ends. The advisory distinguishes recording a licence number for two years from retaining an image after the rental procedure. [S71]

This is not a blanket retention deadline for every document in every industry. It is a concrete reason to review whether image copies remain necessary. The data owner should identify the purpose, applicable duty, supplier copies and deletion evidence for each retained category.

10.5 A reporting pack that can be used early

Prepare a short reporting pack before an incident. Keep its facts consistent across regulators, customers, police and suppliers while recognising that each route can require different information.

Field	Initial content	Update owner
Awareness	First credible evidence and receiving department	Incident coordinator
Service impact	Confirmed unavailable functions and fallback	Business operations
Information	Confirmed or suspected categories and affected scope	Data owner and privacy
Containment	Actions taken, evidence preserved and remaining access	Technical response
Reporting	Applicable route, trigger, deadline and next update	Legal and compliance

Do not fill unknown fields with a criminal post's claimed numbers. Preserve the assertion as a lead. Explain the difference between a reported outage, suspected access and confirmed disclosure. A later update can narrow or expand the account without rewriting the initial awareness record.

JPCERT/CC's 18 November investigation-report checklist asks readers to connect conclusions to evidence, understand exclusions and log gaps, and link remediation to findings. A report should support the next decision rather than merely describe an incident as closed. [S76]

KEY TAKEAWAYS

01

Record awareness across departments and escalate suspected reportable events promptly.

02

Keep APPI duties separate from financial-sector reporting procedures.

03

Review retained identity images and document why each copy remains necessary.

CHAPTER 11

Outlook and conditional scenarios

11

THIS CHAPTER ANSWERS

Which developments justify preparation, and what would change the assessment?

4

planning scenarios with observable triggers

11.1 Key judgements 106
11.2 Supplier service interruption 106
11.3 Credential or session misuse 107
11.4 Information-enabled customer fraud 107
11.5 Operational-system exposure 107
11.6 Signals to revisit 108

CHAPTER 11

Outlook and conditional scenarios

IN SHORT

The evidence supports preparation for supplier disruption, account misuse, information-enabled fraud and operational-system exposure. It does not support a numerical forecast of Japanese attacks or losses. Each scenario below has a trigger and an owner. Use the scenarios to test decisions that can be rehearsed now, then change the response when owned evidence confirms a different scope.

11.1 Key judgements

Confidence here attaches to a stated proposition. It is not a probability of a future incident, a rating of a country or a general judgement about an actor.

Judgement	Confidence and basis	What would change it
Supplier incidents require customer-specific decisions	High for the operational lesson from the public cases	A supplier's validated scope showing the service or information is unaffected
Account and integration evidence needs rapid validation	High for the response need; individual alerts remain unverified	Owned logs, account state and remediation records resolving the alert
Retained identity information can extend harm beyond restoration	High for the risk mechanism and PPC's warning	Verified deletion or an assessed disclosure scope excluding the material
Public claims do not establish physical-process access	High for this evidence boundary	Engineering records or the operator's confirmed assessment of process changes

These judgements remain useful when individual incident counts change. They identify which evidence to seek and which function should decide. They should not be converted into a national ranking or a claim that every supplier, employee or customer is affected.

11.2 Supplier service interruption

Planning assumption. A shared business platform becomes unavailable while its provider investigates unauthorised access. Some customers need only a service fallback. Others also need an information or integration review. Restoration dates can change as the investigation develops.

Trigger. An official supplier notice identifies the organisation's product, tenant or integration as potentially affected. The service owner confirms the dependency through the contract or technical inventory.

Decision. Activate the minimum service route. Preserve the supplier's notices and the organisation's own transaction evidence. Ask separately about customer information, historical contracts and credentials that permit access to another system.

Closure. The business owner demonstrates the service, the security owner resolves privileged access and the privacy owner records the information assessment. A provider's general status message alone does not complete all three decisions.

11.3 Credential or session misuse

Planning assumption. A relevant alert or disclosure identifies an account, key or session associated with an owned service. Its current validity and scope are initially unknown. Historical information may be involved without continued access.

Trigger. The identity owner verifies that the account or integration belongs to the organisation. Logs, privileges and prior remediation are available for review.

Decision. Prioritise active privileged access and cross-system keys. Revoke relevant sessions or credentials when the evidence warrants it. Review account changes and exports, then extend the investigation only where the evidence leads.

Closure. The account has a recorded disposition, necessary revocation is verified and the owner has reviewed affected service activity. A password change does not establish that every existing session or integration was removed.

11.4 Information-enabled customer fraud

Planning assumption. Disclosed contact, booking, identity or transaction information is used to make a later fraudulent message believable. Technical restoration does not remove information already disclosed.

Trigger. The data owner confirms relevant disclosure or customer operations records credible messages using the affected information. A seller's claim alone remains an investigation lead.

Decision. Give customer support a plain warning and an authenticated help route. Strengthen recovery checks and payment-change verification for the affected workflow. Coordinate any notice with legal and privacy owners.

Closure. Support can recognise the scenario, customers have usable protective instructions and fraud monitoring has an accountable owner. Evaluate the measures against observed misuse rather than a claim that all future fraud has been prevented.

11.5 Operational-system exposure

Planning assumption. A public claim or official advisory raises concern about remotely reachable industrial equipment. Website availability, an interface screenshot and a physical-process change are different kinds of evidence.

Trigger. Plant operations confirms that a relevant asset or maintenance path exists in its environment. A safety concern is escalated through established engineering procedures.

Decision. Validate process readings, review remote access and remove unnecessary direct exposure using an approved change. Preserve the change history. Keep any response proportionate to the safety and availability requirements of the equipment.

Closure. Operations verifies the physical state, access is limited to approved routes and a responsible engineer signs off the result. A general IT account reset does not resolve an unreviewed industrial maintenance path.

11.6 Signals to revisit

Revisit these scenarios when a provider changes its affected-product list, a regulator issues a new requirement or owned logs establish a wider access path. Keep the original assessment and document why the decision changed. Changes in public posting volume alone do not establish changes in attack frequency.

KEY TAKEAWAYS

01

Use conditional scenarios to rehearse decisions, not to predict national attack totals.

02

Give identity, service continuity and customer protection separate closure evidence.

03

Reassess when owned evidence or an authoritative update changes the scope.

CHAPTER 12

Action plan

12

THIS CHAPTER ANSWERS

Who should act, in what order, and what demonstrates completion?

30 / 60 / 90

day checkpoints for an owned response programme

12.1 Thirty, sixty and ninety days 110
12.2 Role-specific starting points 112
12.3 A small management scorecard 112
12.4 How Brandefense can help 113

CHAPTER 12

Action plan

IN SHORT

Begin with evidence routes, active identity exposure and the services that must continue. Next test supplier and customer workflows, including historical data and integration credentials. Then demonstrate recovery and management oversight through exercises. The schedule is a planning framework, not an asserted legal deadline. Give every action an owner and require evidence that another team can review.

12.1 Thirty, sixty and ninety days

The lanes below describe recommended checkpoints. An active incident, safety issue or applicable reporting duty can require immediate action. Teams should adjust the schedule to their verified exposure and service dependencies.

1Days 1–30		
Establish routes for relevant credential, supplier and criminal-claim alerts	OWNER CISO and service desk	COMPLETION EVIDENCE Named receiving team, escalation criteria and a tested example
Validate alerts tied to owned accounts; prioritise active privileged access	OWNER Identity and incident response	COMPLETION EVIDENCE Ownership, freshness, privileges and disposition recorded
Revoke relevant sessions or keys when validation warrants containment	OWNER Identity and application owners	COMPLETION EVIDENCE Revocation verified in the affected service
Record awareness and reporting routes for suspected personal-data incidents	OWNER Legal, privacy and compliance	COMPLETION EVIDENCE Current matrix, forms, clocks and a tabletop awareness timeline
Map critical services to hosting, identity and business-platform suppliers	OWNER Procurement and operations	COMPLETION EVIDENCE Service dependency, data categories, privilege and fallback owner

Review unnecessary direct access to industrial interfaces

OWNER

Plant operations and OT security

COMPLETION EVIDENCE

Approved access route and engineering sign-off

Check owned exposed products against applicable vendor advisories

OWNER

Infrastructure and application owners

COMPLETION EVIDENCE

Affected-version decision, remediation and verification record

2Days 31–60

Test a critical supplier outage with an alternate operating route

OWNER

Business continuity and service owner

COMPLETION EVIDENCE

Demonstrated minimum service and recorded recovery obstacles

Review old integration credentials and ended-contract access

OWNER

Application owners and procurement

COMPLETION EVIDENCE

Necessary access approved; obsolete access demonstrably removed

Review retention of identity images and other high-harm information

OWNER

Data owners and privacy

COMPLETION EVIDENCE

Purpose, legal basis, retention decision and deletion evidence

Exercise a believable customer-fraud message using a disclosed data category

OWNER

Fraud, support and communications

COMPLETION EVIDENCE

Authenticated help route and staff response demonstrated

Review email authentication and legitimate sending services

OWNER

Messaging and domain owners

COMPLETION EVIDENCE

Sending inventory and evidence of policy validation

3Days 61–90

Restore a critical service in an isolated environment

OWNER

Infrastructure and business owner

COMPLETION EVIDENCE

Restore test, data integrity checks and business acceptance

Rehearse a claim with disputed impact and a later scope update

OWNER

Communications, legal and incident response

COMPLETION EVIDENCE

Separate claim, confirmed facts, unknowns and next-update statement

Review unresolved identity, supplier and retention decisions with management

OWNER

CISO and accountable executives

COMPLETION EVIDENCE

Accepted risk or funded corrective action with a review date

12.2 Role-specific starting points

Board and executives. Ask which service can continue without its normal supplier or identity platform. Require a demonstration rather than a list of policies. Review unresolved decisions that need funding, contractual support or risk acceptance.

CISO and incident response. Maintain one evidence account with separate claim, service, information and process assessments. Ensure that staff can escalate partial information. Review whether an alert was resolved by evidence or merely closed because its origin was uncertain.

SOC and identity teams. Validate the owned account and access path before widening containment. Inspect administrative changes, session grants, export activity and integrations where relevant. Preserve enough evidence to explain both the action taken and its limits.

Infrastructure and operations. Confirm the version and exposure of owned systems covered by current advisories. Test restoration and fallback paths. In industrial environments, coordinate security changes with engineers who understand physical safety and process availability.

Fraud and customer support. Identify which disclosed information would make an impersonation persuasive. Give staff a consistent way to verify customers without relying on that information alone. Confirm payment changes through a previously known channel.

Legal, privacy and compliance. Keep awareness, applicable triggers and reporting decisions contemporaneous. Separate preliminary facts from final scope. Coordinate supplier notifications while retaining responsibility for the organisation's own duties.

12.3 A small management scorecard

Use measures that show completed decisions. Avoid reporting the number of alerts reviewed as evidence that risk disappeared.

Measure	Evidence of progress	Escalation point
Relevant identity alerts	Owned accounts have a justified disposition	Active privileged access remains unresolved
Critical supplier coverage	Dependency and fallback are demonstrated	A service has no usable alternate route
High-harm data retention	Each category has a current purpose and retention decision	Images or copies remain without an accountable owner
Reporting readiness	Awareness and initial-notice exercise completed	Teams disagree about when escalation begins
Recovery readiness	Business owner accepts an actual restoration test	Technical restoration cannot support minimum service

12.4 How Brandefense can help

Brandefense combines Cyber Threat Intelligence, Digital Risk Protection and External Attack Surface Management. For this report, the relevant use is to connect external alerts to an owned decision: validate an account, assess a claim, review a supplier or investigate an exposed service.

The report's aggregate observations do not identify the reader's active accounts or prove an intrusion. A useful engagement begins with the organisation's authorised domains, service dependencies and response owners. It should end with evidence that those owners can assess and act on.

Discuss the relevant monitoring and response scope with Brandefense. The organisation retains responsibility for validation, containment, reporting and business decisions.

KEY TAKEAWAYS

01

Start with owned accounts, reporting routes and critical service dependencies.

02

Require demonstrated fallback, retention and recovery decisions at the next checkpoints.

03

Close actions with evidence an accountable business owner can review.

APPENDICES

Appendices

A–D

THIS CHAPTER ANSWERS

What do the populations and evidence labels permit a reader to conclude?

2026

the main observation window; historical context is labelled separately

Appendix A. Scope and evidence boundaries 115
Appendix B. Evidence register 119
Appendix C. Sources 124
Appendix D. Glossary 134

Appendix A. Scope and evidence boundaries

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

A.1 Window and dates

The main window is 1 January–22 November 2026. Underground material uses posting time. The recent-activity view covers 8–22 November. Public accounts can describe earlier activity, later detection and a current update; those dates remain separate.

The cut-off day was in progress during review. This is not a completed end-of-day census. Historical laws, older incident material and earlier-year statistics appear only with their periods stated. A new publication does not establish a new intrusion.

A.2 Source populations

The source categories have different units and coverage. They should be read beside their chapter-level limitations.

Population	Unit	Boundary
Underground observations	Retained posts	Not unique advertisements, verified incidents or affected people
Ransomware listings	Criminal listings	Not verified encryption, extraction, payment or unique organisations
Selected organisation set	Primary-domain entries	Not independent corporate groups or a national sample
DNS observations	Assessed domains and policies	Not delivery effectiveness or complete application security
Public incident accounts	Source-scoped disclosures and research	Not a national incident census
Official statistics	The authority's defined reports or cases	Only the stated period and population
Payment-card view	Payment-card observations	Not national card theft or fraud loss

Atlas supplies the national headline of 51/100 (B) for 250 selected domains as of 22 November 2026. Anonymous sector aggregates describe the observed signals; no sector or organisation ratings are published. Historical credential records are cumulative and can overlap across domains. The listing-history period and overlap with current listings are unspecified. [S3]

DNS-policy observations cover 250 domains. The edition has no complete TLS, homepage-header or combined hygiene-index dataset. Missing observations are unknown. [S4]

The payment-card observations concern a limited population. They do not establish current validity, unique cardholders, national theft prevalence or fraud losses. [S5]

A.3 Evidence language and confidence

An observation establishes what a retained source contains. A criminal claim is an assertion within that source. External corroboration can support a specific proposition, such as an organisation confirming access or disruption. An analyst inference explains a possible consequence without upgrading the underlying claim.

Confidence attaches to that proposition. Confidence that an advertisement exists is not confidence in its contents. A detailed schema, a claimed sample, a price or a familiar alias does not authenticate a file. An absence of confirmation is also not proof that a claim is fabricated.

Official investigations can change scope. A finding of no observed extraction has a different meaning from proof that extraction was impossible. The report retains qualifications, logging limits and later revisions where the source provides them.

A.4 Relationships and scenarios

Map edges identify their supporting source and relationship type. Own listing data, official statements and public research remain separate. A source reporting on an actor does not establish a relationship between that actor and another campaign in the map.

Similar advertising can establish repeated wording. It does not establish identical files, a sale, an original intruder or a common operator. An unsupported broader grouping would be an analytical model. Conditional scenarios in Chapter 11 are planning assumptions with triggers and closure evidence.

A.5 Naming and public scope

An incident subject is named only where an official confirmation and wider reporting support that use. Other subjects receive broad roles. Citation titles follow the same boundary. Withheld subjects are cited without an address. A press or neutral disclosure platform may retain its root address, without the article URL.

State and political attributions remain their sources' assessments. No nationality is inferred from language or infrastructure location. The report takes no position on territorial disputes, historical controversies, elections or government decisions.

A.6 Coverage limits

Visible posts and public disclosures cover only part of the threat environment. Private sales, unpublished incidents and unavailable original notices remain outside the account. Country and sector labels can be inaccurate. The report does not infer national prevalence or attack probability from its selected populations.

The 26 case cards and 11 additional accounts are editorial units. They include unverified offers, evolving organisational disclosures and campaign research. They do not define a common incident-count denominator. Source-specific limits remain beside the relevant account.

APPENDICES

Appendices

A–D

THIS CHAPTER ANSWERS

Where does each public card or detailed account appear?

12

redacted underground post cards

Appendix A. Scope and evidence boundaries 115

Appendix B. Evidence register 119

Appendix C. Sources 124

Appendix D. Glossary 134

Appendix B. Evidence register

B.1 Post cards

The card IDs are stable across editions. Dates are post dates, and aliases with contact value are withheld. The excerpts establish assertions rather than authenticated datasets. [S1]

Card	Date	Venue	Alias	Language	Chapter
B01	2026-11-18	Forum	Withheld	English	4
B02	2026-11-16	Forum	Withheld	Japanese	4
B03	2026-11-06	Forum	Withheld	English	4
B04	2026-03-02	Forum	Withheld	English	4
B05	2026-02-03	Forum	Withheld	English	4
B06	2026-08-22	Forum	Withheld	English	4
B07	2026-01-13	Forum	Withheld	English	4
B08	2026-11-05	Forum	Withheld	English	4
B09	2026-05-13	Forum	Withheld	English	4
B10	2026-01-01	Forum	Withheld	Chinese	4
B11	2026-11-14	Forum	Withheld	English	4
B12	2026-11-15	Forum	Withheld	English	4

B.2 Detailed accounts

The first 6 case cards concern underground claims. The next 20 concern public disclosures. Another 11 detailed accounts cover additional disclosures and campaign research. Revisions and downstream effects remain part of their stated source account rather than an automatically new intrusion.

ID	Subject or assertion	Evidence	Chapter
A	Description and schema mismatch	Unverified post claim; B02	4
B	Staged disclosure narrative	Unverified post claim; B03	4
C	Purported bank vulnerability offer	Unverified post claim; B04	4
D	Sports registration data offer	Unverified post claim; B05	4

ID	Subject or assertion	Evidence	Chapter
E	Source-code redistribution claim	Unverified post claim; B06	4
F	Insurance data offer	Unverified post claim; B09	4
G	RIKEN: external credentials widened the response	Source-scoped public account [S6][S7]	5
H	IDC Frontier: encryption disrupted shared cloud capacity	Source-scoped public account [S8][S9]	5
I	PLAID: a customer platform faced an extended interruption	Source-scoped public account [S10][S11]	5
J	A payments provider: recovery required separate decisions	Source-scoped public account [S12][S13]	5
K	Nitori: a large possible exposure remained qualified	Source-scoped public account [S14][S15]	5
L	An education institution: supplier exposure and disruption differed	Source-scoped public account [S16]	5
M	Times Car: identity-image findings changed the response	Source-scoped public account [S17][S18]	5
N	KDDI: corrected mail-platform figures superseded the first estimate	Source-scoped public account [S19][S20]	5
O	Aflac Japan: bulk queries required a separate detection response	Source-scoped public account [S21][S22]	5
P	Nippon Medical School Musashikosugi Hospital: a nurse-call system carried sensitive information	Source-scoped public account [S23][S24]	5
Q	Advantest: later notification confirmed extraction	Source-scoped public account [S25][S26][S27]	5
R	Money Forward: copied repositories differed from production access	Source-scoped public account [S28][S29]	5
S	An online platform: incomplete logs constrained the conclusion	Source-scoped public account [S30]	5

ID	Subject or assertion	Evidence	Chapter
T	A financial services operator: retained test data created exposure	Source-scoped public account [S31]	5
U	A manufacturer: external transmission did not resolve file scope	Source-scoped public account [S32]	5
V	Nihon Kotsu: operational and historical records had different scopes	Source-scoped public account [S33][S34][S35]	5
W	A transport operator: business applications held personal information	Source-scoped public account [S36]	5
X	A technology provider: investigate environments separately	Source-scoped public account [S37]	5
Y	BOOKOFF: a confirmed leak and corrected field list	Source-scoped public account [S38][S39]	5
Z	ANA: provider records included different passenger-data tiers	Source-scoped public account [S40][S41]	5
AA	OpJapan: attack claims remained different from proven outages	Source-scoped public account [S42][S43]	5
AB	CoGUI: disruption targeted a phishing ecosystem focused on Japan	Source-scoped public account [S44][S45]	5
AC	A manufacturer: ransomware halted production	Source-scoped public account [S46]	5
AD	Rakuten Securities: test-system scope involved two account categories	Source-scoped public account [S47][S48][S49]	5
AE	Monex: onboarding documents remained a supplier-side concern	Source-scoped public account [S50][S51]	5
AF	SBC Medical: customer history and staff records had overlapping scope	Source-scoped public account [S52][S53][S54]	5
AG	Rokkatei: a payment page exposed data without storing cards	Source-scoped public account [S55][S56]	5
AH	Arara: an address count required careful interpretation	Source-scoped public account [S57][S58]	5

ID	Subject or assertion	Evidence	Chapter
AI	A messaging provider: shared-platform exposure reached customers	Source-scoped public account [S59][S60][S61]	5
AJ	GMO Internet: hosted desktops carried trading-session risk	Source-scoped public account [S62][S63][S64]	5
AK	A consumer app: usage information required protection	Source-scoped public account [S65]	5

B.3 Map and behaviour matrix

The map's own-data edges describe listing presence. Official edges connect authorities to their reported campaign. Public-reporting edges connect vendor research to the labels it discusses. No edge establishes a shared operator across all the nodes. [S2][S77][S78][S42][S44]

The behaviour matrix maps described actions to ATT&CK terminology as analysis. It is not a source's attribution method. Initial-access, execution and stealth labels apply to the mapped behaviours, not to every incident in Japan. [S90][S91][S92]

APPENDICES

Appendices

A–D

THIS CHAPTER ANSWERS

Which source supports each cited proposition?

2026

observation cutoff 22 November; sources verified on 22–23 November

Appendix A. Scope and evidence boundaries 115
Appendix B. Evidence register 119
Appendix C. Sources 124
Appendix D. Glossary 134

Appendix C. Sources

Source numbers that do not appear were retired during review and are not cited. The observation window closes on 22 November 2026, while source verification continued through 23 November 2026. Own-source entries describe the report's retained evidence. External entries identify material read at its source. Withheld subjects are cited without an address. A retained press or disclosure-platform root does not substitute for the supporting article.

S1: Odin by Brandefense. Retained Japan-related underground post observations. Own retained evidence. Verified on 2026-11-22.

S2: Ransompedia. Japan and four regional-peer ransomware listing aggregates. Own retained evidence. Verified on 2026-11-22.

S3: Atlas. Selected Japan organisation exposure snapshot and national headline. Own retained evidence. Verified on 2026-11-22.

S4: Odin by Brandefense. Public DNS policy observations for selected Japanese domains. Own retained evidence. Verified on 2026-11-22.

S5: Odin by Brandefense. Japan-associated payment-card observations. Own retained evidence. Verified on 2026-11-22.

S6: RIKEN. Investigation update, second report. https://www.riken.jp/pr/news/2026/20261120_1/index.html. Verified on 2026-11-22.

S7: news.tv-asahi.co.jp. TV Asahi reports Fugaku unauthorized access. https://news.tv-asahi.co.jp/news_society/articles/000548214.html. Verified on 2026-11-22.

S8: IDC Frontier. IDCF seventh report: investigation results and response. https://www.idcf.jp/news/topics/20261027001. Verified on 2026-11-22.

S9: itmedia.co.jp. IDCF ransomware affects 495 corporate and municipal customers. https://www.itmedia.co.jp/news/article/2610/07/2000002107/. Verified on 2026-11-22.

S10: PLAID. KARTE investigation results and service-restart outlook. https://plaid.co.jp/news/20261120/. Verified on 2026-11-22.

S11: watch.impress.co.jp. KARTE inquiry complete, restart targeted for January 2027. https://www.watch.impress.co.jp/docs/news/2158411.html. Verified on 2026-11-22.

S12: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S13: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S14: Nitori. Nitori notice of potential personal-information leakage. https://www.nitorihd.co.jp/news/items/2b702dbe4d438f7fef74945d68e5bd27_3.pdf. Verified on 2026-11-22.

S15: watch.impress.co.jp. Nitori possible 37.62 million-record leak. https://www.watch.impress.co.jp/docs/news/2154952.html. Verified on 2026-11-22.

S16: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S17: Times Car. Times Car fifth report and revised scope. https://park24.co.jp/news/2026/10/20261023-1.html. Verified on 2026-11-22.

S18: ascii.jp. Times Car fifth report covered by ASCII. https://ascii.jp/elem/000/004/445/4445381/. Verified on 2026-11-22.

S19: KDDI. KDDI July6 report, corrected July21. https://newsroom.kddi.com/news/assets/2026/kddi_nr_s-73_4619/kddi_nr_s-73_4619_pdf_01.pdf. Verified on 2026-11-22.

S20: k-tai.watch.impress.co.jp. MIC administrative guidance after ISP mail incident. https://k-tai.watch.impress.co.jp/docs/news/2129178.html. Verified on 2026-11-22.

S21: Aflac Japan. Aflac incident FAQ updated November13. https://www.aflac.co.jp/info/yorisou_faq.html. Verified on 2026-11-22.

S22: bleepingcomputer.com. Aflac discloses Japan subsidiary breach. https://www.bleepingcomputer.com/news/security/insurance-giant-aflac-discloses-data-breach-after-subsidiary-hack/. Verified on 2026-11-22.

S23: Nippon Medical School Musashikosugi Hospital. Hospital fifth report with revised scope and route. https://www.nms.ac.jp/kosugi-h/news/_28850.html. Verified on 2026-11-22.

S24: news.tv-asahi.co.jp. National TV report of ransomware and initial patient leak. https://news.tv-asahi.co.jp/news_society/articles/000485236.html. Verified on 2026-11-22.

S25: Advantest. Advantest October6 notice filed with California AG. https://oag.ca.gov/system/files/Advantest%20Corporation%20-%20Notice%20of%20Data%20Breach%20-%20Individual%20Letter.pdf. Verified on 2026-11-22.

S26: Advantest. Advantest responds to cybersecurity incident. https://www.advantest.com/en/news/2026/20260219.html. Verified on 2026-11-22.

S27: bleepingcomputer.com. Advantest confirms information theft. https://www.bleepingcomputer.com/news/security/advantest-confirms-personal-information-stolen-in-ransomware-attack/. Verified on 2026-11-22.

S28: Money Forward. GitHub detailed investigation complete, fourth report. https://corp.moneyforward.com/news/info/20260623-mf-press-1/. Verified on 2026-11-22.

S29: itmedia.co.jp. Money Forward production-database assessment. https://www.itmedia.co.jp/news/article/2605/11/1260511106/. Verified on 2026-11-22.

S30: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S31: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S32: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S33: Nihon Kotsu. Sixth notice with affected groups. https://www.nihon-kotsu.co.jp/news/20261030-3479/. Verified on 2026-11-22.

S34: Nihon Kotsu. Initial unauthorized-access and system-suspension notice. https://www.nihon-kotsu.co.jp/news/20260713-3334/. Verified on 2026-11-22.

S35: internet.watch.impress.co.jp. Nihon Kotsu confirms some file leakage. https://internet.watch.impress.co.jp/docs/news/2133999.html. Verified on 2026-11-22.

S36: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S37: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S38: BOOKOFF. BOOKOFF third report, linked from corporate news page. https://ssl4.eir-parts.net/doc/9278/tdnet/2906882/00.pdf. Verified on 2026-11-22.

S39: game.watch.impress.co.jp. BOOKOFF begins individual breach notices. https://game.watch.impress.co.jp/docs/news/2148433.html. Verified on 2026-11-22.

S40: ANA. ANA notice on reservation-system-provider access. https://www.ana.co.jp/ja/jp/special-notice/001612.html?p1=top&p2=ja&p3=global. Verified on 2026-11-22.

S41: news.tv-asahi.co.jp. ANA confirms provider incident. https://news.tv-asahi.co.jp/news_economy/articles/000543786.html. Verified on 2026-11-22.

S42: blog.checkpoint.com. Check Point: renewed OpJapan claim wave. https://blog.checkpoint.com/exposure-management/noname05716-renews-opjapan/. Verified on 2026-11-22.

S43: s2w.inc. S2W February third-week claim report. https://s2w.inc/ja/resources/1022. Verified on 2026-11-22.

S44: proofpoint.com. Proofpoint: Japanese-focused phishing-kit disruption. https://www.proofpoint.com/us/blog/threat-insight/disruption-targets-major-chinese-language-phishing-kits-japanese-focus. Verified on 2026-11-22.

S45: CoGUI phishing disruption. Microsoft DCU action docket. https://www.microsoft.com/en-us/corporate-responsibility/customer-security-trust/digital-crimes-unit/notice-of-pleadings/yam-cogui-ironman/. Verified on 2026-11-22.

S46: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S47: Rakuten Securities. Unauthorized access and possible test-system information leak. https://www.rakuten-sec.co.jp/web/info/info20261117-02.html. Verified on 2026-11-22.

S48: Rakuten Securities. Corporate notice of Financial Services Agency reporting order. https://www.rakuten-sec.co.jp/web/company/newsrelease/pdf/press2026111901.pdf. Verified on 2026-11-22.

S49: watch.impress.co.jp. Rakuten Securities test-environment disclosure. https://www.watch.impress.co.jp/docs/news/2157207.html. Verified on 2026-11-22.

S50: Monex. Monex corporate interim report PDF. https://prtimes.jp/a/?c=5159&f=d5159-595-9f0a3826f4b4d2d6569f7c0693728a0b.pdf&r=595. Verified on 2026-11-22.

S51: news.tv-asahi.co.jp. National television reports Monex contractor incident. https://news.tv-asahi.co.jp/news_economy/articles/000547701.html. Verified on 2026-11-22.

S52: SBC Medical Group. SBC corporate Japan incident notice. https://prtimes.jp/main/html/rd/p/000000416.000097803.html. Verified on 2026-11-22.

S53: SBC Medical Group. Group notice of Japan cybersecurity incidents. https://ir.sbc-holdings.com/ja/sbc-medical-group-reports-cybersecurity-incidents-in-japan/. Verified on 2026-11-22.

S54: itmedia.co.jp. SBC incident scope and separate clinic-management access. https://www.itmedia.co.jp/news/article/2611/20/2000003355/. Verified on 2026-11-22.

S55: Rokkatei. Online-shop incident second notice. https://www.rokkatei.co.jp/news/info/20261121-25796/. Verified on 2026-11-22.

S56: itmedia.co.jp. Rokkatei online-shop card exposure notice. https://www.itmedia.co.jp/news/article/2611/19/2000003316/. Verified on 2026-11-22.

S57: Arara. Messaging-platform incident third report. https://www.arara.com/dcms_media/other/arara_20261106.pdf. Verified on 2026-11-22.

S58: news.tv-asahi.co.jp. National report on Arara messaging incident. https://news.tv-asahi.co.jp/news_economy/articles/000545959.html. Verified on 2026-11-22.

S59: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S60: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S61: FNN. Incident notice. https://www.fnn.jp/ (article URL withheld). Verified on 2026-11-22.

S62: GMO Internet. Hosted desktop incident third report. https://internet.gmo/news/article/248. Verified on 2026-11-22.

S63: GMO Internet. Hosted desktop incident fifteenth report. https://internet.gmo/news/article/261/. Verified on 2026-11-22.

S64: itmedia.co.jp. GMO response to actor threats and customer endpoint impact. https://www.itmedia.co.jp/news/article/2610/27/2000002624/. Verified on 2026-11-22.

S65: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S66: National Police Agency. 令和８年上半期におけるサイバー空間をめぐる脅威の情勢等について. https://www.npa.go.jp/publications/statistics/cybersecurity/data/R8kami/R08_kami_cyber_jousei.pdf. Verified on 2026-11-22.

S67: National Police Agency. 巧妙化するボイスフィッシング被害に注意. https://www.npa.go.jp/bureau/cyber/pdf/R8_Vol.6cpal.pdf. Verified on 2026-11-22.

S68: IPA. 社長等をかたる詐欺メールに注意. https://www.ipa.go.jp/security/anshin/attention/2025/mgdayori20260312.html. Verified on 2026-11-22.

S69: IPA. サイバーセキュリティ相談窓口の相談状況2026年第2四半期. https://www.ipa.go.jp/security/support/reports/2026q2outline.html. Verified on 2026-11-22.

S70: IPA. サイバーセキュリティ相談窓口の相談状況2026年第3四半期. https://www.ipa.go.jp/security/support/reports/2026q3outline.html. Verified on 2026-11-22.

S71: PPC. 運転免許証等の顔写真付きの公的身分証明書の画像の消去について. https://www.ppc.go.jp/files/pdf/261118_houdou.pdf. Verified on 2026-11-22.

S72: National Police Agency. 家庭用IoT機器を悪用するレジデンシャルプロキシの現状. https://www.npa.go.jp/bureau/cyber/pdf/20260721-1_residentialproxy.pdf.pdf. Verified on 2026-11-22.

S73: JPCERT/CC. 直近で相次いでいる国内組織における不正アクセスに関する注意喚起. https://www.jpcert.or.jp/at/2026/at260030.html. Verified on 2026-11-22.

S74: National Police Agency. マイクロソフト・ＪＣ３と連携した犯罪インフラのテイクダウンについて. https://www.npa.go.jp/bureau/cyber/pdf/20261015.pdf. Verified on 2026-11-23.

S75: National Police Agency. 事業者に求められる不正アクセス対策のポイント. https://www.npa.go.jp/bureau/cyber/pdf/R8_Vol.22cpal.pdf. Verified on 2026-11-22.

S76: JPCERT/CC. インシデント調査報告書受領時のチェックリスト. https://blogs.jpcert.or.jp/ja/2026/11/ir_report_checklist.html. Verified on 2026-11-22.

S77: JPCERT/CC. APT-C-60による2026年の攻撃. https://blogs.jpcert.or.jp/ja/2026/07/apt-c-60_2026.html. Verified on 2026-11-23.

S78: National Police Agency. WaterPlum joint advisory. https://www.npa.go.jp/bureau/cyber/pdf/20260918_e.pdf. Verified on 2026-11-22.

S79: FSA. インターネット取引サービスへの不正アクセス・不正取引にご注意ください. https://www.fsa.go.jp/ordinary/chuui/chuui_phishing.html. Verified on 2026-11-23.

S80: IPA. PHPの脆弱性対策について（2026年11月）. https://www.ipa.go.jp/security/security-alert/2026/alert20261120.html. Verified on 2026-11-23.

S81: National Police Agency. 不正アプリによる不正送金被害が発生. https://www.npa.go.jp/bureau/cyber/pdf/R8_Vol.18cpal.pdf. Verified on 2026-11-22.

S82: National Police Agency. 大規模な個人情報等の流出事案に係る警察庁長官の指示. https://www.npa.go.jp/news/release/2026/20261106news.pdf. Verified on 2026-11-22.

S83: PPC. 共有メールシステムに関する行政上の対応. https://www.ppc.go.jp/files/pdf/260819_01_houdou.pdf. Verified on 2026-11-22.

S84: PPC. APPI breach reporting and affected-person notification. https://www.ppc.go.jp/personalinfo/legal/guidelines_tsusoku/. Verified on 2026-11-22.

S85: FSA. FSA cybersecurity guidelines. https://www.fsa.go.jp/news/r6/sonota/20241004/20241004.html. Verified on 2026-11-22.

S86: FSA. FSA 2026 supervisory amendments. https://www.fsa.go.jp/news/r7/sonota/20260227/20260227.html. Verified on 2026-11-22.

S87: FSA. FSA common cyber incident report forms. https://www.fsa.go.jp/news/r8/sonota/20260918/20260918.html. Verified on 2026-11-22.

S88: Cabinet Office. Cyber response legislation partial commencement. https://www.cao.go.jp/minister/2609_t_furukawa/photo/2026_005.html. Verified on 2026-11-22.

S89: JPCERT/CC. OpenJDK urgent update review. https://www.jpcert.or.jp/newsflash/2026111801.html. Verified on 2026-11-22.

S90: MITRE. ATT&CK Spearphishing Link. https://attack.mitre.org/techniques/T1566/002/. Verified on 2026-11-22.

S91: MITRE. ATT&CK User Execution: Malicious File. https://attack.mitre.org/techniques/T1204/002/. Verified on 2026-11-22.

S92: MITRE. ATT&CK System Binary Proxy Execution: Mshta. https://attack.mitre.org/techniques/T1218/005/. Verified on 2026-11-22.

S93: RFC Editor. RFC 7489: Domain-based Message Authentication, Reporting, and Conformance. https://www.rfc-editor.org/rfc/rfc7489.html. Verified on 2026-11-22.

S94: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S95: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S96: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S97: Organisation notice. Public-sector incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S98: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S99: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S100: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S101: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S102: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S103: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S104: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S105: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S106: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S107: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S108: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S109: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S110: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S111: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S112: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S113: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S114: Organisation notice. Public-sector incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S115: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S116: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-23.

S117: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S118: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S119: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S120: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S121: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S122: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S123: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S124: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S125: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S126: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S127: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S128: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S129: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S130: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S131: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S132: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S134: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S135: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S136: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S137: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S138: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S139: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S140: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S141: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S142: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S143: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S144: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S145: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S146: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S147: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S148: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S149: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S150: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S151: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S152: Organisation notice. Incident notice. https://www.release.tdnet.info/ (article URL withheld). Verified on 2026-11-22.

S153: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S154: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S155: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S156: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S157: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S158: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S160: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S161: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S162: Organisation notice. Incident notice. https://www.release.tdnet.info/ (article URL withheld). Verified on 2026-11-22.

S163: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S164: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S165: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S166: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S167: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S168: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S169: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S170: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S171: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S172: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S173: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S174: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S175: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S176: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S177: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S178: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S179: Organisation notice. Incident notice. https://www.release.tdnet.info/ (article URL withheld). Verified on 2026-11-22.

S180: Organisation notice. Incident notice. https://www.release.tdnet.info/ (article URL withheld). Verified on 2026-11-22.

S181: Organisation notice. Incident notice. https://www.release.tdnet.info/ (article URL withheld). Verified on 2026-11-22.

S182: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S183: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S184: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S185: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S186: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S187: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S188: Organisation notice. Incident notice. https://www.release.tdnet.info/ (article URL withheld). Verified on 2026-11-22.

S189: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S190: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S191: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S192: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S193: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S194: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S195: Organisation notice. Incident notice. https://www.release.tdnet.info/ (article URL withheld). Verified on 2026-11-22.

S196: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S197: Organisation notice. Incident notice. https://www.release.tdnet.info/ (article URL withheld). Verified on 2026-11-22.

S198: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S199: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S200: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S201: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S202: Organisation notice. Incident notice. https://www.release.tdnet.info/ (article URL withheld). Verified on 2026-11-22.

S203: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S204: Organisation notice. Incident notice. https://data.swcms.net/ (article URL withheld). Verified on 2026-11-22.

S205: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S206: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S207: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S208: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-23.

S209: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-23.

S210: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-23.

S211: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S212: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S213: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S214: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S215: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S216: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S217: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S218: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S219: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S220: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S221: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S222: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S223: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S224: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S225: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S226: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S227: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S228: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S229: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S230: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S231: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S232: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S233: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S234: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S235: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S236: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S237: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S238: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S239: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S240: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S241: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S242: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S243: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S244: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S245: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S246: Organisation notice. Public-sector incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S247: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S248: Organisation notice. Incident notice. Official notice (article URL withheld). Verified on 2026-11-22.

S249: CVE Program. CVE-2026-114938 record. https://cveawg.mitre.org/api/cve/CVE-2026-114938. Verified on 2026-11-22.

S250: OpenJDK. OpenJDK Vulnerability Advisory 2026-11-17. https://openjdk.org/groups/vulnerability/advisories/2026-11-17. Verified on 2026-11-22.

S251: Ubuntu. CVE-2026-114938 package status and fixes. https://ubuntu.com/security/CVE-2026-114938. Verified on 2026-11-22.

S252: The PHP Group. PHP November security releases in the 2026 news archive. https://www.php.net/archive/2026.php. Verified on 2026-11-22.

S253: PPC. APPI reporting guidance for private businesses and administrative bodies. https://www.ppc.go.jp/personalinfo/legal/leakAction/. Verified on 2026-11-22.

S254: National Police Agency. 令和７年上半期におけるサイバー空間をめぐる脅威の情勢等について (18 September 2025). https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7kami/R07_kami_cyber_jyosei.pdf. Verified on 23 November 2026.

S255: FSA. インターネット取引サービスへの不正アクセス・不正取引の発生状況 (13 November 2026). https://www.fsa.go.jp/ordinary/chuui/chuui_phishing/20261113.pdf. Verified on 23 November 2026.

S256: National Police Agency and NISC. Alert: Cyberattacks by MirrorFace (Provisional Translation) (4 February 2025). https://www.npa.go.jp/bureau/cyber/pdf/20250204_mf.pdf. Verified on 23 November 2026.

APPENDICES

Appendices

A–D

THIS CHAPTER ANSWERS

Which terms help a reader act on the evidence?

3

evidence distinctions: observation, claim and inference

Appendix A. Scope and evidence boundaries 115

Appendix B. Evidence register 119

Appendix C. Sources 124

Appendix D. Glossary 134

Appendix D. Glossary

Term	Plain meaning
APPI	Japan's personal-information protection law; applicability and notification decisions require the actual scope and circumstances. [S84]
API	An interface through which software requests functions or information; authorisation must apply to the requested action and data. [S73]
Credential	Information used to authenticate an account or integration; an advertised credential is not automatically current or usable
DMARC	A domain-level email policy and reporting mechanism; quarantine and reject request handling of authentication failures. [S93]
DDoS	Distributed denial of service; an attempt to exhaust a service's resources or availability
Exposure	An observed condition or association needing validation, rather than a synonym for confirmed intrusion
Integration key	A credential allowing a service to communicate with another system; its scope depends on the receiving system
IoT	Network-connected devices such as cameras and home equipment; some can be misused to relay traffic. [S72]
MFA	Authentication using more than one factor; its presence does not resolve every session, integration or application-permission issue
OAuth consent	A user's or administrator's permission for an application to act within granted scope. [S70]
OT	Operational technology used to monitor or control physical processes
Ransomware listing	A criminal publication naming a claimed target; it does not independently confirm theft or encryption
Record or row	One data entry; repeated entries can concern the same person
Repository	A store of source code and related development material; its contents differ from the production database
Residential proxy	A service that relays traffic through a household connection, potentially disguising its origin. [S72]
Session	An authenticated interaction that can remain relevant after a password change

Term	Plain meaning
Supplier scope	The product, environment, information and customers actually covered by a provider's incident findings
Vishing	Deceptive voice contact used to obtain information or induce an action. [S67]
SpyGlace	Malware named by JPCERT/CC in its APT-C-60 delivery research. [S77]
WaterPlum	The campaign label used in the joint recruitment and fraudulent-workforce advisory. [S78]

About this report

Odin by Brandefense prepared this public research edition for security, fraud, privacy and business-continuity teams. It supports evidence-based decisions within the stated scope. It does not identify the reader's own active exposures or replace incident-specific technical, legal or operational assessment.

The Japanese edition is translated with AI from the English master. The English edition prevails where meanings differ. Both editions retain the same evidence IDs and numerical values. Distribution is TLP:CLEAR.

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