BRANDEFENSE COUNTRY REPORT · SOUTH KOREA 2026

Brandefense South Korea Cyber Threat Landscape Report 2026

Identity, external business applications and recovery across a connected economy

Odin by Brandefense
Research window: 2026-01-01–2026-11-22, by post date
Version 1.0 · Public Research Edition · TLP:CLEAR · 2026-11-08–2026-11-22

4
leader decisions tied to evidence and closure tests

250
candidate domains across ten merged sector cells

8
detailed claim cases with distinct evidential limits

73
South Korea ransomware listings in Ransompedia

CONTENTS

Contents

01	Executive summary	05
	Report map	09
02	South Korea's digital and security context	10
03	Organisation exposure and public-facing hygiene	14
04	Dark-web and forum evidence	24
05	Public incidents and targeting by sector	46
06	Hacktivism, DDoS and service continuity	63
07	Actors, campaigns and relationships	69
08	Fraud, identity and the secondary-use problem	81
09	Banking and financial services	86
10	Regulatory and national response	91
11	Outlook and conditional scenarios	96
12	Action plan	100
A	Appendix A. Scope, evidence and limitations	107
B	Appendix B. Evidence register	110
C	Appendix C. Sources	111
D	Appendix D. Glossary	116
	About this report	119

Board and executives	01 05 11 12
CISO and security leads	03 04 05 07 12
SOC and threat intelligence	04 06 07 B
Fraud and customer operations	05 08 09
Privacy, legal and procurement	05 09 10 12

About this edition

Prepared with AI assistance. Observations, criminal claims, source attributions and confirmed disclosures remain distinct. Scope and confidence are explained in Appendix A.

South Korea's evidence calls for a joined response: validate identities, review supporting business applications, protect affected people and demonstrate essential-service recovery.

73

South Korea ransomware listings; criminal claims

250

selected candidate domains across ten sector cells

26

detailed cases, including claims and public disclosures

4

decisions for leaders with accountable completion evidence

Contents and reading routes

Chapter	Question	First reader
1 Executive summary	Which decisions follow from the evidence?	Leadership
2 Context	Which service dependencies matter?	CISO and business owners
3 Organisation exposure	What do the selected-domain observations establish?	Identity and infrastructure
4 Underground activity	What is offered, and what remains unverified?	Threat intelligence
5 Sector incidents	What did sources actually confirm or report?	Incident and sector owners
6 Availability	How does a claim differ from demonstrated impact?	Service operations
7 Actors	Which attributions and relationships are supported?	Threat intelligence and SOC
8 Fraud	Which workflows can reuse circulating information?	Fraud and customer operations
9 Banking	How do application, identity and customer decisions connect?	Financial-sector leaders
10 Regulation	Which current duties and later measures differ?	Privacy and legal
11 Outlook	Which conditional scenarios justify preparation?	Leadership
12 Action plan	Who acts, and what demonstrates completion?	All owners
Appendices A–D	Scope, evidence register, sources and definitions	Reference

CHAPTER 01

Executive summary

01

THIS CHAPTER ANSWERS

Which South Korea findings justify immediate decisions?

4

leader decisions tied to evidence and closure tests

Four decisions for leaders 07

The year in numbers 07

CHAPTER 01

Executive summary

IN SHORT

South Korea's evidence links identity risk, peripheral applications, suppliers and recovery. Ransompedia records 73 listing claims. Public sources describe application-level information access, ransomware and targeted correspondence. The closing fortnight includes scope revisions that cannot be added into unique people. Criminal advertisements remain unverified, and state attributions remain their sources' assessments. Validate relevant account evidence, test sensitive application access, confirm supplier notification routes and rehearse restoration with business owners.

Posts, listings, selected domains, source disclosures and people are different populations. This report does not add them into a national incident total. It also separates an event's occurrence, discovery, disclosure and later enforcement. [S1][S2][S3]

The requested cut-off is 2026-11-22. Evidence reflects material available when checked on that date; the day was still in progress. The recent-activity sections concern publications and observations during 2026-11-08–2026-11-22, without assuming the underlying intrusion began then.

1. Supporting business applications need accountable security ownership. The FSC's dated disclosure population and the Financial Security Institute case show why customer, staff and assessment information matter outside core transaction systems. Review object access, exports and identity dependencies according to actual privilege and information. [S5][S6]

2. Visible extortion supports recovery investment, without establishing every outcome. Ransompedia has 73 South Korea listings, compared with 41 for all of 2025. Manufacturing carries the largest industry label, at 19 listings. Partial-year and full-year totals are not a matched-period growth rate. [S2]

3. Advertised quantities require a unit before they inform impact. The cases include lending information, healthcare tables, business-system bundles and technical documents. Rows, accounts, files and people are not interchangeable. The report does not authenticate the advertised files or infer successful transactions. [S1]

4. Recent disclosures require controlled updates rather than a single combined total. University and supplier accounts describe different services and changing categories. A system-level record sum is not necessarily unique people, and a program subset must not be added to its supplier's total. Chapter 5 preserves each boundary.

5. Source confidence must survive the move from analysis to action. Genians assigns moderate confidence to a Kimsuky connection in its research and retains imitation as an alternative. AhnLab's separate domestic review supports behavioural attention without attributing its entire observed population to one group. [S14][S15]

6. The selected portfolio supports validation, not a national prevalence estimate. The 250 candidate domains span ten merged cells of 25. Ownership, related groups and unavailable observations limit interpretation. 121 of 250 selected domains had an associated credential listing when checked. The national Atlas headline is 54 out of 100. Validate active accounts first. [S3]

Four decisions for leaders

1. **Assign identity-alert validation.** Establish an internal or provider alert route and match relevant offers to active accounts, privilege and sessions. Each alert needs a dated disposition; corroborated active misuse enters incident response immediately.
2. **Review external business interfaces.** Inventory customer, partner, staff and support applications. Test that authenticated users can reach only authorised information, and give every sensitive interface a business owner.
3. **Exercise suppliers and customer protection together.** Confirm which records a supplier holds, who sends an initial notice and who preserves access evidence. Test recovery and payment changes against a caller with accurate personal details.
4. **Demonstrate restoration and factual communications.** Restore an essential service with independent recovery credentials. Practise a statement that distinguishes a claim, confirmed service impact and established information scope.

The year in numbers

73

South Korea listing claims in the requested 2026 window

WHAT IT DOES NOT MEASURE

Confirmed intrusions or unique organisations

41

South Korea listings for all of 2025 in the same snapshot

WHAT IT DOES NOT MEASURE

A matched-period baseline

12 / 8 / 6

N0n / Qilin / Metaencryptor listing labels

WHAT IT DOES NOT MEASURE

Unique operators or verified outcomes

146 / 122 / 67 / 110

Japan / Taiwan / Hong Kong / Singapore listing counts

WHAT IT DOES NOT MEASURE

A national security ranking

250

Selected candidate domains across ten merged sectors

WHAT IT DOES NOT MEASURE

A representative national sample

26

Detailed report cases across claims and public-source accounts

WHAT IT DOES NOT MEASURE

A national incident count

24

Redacted source-post cards

WHAT IT DOES NOT MEASURE

Unique incidents or authenticated files

39,733

Available country-associated post measurement

WHAT IT DOES NOT MEASURE

Attack frequency or loss

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

KEY TAKEAWAYS

01

Own the identity and application validation decisions.

02

Keep claims, official disclosures and changing populations separate.

03

Test supplier response, customer protection and restoration with completion evidence.

Report map

Follow the decision you own, then its evidence, limitation and completion test.

Board and executives	Fund service and information resilience	01 05 11 12
CISO and security leads	Prioritise relevant signals and dependencies	03 04 05 07 12
SOC and threat intelligence	Distinguish claims from corroborated behaviour	04 06 07 B
Fraud and customer operations	Prevent information reuse from authorising harm	05 08 09
Privacy, legal and procurement	Decide applicability and supplier responsibilities	05 09 10 12

Observation means the material or measurement is held. **Claim** means a poster or listing asserts an outcome. **Official account** means an organisation or authority states the fact within its reported scope.

Analyst inference connects evidence to a decision without supplying missing proof. **Source attribution** remains the cited researcher's assessment, including confidence and alternatives.

CHAPTER 02

South Korea's digital and security context

02

THIS CHAPTER ANSWERS

Which features of South Korea's connected economy should shape security decisions?

96.9%

internet penetration in DataReportal's late-year estimate

2.1 Connectivity creates dependencies 11

2.2 Peripheral systems deserve central accountability 11

2.3 Espionage and criminal activity need separate explanations 12

2.4 Political context is not attribution evidence 12

2.5 Multiple authorities mean multiple reporting decisions 12

CHAPTER 02

South Korea's digital and security context

IN SHORT

Shared identity, business software and communications services connect otherwise separate organisations. Public disclosures show why a peripheral application can matter even when a payment system remains outside the reported incident. Espionage research describes targeted business correspondence and document lures. Keep service dependencies, personal-data obligations and source-attributed actor assessments separate. Map who can authenticate, export information, change a payment instruction and restore an essential service.

2.1 Connectivity creates dependencies

DataReportal's Digital 2027 edition reports 50.0 million internet users and 96.9% penetration for South Korea. Its underlying internet estimate concerns October 2026. It also reports 61.4 million mobile connections and 49.6 million social-media identities. Connections and identities do not count unique people. [S8]

These figures describe the operating environment, rather than the frequency of attacks. Organisations interact with customers through mobile applications, messages, websites and outsourced support. The security boundary follows those relationships beyond a corporate network.

A useful inventory therefore connects each important service to its identity provider, data owner, supplier and recovery channel. It should show who can retrieve a document or reset a user's access. A list of servers cannot answer those questions alone.

For a bank, a sales-support application can hold sensitive customer information without processing deposits. For a university, a teaching portal can expose identity information without interrupting every campus service. Treat each application's actual privileges and data as the basis for response.

2.2 Peripheral systems deserve central accountability

The FSC's November measures expressly cover external interfaces, staff and internal-work applications, development environments and associated business systems. That scope matters because a system outside a core transaction platform can still hold valuable information. [S5]

The defensive interpretation is to assign the same business accountability to these applications as to production systems. Each needs an owner, supported software, an access review and evidence that an unauthenticated user cannot obtain another person's records.

A central security policy can coexist with decentralised procurement. Departments may commission event, training, marketing or assessment services. Their contracts should identify what information is necessary, how long it remains available, and who can preserve access records after an incident.

This is a planning implication from the disclosed mechanisms. It is not a finding that every Korean organisation has the same architecture or has omitted these controls.

2.3 Espionage and criminal activity need separate explanations

Genians' November research concerns a targeted correspondence chain aimed at a seminar attendee. AhnLab's October domestic activity review describes malicious shortcuts and document-themed delivery. These sources support attention to trusted business workflows and endpoint behaviour. They do not establish the national prevalence of espionage. [S14][S15]

An underground advertisement has a different evidential role. It can establish that someone offered information or requested access. It does not independently establish the origin of a file, a successful intrusion or the identity of an operator.

Similarly, a ransomware listing is a criminal assertion. The source's country and industry labels describe the listing population. They do not resolve corporate ownership, every operating location, or whether a listed organisation experienced encryption.

2.4 Political context is not attribution evidence

The authors take no position on governments, parties, politicians, elections or foreign relations. Political subject matter, Korean-language text and a familiar malware label do not independently identify an operator.

This report does not use the December 2024 martial-law episode, its aftermath or the 2025 presidential election to infer responsibility for a cyber incident. Those events precede the observation window. Any campaign reference to a public office is evaluated for impersonation and access consequences.

Descriptions involving North Korea, China or Japan appear only where a cited source makes an attribution or where a regional comparison requires the country label. The source's confidence and alternative explanations remain part of the account.

2.5 Multiple authorities mean multiple reporting decisions

Personal-data protection, financial supervision and technical incident response overlap, but they answer different questions. PIPC's reporting guidance distinguishes general personal-data incidents from financial-sector personal-credit information. Financial institutions are directed to consult the FSS about their reporting route. [S9]

The practical task is to name the decision owner before an event. Legal and privacy teams determine applicable duties; technical responders preserve evidence; business owners explain service consequences. Filing through one channel should not be assumed to discharge every obligation.

KEY TAKEAWAYS

01

Map identity, data and suppliers around each important service.

02

Investigate peripheral applications according to the information and privileges they hold.

03

Preserve source confidence and assign reporting responsibilities before an incident.

CHAPTER 03

Organisation exposure and public-facing hygiene

THIS CHAPTER ANSWERS

What can the selected-domain observations support, and where do the evidence limits begin?

250

candidate domains across ten merged sector cells

3.1 Universe card 15

3.2 Exposure signals and their limits 15

3.3 Email and web observations 19

3.4 A response sequence for asset owners 22

3.5 What the portfolio cannot answer 23

CHAPTER 03

Organisation exposure and public-facing hygiene

IN SHORT

121 of 250 selected domains had an associated credential listing when checked. The national Atlas headline is 54 out of 100. Device associations and historical records require separate validation. This purposive portfolio does not estimate national prevalence, and related domains may share owners. Validate active accounts, reconcile employee devices and plan email-control changes with accountable owners.

3.1 Universe card

Item	Definition
Selected population	250 candidate primary domains across ten sector cells
Sector coverage	25 domains in each cell; related activities are merged
Selection	Systemic role, public-service function and sector coverage; no revenue ranking
Unit	A selected domain; independent legal-entity ownership is not established for the whole portfolio
Observation date	2026-11-22; unavailable checks remain unknown
Interpretation	A configuration observation is distinct from an incident or an account validation
National inference	The portfolio cannot estimate national prevalence

The portfolio includes national and regional administration, banking and payments, insurance and capital markets, education and research, industry and technology, energy and infrastructure, transport and logistics, communications and consumer services, and health and life sciences.

Domains can share a corporate group or a service provider. A primary domain can also serve several populations. A login associated with a university, for example, does not by itself identify a staff member rather than a student.

3.2 Exposure signals and their limits

121 of 250 selected domains had an associated credential listing when checked on 2026-11-22. The national Atlas headline is 54 out of 100. The portfolio is purposive and does not estimate national prevalence. [S3]

121 of 250

selected domains with an associated credential listing

54 of 100

national Atlas headline

238 of 250

domains with infected-device associations

236 of 250

domains with historical credential records

121 selected domains have an associated credential listing

	Current listing	Device associations	Credential associations	Document associations
Banking and payments	15/25	24/25	23/25	15/25
Communications and consumer services	17/25	25/25	25/25	17/25
Education and research	14/25	25/25	25/25	24/25
Energy and infrastructure	2/25	23/25	25/25	12/25
Health and life sciences	10/25	22/25	22/25	6/25
Industry and technology	8/25	22/25	22/25	14/25
Insurance and capital markets	17/25	25/25	24/25	17/25
Public administration	9/25	25/25	22/25	4/25
Regional administration	14/25	24/25	23/25	6/25
Transport and logistics	15/25	23/25	25/25	12/25

Current credential listings by sector (coral). Cells show selected domains with each signal / selected domains; categories overlap. Source: selected-domain exposure observations, 22 November 2026 [S3]. 250 candidate domains, ten sector cells of 25. Associations can overlap and include historical material; not national prevalence or confirmed intrusions.

Sector	Domains	Domains with current credential listings	Domains with device associations	Credential records	Documents
Banking and payments	25	15	24	23	15

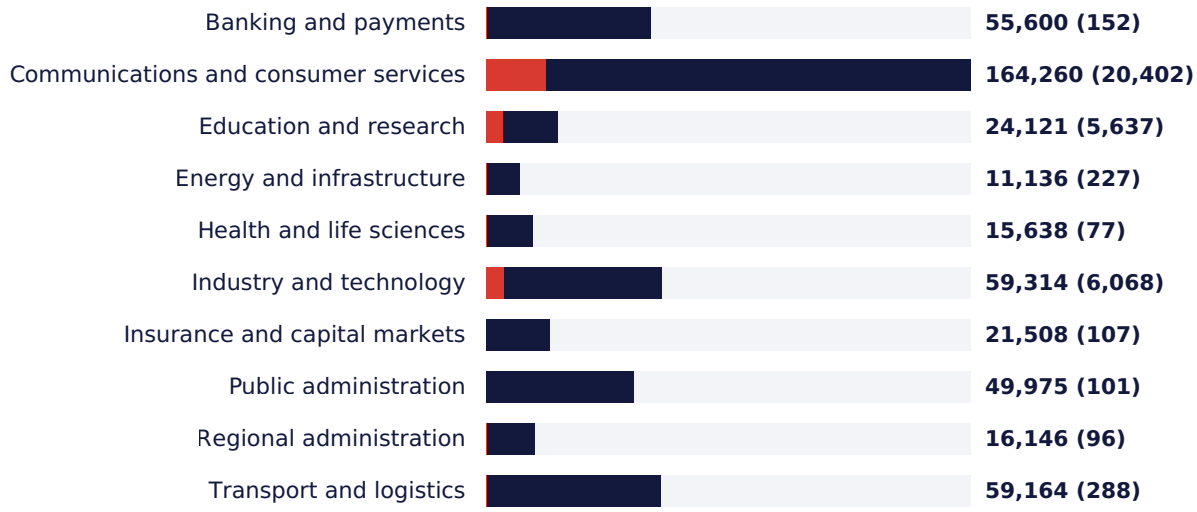
Sector	Domains	Domains with current credential listings	Domains with device associations	Credential records	Documents
Communications and consumer services	25	17	25	25	17
Education and research	25	14	25	25	24
Energy and infrastructure	25	2	23	25	12
Health and life sciences	25	10	22	22	6
Industry and technology	25	8	22	22	14
Insurance and capital markets	25	17	25	24	17
Public administration	25	9	25	22	4
Regional administration	25	14	24	23	6
Transport and logistics	25	15	23	25	12
All selected domains	250	121	238	236	127

Only the national Atlas headline is published. Sector entries count domains with each signal; the columns overlap and must not be added. A current listing requires account validation, rather than establishing a successful intrusion. [S3]

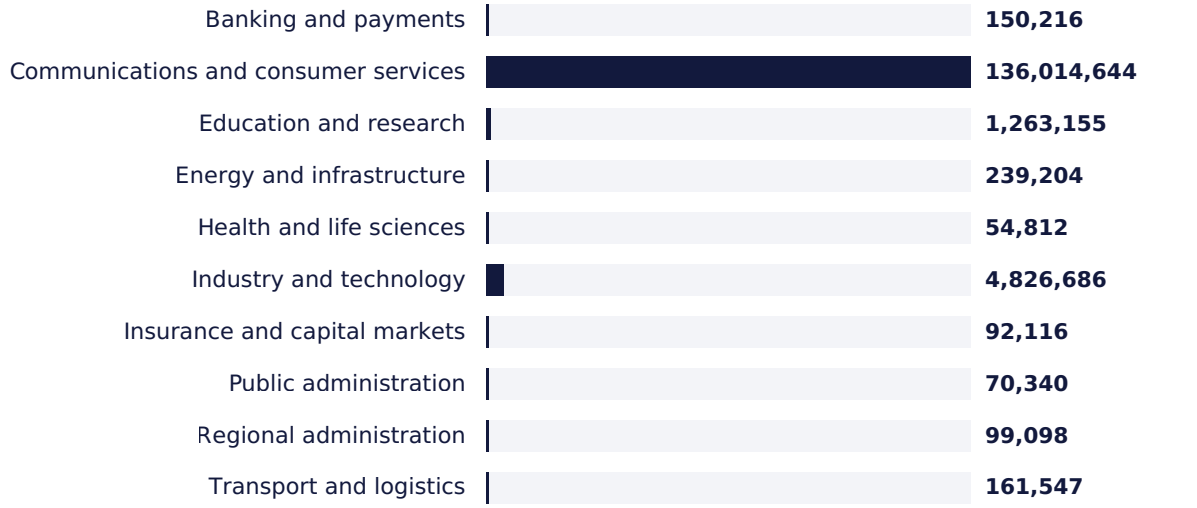
Device associations are concentrated outside the employee classification

Employee devices Other associations

Device associations (employee subset in parentheses)



Credential-record associations (separate scale)



Source: selected-domain exposure observations, 22 November 2026 [S3]. 250 candidate domains, ten sector cells of 25. Associations can overlap and include historical material; not national prevalence or confirmed intrusions.

Sector	Device associations	Employee-classified device associations	Other device associations	Credential records
Banking and payments	55,600	152	55,448	150,216
Communications and consumer services	164,260	20,402	143,858	136,014,644
Education and research	24,121	5,637	18,484	1,263,155
Energy and infrastructure	11,136	227	10,909	239,204
Health and life sciences	15,638	77	15,561	54,812

Sector	Device associations	Employee-classified device associations	Other device associations	Credential records
Industry and technology	59,314	6,068	53,246	4,826,686
Insurance and capital markets	21,508	107	21,401	92,116
Public administration	49,975	101	49,874	70,340
Regional administration	16,146	96	16,050	99,098
Transport and logistics	59,164	288	58,876	161,547
All selected domains	476,862	33,155	443,707	142,971,818

The portfolio has 476,862 infected-device associations, including 33,155 employee-classified and 443,707 other associations. Totals are not a count of unique devices. Ownership of devices outside the employee classification is unresolved. They can include customers or other users, rather than organisational endpoints. [S3]

Historical credential records total 142,971,818: 51,019,801 breach-database records, 11,103,468 stealer records and 80,848,549 combolist records. These are cumulative records held on the observation date, not credentials first exposed during 2026. Records can overlap across people, sources and organisations. [S3]

The snapshot also contains 1,611 document associations and 46,750 lookalike candidates from the preceding 30 days. Neither count establishes malicious origin, current access or a successful intrusion. Validate documents and candidate domains against their actual content and ownership. [S3]

Where an organisation receives a current credential offer affecting its own domain, the first task is account validation. Confirm that the account belongs to the organisation, remains active, and has privileges or sessions requiring containment. Record historical or already remediated observations separately.

Device associations, credential records, documents, mentions and lookalike candidates describe different populations. They must not be added into a count of affected people. A device can contain accounts for more than one service, and a person can appear in several records.

A mention can be ordinary discussion. A lookalike candidate can be unrelated to the brand. A document can reference an organisation without originating from its systems. These limits determine the next validation step; they do not dismiss a relevant alert.

3.3 Email and web observations

Observation	Domains
Selected domains	250

Observation	Domains
Configuration records available	229
DMARC reject observed	5
DMARC quarantine observed	14
DMARC monitoring policy observed	108
DMARC policy not established	123
SPF record observed	205
DKIM key observed	67
Parent-zone DS observed	2
CAA observed (Appendix D)	1
Certificate validation observed	197
Certificate verification issue	7
Certificate observation unavailable	46

These observations concern the selected 250-domain portfolio. Unestablished policies and unavailable services remain unknown, rather than failed controls. Certificate and web-response observations can concern different services. [S3]

Web-response observations were available for 191 domains. HSTS appeared in 58 of those responses, CSP in 25, frame restrictions in 50 and content-type restrictions in 58. These are response observations, rather than coverage of every application. Appendix D defines HSTS and CSP. [S3]

Sector configuration observations are counts rather than ratings

	DMARC reject	DMARC quarantine	SPF	DKIM
Public administration	0/25	2/25	24/25	4/25
Regional administration	0/25	0/25	16/25	0/25
Banking and payments	0/25	0/25	23/25	8/25
Insurance and capital markets	1/25	1/25	22/25	6/25
Education and research	1/25	2/25	22/25	14/25
Industry and technology	0/25	3/25	17/25	5/25
Energy and infrastructure	1/25	1/25	19/25	7/25
Transport and logistics	0/25	1/25	24/25	8/25
Communications and consumer services	1/25	4/25	22/25	10/25
Health and life sciences	1/25	0/25	16/25	5/25

Source: selected-domain public configuration observations, 22 November 2026 [S3]. Counts use selected-domain denominators; a missing observation does not establish a missing control.

Sector	Selected	DMARC reject	DMARC quarantine	SPF observed	DKIM observed
Public administration	25	0	2	24	4
Regional administration	25	0	0	16	0
Banking and payments	25	0	0	23	8
Insurance and capital markets	25	1	1	22	6
Education and research	25	1	2	22	14
Industry and technology	25	0	3	17	5
Energy and infrastructure	25	1	1	19	7
Transport and logistics	25	0	1	24	8

Sector	Selected	DMARC reject	DMARC quarantine	SPF observed	DKIM observed
Communications and consumer services	25	1	4	22	10
Health and life sciences	25	1	0	16	5

Each cell contains 25 selected domains. The figures are signal counts, not sector ratings or evidence of intrusion. [S3]

A DMARC policy instructs receiving systems how to handle unauthenticated mail claiming the domain. Its presence is not a measure of phishing success. A monitoring policy can be part of a managed rollout, so the next decision is to identify legitimate senders before enforcement changes.

An SPF record describes authorised sending infrastructure. A published DKIM key is evidence of a key at that name, rather than proof that every message is signed. An unobserved key leaves deployment unresolved.

A parent-zone DS record provides a link used by DNSSEC validation. Its presence alone does not establish a valid chain for every response. Web certificate and header observations likewise concern the service that answered, rather than every application operated by the organisation.

3.4 A response sequence for asset owners

Signal	Initial owner	Validation	Completion evidence
Credential offer	Identity operations	Ownership, activity, privilege and session review	Dated account disposition
Device association	Endpoint and identity	Asset and account reconciliation	Relevant sessions contained or observation closed
Uncertain mail policy	Messaging	Legitimate sender and alignment review	Approved enforcement plan
Web certificate issue	Service owner	Certificate chain and service dependency	Valid service and renewal ownership
Lookalike candidate	Brand protection	Ownership and actual content	Documented classification and action
Exposed document	Data owner	Origin, access and sensitivity	Access corrected and impact assessed

Use business criticality and corroborating evidence to order the queue. A historical record alone does not justify disabling every user in a sector. A validated active privileged account can justify immediate containment without waiting for a portfolio summary.

3.5 What the portfolio cannot answer

The observations cannot establish how many Korean organisations were attacked, how many people lost information, or how well a control performed during an incident. They also cannot settle the relationship between an underground offer and an official disclosure without matching evidence.

For management reporting, distinguish an observation requiring review from an accepted incident. Report unresolved ownership and unavailable measurements alongside the completed checks. A blank entry should never become a reassuring zero.

KEY TAKEAWAYS

01

Treat selected-domain observations as a validation queue.

02

Keep unavailable checks and ownership uncertainty visible.

03

Close each alert with evidence from the responsible asset or account owner.

CHAPTER 04

Dark-web and forum evidence

04

THIS CHAPTER ANSWERS

What do the retained posts establish, and which claims deserve investigation?

8

detailed claim cases with distinct evidential limits

4.1 Universe card 25

4.2 Volume, platforms and languages 25

4.3 Eight claim cases 30

4.4 Additional offers and recirculated material 38

4.5 Recent activity: 2026-11-08 through 2026-11-22 44

CHAPTER 04

Dark-web and forum evidence

IN SHORT

The retained material mixes data advertisements, access offers, requests, reposts and ordinary market discussion. The useful evidence is what a particular post says and what corroborates it. Large quantities often describe heterogeneous rows or files rather than people. Some recent-looking activity concerns older material. Validate provenance, account relevance and the claimed unit before deciding on containment, public communications or a notification assessment.

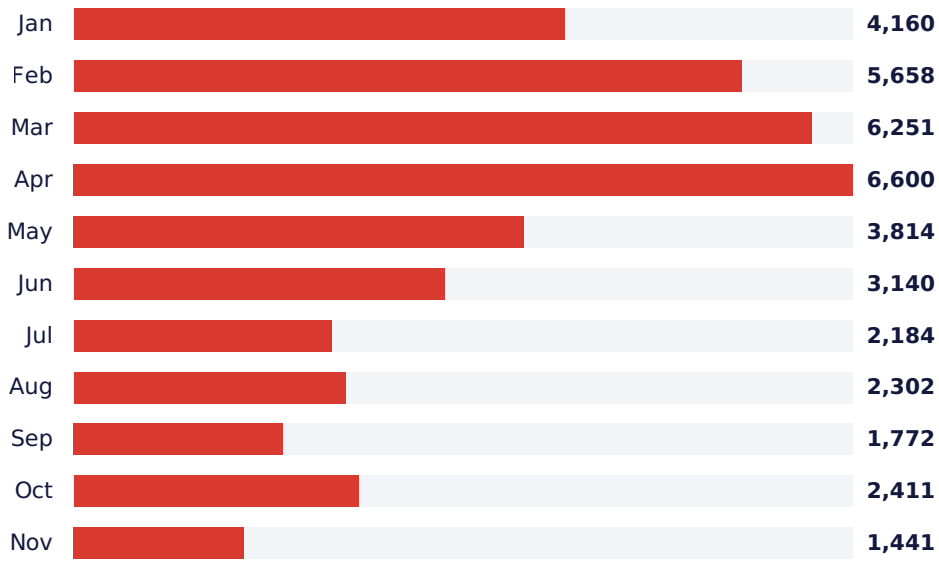
4.1 Universe card

Item	Definition
Source	Retained Brandefense Blackhole posts and advertisements
Window	Post publication time 2026-01-01 through 2026-11-22
Country association	South Korea references in the available source material; not verified targeting
Measured volume	39,733
Unit	A post; different records can repeat a source statement
Unresolved	File authenticity, original acquisition date, successful sales and continuing access

4.2 Volume, platforms and languages

The retained evidence population contains 39,733 post records, including specific claims and wider context. It is not a national incident total or a representative sample of criminal activity. Post dates describe publication and circulation, rather than intrusion starts. [S1]

Monthly post observations describe circulation rather than intrusion starts



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

Post month	Retained records
2026-01	4,160
2026-02	5,658
2026-03	6,251
2026-04	6,600
2026-05	3,814
2026-06	3,140
2026-07	2,184
2026-08	2,302
2026-09	1,772
2026-10	2,411
2026-11	1,441
Total	39,733

Platform volumes describe this retained evidence population

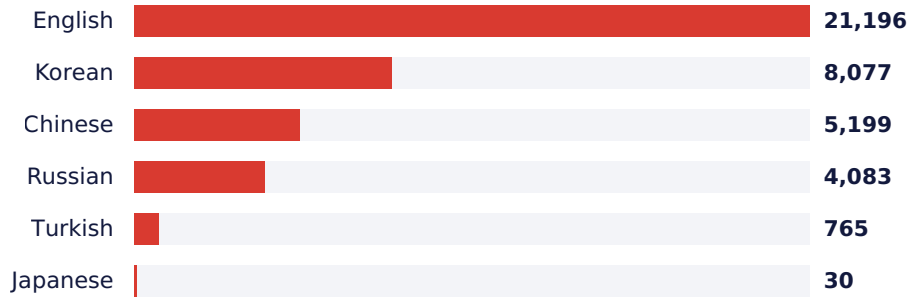


Source: Odin by Brandefense, retained post observations concerning South Korea, 1 January–22 November 2026, closing day partial [S1]. Retained and country-tagged posts are separate populations; not attack counts.

Platform	Retained records
telegram	38,899
forum	707
discord	72
paste	55

Platform volumes reflect the available evidence population. They do not measure market share, attack success or relative platform safety.

Language labels do not establish an operator's nationality



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

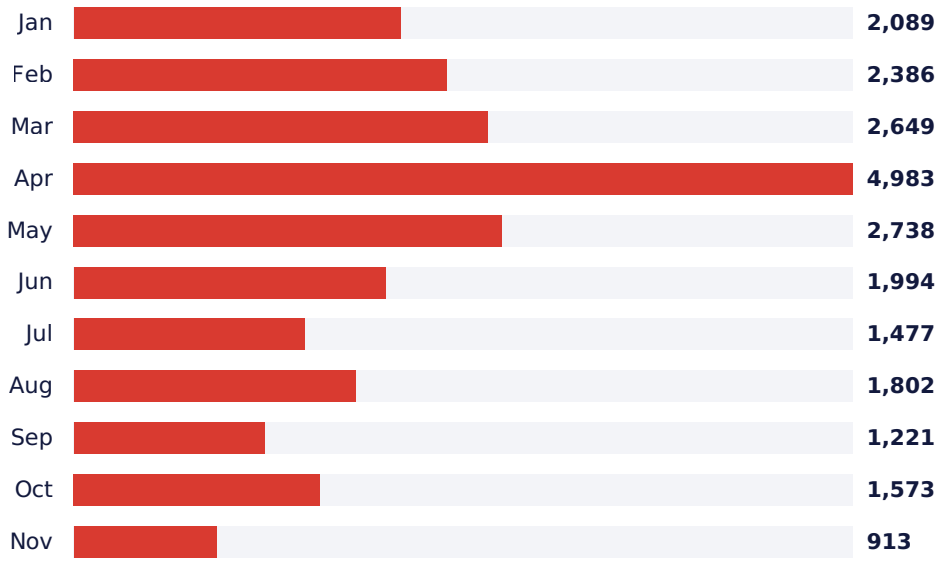
Language label	Retained records
English	21,196
Korean	8,077
Chinese	5,199
Russian	4,083
Turkish	765
Japanese	30

Language labels can overlap and do not cover every retained record. These selected label counts must not be added into a new post total or used to infer an operator's nationality. [S1]

Brandefense Blackhole records 23,825 country-tagged posts dated 2026-01-01–2026-11-22. This is a tagged-post population, not a count of relevant incidents or confirmed targeting. It overlaps the retained research population and must not be added to it. November is a partial month. [S1]

The retained total covers South Korea references, while the tagged total counts posts carrying the country tag. These are different scopes, so the retained total can be larger. [S1]

Country-tagged monthly volumes describe publication rather than confirmed incidents



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

Month	Tagged posts
2026-01	2,089
2026-02	2,386

Month	Tagged posts
2026-03	2,649
2026-04	4,983
2026-05	2,738
2026-06	1,994
2026-07	1,477
2026-08	1,802
2026-09	1,221
2026-10	1,573
2026-11	913
Total	23,825

The following language counts concern the country-tagged population, rather than the retained-evidence tables above. Language labels can overlap and do not establish nationality. [S1]

Language label	Tagged posts
KO	3,521
EN	11,048
RU	2,013
ZH	5,059
JA	25
TR	646

A large post total cannot establish a large incident total. Global catalogues can list South Korea alongside many other markets. Replies, mirrors and renewed offers can continue without a new intrusion.

Use the case evidence for decisions about a particular claim. Use aggregate volume to describe the retained source population. Neither alone establishes how much harm occurred in South Korea or how visible an organisation would be to an adversary.

4.3 Eight claim cases

CASE A

A

Lending data advertised with inconsistent sale narratives

Evidence card B01 | 11 Mar 2026 | Forum | a financial-services organisation

Claim unverified

CLAIM	March posts advertise a 2 TB lending dataset. Korean text describes identity, contact, home, work and borrowing-related fields, with a claimed current date in March. [S1]
CHRONOLOGY	Related posts on 2026-03-10 and 2026-03-11 describe both exclusive-sale and public-release contexts. They do not establish separate intrusions.
ESTABLISHED EVIDENCE	The retained material supports the existence of related advertisements. It does not authenticate the information or establish which party first obtained it.
ALTERNATIVES	A genuine new file, older material, aggregation, resale or inaccurate advertising remain possible. Different sale narratives do not establish a completed exclusive transaction.
RESPONSE	The relevant lender and processors should compare any lawfully available evidence with their own export schemas and access records. Fraud teams should review recovery processes that rely on the advertised biographical fields.

Bottom line

Validate provenance, ownership and relevant internal evidence before choosing containment or notification.

Evidence card B01 — 11 Mar 2026

FantancyHacker | Forum | Forum | Korean

ORIGINAL

이름, 주민번호, 전번, 집주소, 거주지, 직장직위, 돈 빌린 이유, 동거자 기타 ...

TRANSLATION

Name, national ID number, phone number, home address, residence, workplace position, reason for borrowing, cohabitants and other information.

Note. Advertisement or source assertion; not independently authenticated.

Held

A retained post describes loan database sale and release, attributed to a financial-services organisation. The advertised contents remain unverified.

Not established

Authentic files, a new intrusion, active access, a completed transaction, unique affected people or a shared operator.

B

CASE B

Healthcare row counts do not identify a patient population

Evidence card B02 | 14 Jan 2026 | Forum | a healthcare organisation

Claim unverified

CLAIM	A January advertisement describes a hospital-related database. Its title, overall body quantity and patient-table quantity differ. [S1]
ESTABLISHED EVIDENCE	The body lists 34,438 patient rows alongside other account, event and operational rows. Its broader 1.5 million figure cannot be treated as patients or unique people.
ALTERNATIVES	The post may describe several tables about overlapping individuals, an older export or inaccurate contents. The displayed narrative does not settle provenance or freshness.
LIMITS	A related offer of administrative access is also a claim. The report does not establish active access to a clinical service.
RESPONSE	The data owner should establish which categories and people are actually represented, then assess clinical continuity and notification separately. Do not size a customer notice from the largest advertised total.

Bottom line

Validate provenance, ownership and relevant internal evidence before choosing containment or notification.

Evidence card B02 — 14 Jan 2026

Solonik | Forum | Forum | English

ORIGINAL

34,438 records

Note. Advertisement or source assertion; not independently authenticated.

Held

A retained post describes hospital SQL dump claim, attributed to a healthcare organisation. The advertised contents remain unverified.

Not established

A unique-patient total, current administrative access, authenticated files or a verified intrusion date.

CASE C

C

An access offer is challenged within its own thread

Evidence card B03 | 11 Mar 2026 | Forum | a public-sector body

Claim unverified

CLAIM	A March seller advertises privileged access attributed to a public-sector environment and invites offers. [S1]
ESTABLISHED EVIDENCE	Another participant challenges whether the displayed system information identifies the stated target. The seller clarifies that the offer concerns access rather than a database or traffic service.
ALTERNATIVES	Genuine access, misattributed infrastructure, generic demonstration material or false advertising remain possible. The challenge is relevant but does not prove fabrication.
LIMITS	Successful lateral movement, database theft and the identity of the operator are not established.
RESPONSE	A potentially relevant public body should validate account and host ownership privately, preserve access evidence and investigate any corroborated privileged session. A forum assertion alone is insufficient for a public breach statement.

Bottom line

Validate provenance, ownership and relevant internal evidence before choosing containment or notification.

Evidence card B03 — 11 Mar 2026

zSenior | Forum | Forum | English

ORIGINAL

i am selling the Full Access Only

Note. The source thread includes a participant challenge to the access proof.

Held

A retained post describes claimed privileged server access, attributed to a public-sector body. The advertised contents remain unverified.

Not established

Government ownership, successful lateral movement, information theft, usable access or a completed sale.

CASE D

D

Several business systems appear in one offer

Evidence card B04 | 26 Apr 2026 | Forum

a membership organisation and affiliated employers

Claim unverified

CLAIM	An April advertisement combines membership, account, business-management, human-resources and employee-document material. It offers shared and exclusive terms. [S1]
ESTABLISHED EVIDENCE	The post describes several related services and different claimed export dates. That supports one multi-system offer, not a confirmed incident at every named affiliate.
ALTERNATIVES	Shared administration, a common processor, unrelated files assembled for sale, older backups or inaccurate descriptions could explain the bundle.
LIMITS	Ownership, file authenticity, access freshness and exclusivity are unverified. A seller's assertion that material was never previously exposed is not independent evidence.
RESPONSE	Identify which business and supplier relationships could hold the described categories. Review privileged access and export permissions across those relationships before assuming a common entry point.

Bottom line

Validate provenance, ownership and relevant internal evidence before choosing containment or notification.

Evidence card B04 — 26 Apr 2026

0xCAFE | Forum | Forum | English

ORIGINAL

All of the data never exposed to public ever, and never used.

Note. Advertisement or source assertion; not independently authenticated.

Held

A retained post describes multi-system database and employee-document sale, attributed to a membership organisation and affiliated employers. The advertised contents remain unverified.

Not established

Authentic files, a new intrusion, active access, a completed transaction, unique affected people or a shared operator.

CASE E

E

Remote administrative access offered for a price

Evidence card B05 | 28 Apr 2026 | Forum | an insurance-sector organisation

Claim unverified

CLAIM	An April seller offers privileged remote access attributed to an insurance-sector organisation, asking 898 USD. [S1]
ESTABLISHED EVIDENCE	The advertisement describes a remote-work environment and asserted privilege. The report establishes the offer rather than usable access or ownership of the account.
ALTERNATIVES	An expired account, a supplier environment, a mislabelled target or a genuine active session remain possible.
LIMITS	The seller's operational and business descriptors are unverified. They are not reproduced as a victim profile.
RESPONSE	A relevant insurer should confirm its remote-access estate, privileged accounts and sessions. Contain corroborated unauthorised use under the incident process, rather than resetting a whole sector on the advertisement alone.

Bottom line

Validate provenance, ownership and relevant internal evidence before choosing containment or notification.

Evidence card B05 — 28 Apr 2026

TunaFish | Forum | Forum | English

ORIGINAL
$898 (BTC)

Note. Advertisement or source assertion; not independently authenticated.

Held
A retained post describes privileged remote-access sale, attributed to an insurance-sector organisation. The advertised contents remain unverified.

Not established
Authentic files, a new intrusion, active access, a completed transaction, unique affected people or a shared operator.

CASE F

F

A separate cloud-administrator offer

Evidence card B06 | 23 Aug 2026 | Forum | an insurance-sector organisation

Claim unverified

CLAIM	An August post advertises cloud-owner access attributed to an insurer labelled South Korea. [S1]
ESTABLISHED EVIDENCE	The retained description states a cloud-administrator privilege. Network size, account ownership, current validity and a transaction are not established.
RELATIONSHIP LIMIT	Nothing in the retained evidence links this offer to Case E. A common sector does not establish the same target, seller or access route.
RESPONSE	Cloud and identity teams should validate relevant administrator accounts, recent role changes and sensitive API activity. Review standing credentials and recovery paths where internal evidence corroborates the alert.

Bottom line

Validate provenance, ownership and relevant internal evidence before choosing containment or notification.

Evidence card B06 — 23 Aug 2026

HighWayToShell | Forum | Forum | English

ORIGINAL

Privilege ..... Cloud Admin (Owner)

Note. Advertisement or source assertion; not independently authenticated.

Held

A retained post describes cloud administrator access offer, attributed to an insurance-sector organisation. The advertised contents remain unverified.

Not established

Authentic files, a new intrusion, active access, a completed transaction, unique affected people or a shared operator.

CASE G

G Technical documents advertised during the closing fortnight

Claim unverified

Evidence card B07 | 12 Nov 2026 | Forum | a defence-sector supplier

CLAIM	A 2026-11-12 post advertises technical documents attributed to a defence-sector supplier. Its title gives 536 G as the claimed volume. [S1]
ESTABLISHED EVIDENCE	The seller describes electronic-warfare and radar-related information and asserts business relationships. The report holds the advertisement, without authenticating the documents.
LIMITS	Claimed customer relationships do not create additional confirmed victims. No transfer, ongoing access or state attribution is established.
RESPONSE	A potentially relevant supplier should involve engineering and data owners, check controlled technical repositories and preserve access evidence. Assess contractual and disclosure duties from verified information categories.

Bottom line

Validate provenance, ownership and relevant internal evidence before choosing containment or notification.

Evidence card B07 — 12 Nov 2026

taltikgoo | Forum | Forum | English

ORIGINAL

We have obtained [a defence-sector supplier's] complete set of technical documents, including data on its electronic warfare and radar equipment.

Note. Advertisement or source assertion; not independently authenticated.

Held

A retained post describes technical-document sale claim, attributed to a defence-sector supplier. The advertised contents remain unverified.

Not established

Authentic technical documents, a customer intrusion, a transfer, continuing access or state attribution.

H

CASE H

Procurement categories cannot be added into people

Evidence card B08 | 19 Nov 2026 | Forum | an energy-sector organisation

Claim unverified

CLAIM	A 2026-11-19 post advertises personal, supplier, bidding and contract records attributed to an energy-sector organisation. [S1]
ESTABLISHED EVIDENCE	The advertisement describes multiple categories, including internal users and supplier-related records. The categories can overlap and mix people, companies and transactions.
LIMITS	Its title's size expression is ambiguous. It does not establish hundreds of millions of people, and the category figures are not a unique-person total.
OFFICIAL-SOURCE BOUNDARY	A later public disclosure concerning an energy-sector organisation is discussed separately in Chapter 5. Similar themes or field names do not authenticate the advertised file or establish the same acquisition.
RESPONSE	The relevant data owner should reconcile internal users, external users, suppliers and procurement records separately. Investigate corroborated access and assess affected people before publishing a population figure.

Bottom line

Validate provenance, ownership and relevant internal evidence before choosing containment or notification.

Evidence card B08 — 19 Nov 2026

Noiem | Forum | Forum | English

ORIGINAL

Internal user PII 48,697

Note. Advertisement or source assertion; not independently authenticated.

Held

A retained post describes personal and procurement dataset claim, attributed to an energy-sector organisation. The advertised contents remain unverified.

Not established

A unique-person total, additive categories, file authenticity or a proven match to a later official disclosure.

4.4 Additional offers and recirculated material

Card	Post date	Observed claim	Limit
B09	2026-01-13	Hosted-service data claim	A hosting name and apparent tenant records do not establish provider-wide access
B10	2026-03-01	Population/trader release claim	Older profile dates and a bulk title do not establish a new national-register intrusion
B11	2026-03-10	Professional and manufacturing release claim	Two organisations in one statement do not establish one intrusion
B12	2026-03-30	Large data-line offer	Lines are not verified unique people; no government origin established
B13	2026-03-31	Large community-data advertisements	Templated descriptions and illustrative samples leave scale and authenticity unresolved
B14	2026-04-03	Business-system dataset offers	Similar schemas do not establish a shared backend or completed transactions
B15	2026-05-28	Technical-document release claim	A file-size assertion does not establish provenance or state attribution

Card	Post date	Observed claim	Limit
B16	2026-07-06	Automotive data offer	Ambiguous source chronology prevents a fresh-intrusion conclusion
B17	2026-08-23	Life-sciences business-document claim	A partial archive and older listing overlap leave origin and original incident date unresolved
B18	2026-09-09	Telecommunications data offer	Estimated quantity and original incident date remain unverified
B19	2026-10-07	Commerce customer-data circulation	A later sample remains part of a continuing claim family
B20	2026-10-17	Academic recruitment and staff tables	Older sample dates and different row categories prevent a new unique-person total
B21	2026-11-08	Recent customer relationship management (CRM) administrator claim	A claimed export and proposed schema do not establish active access
B22	2026-11-10	Recent education-services administrator offer	Platform and customer-data assertions remain unverified
B23	2026-11-17	Older member material in a November post	Title date does not establish current account validity or new theft
B24	2026-11-21	Recent financial-services dataset advertisement	Record quantity, payment-like samples and asking price do not authenticate the file or establish affected people

Evidence card B09 — 13 Jan 2026

Solonik | Forum | Forum | English

ORIGINAL

82 structured MySQL tables, ~144,000 rows total

Note. Advertisement or source assertion; not independently authenticated.

Held

A retained post describes database dump claim, attributed to a hosted-service environment. The advertised contents remain unverified.

Not established

Authentic files, a new intrusion, active access, a completed transaction, unique affected people or a shared operator.

Evidence card B10 — 1 Mar 2026

INDOHAXSEC | Forum | Forum | English

ORIGINAL

514.475 SOUTH KOREAN POPULATION AND TRADER DATA

Note. Advertisement or source assertion; not independently authenticated.

Held

A retained post describes bulk personal-data release claim, attributed to a national consumer/trader dataset. The advertised contents remain unverified.

Not established

Authentic files, a new intrusion, active access, a completed transaction, unique affected people or a shared operator.

Evidence card B11 — 10 Mar 2026

ZeusHacking | Forum | Forum | Korean

ORIGINAL

[an aerospace organisation]과 [a professional-services organisation]의 데이터를 무료 공개.

TRANSLATION

Data attributed to [an aerospace organisation] and [a professional-services organisation] released free.

Note. Advertisement or source assertion; not independently authenticated.

Held

A retained post describes Korean-language free-release claim, attributed to professional-services and manufacturing organisations. The advertised contents remain unverified.

Not established

Authentic files, a new intrusion, active access, a completed transaction, unique affected people or a shared operator.

Evidence card B12 — 30 Mar 2026

GlitchX | Forum | Forum | English

ORIGINAL

Total records: 9 Million Lines

Note. Advertisement or source assertion; not independently authenticated.

Held

A retained post describes national population database offer, attributed to a consumer dataset. The advertised contents remain unverified.

Not established

Authentic files, a new intrusion, active access, a completed transaction, unique affected people or a shared operator.

Evidence card B13 — 31 Mar 2026

xorcat | Forum | Forum | English

ORIGINAL

Records: 15,000,000+ users

Note. Advertisement or source assertion; not independently authenticated.

Held
A retained post describes large database advertisements, attributed to community and discussion services. The advertised contents remain unverified.

Not established
Authentic files, a new intrusion, active access, a completed transaction, unique affected people or a shared operator.

Evidence card B14 — 3 Apr 2026

Grubber | Forum | Forum | English

ORIGINAL

Price: $1000

Note. Advertisement or source assertion; not independently authenticated.

Held
A retained post describes three customer relationship management (CRM)-style database sale offers, attributed to commerce and education services. The advertised contents remain unverified.

Not established
Authentic files, a new intrusion, active access, a completed transaction, unique affected people or a shared operator.

Evidence card B15 — 28 May 2026

Forum participant | Forum | Forum | English

ORIGINAL

South Korea [...] UAV [...] Documents [...] Size: 3.8 GB

Note. Advertisement or source assertion; not independently authenticated.

Held
A retained post describes technical-document release claim, attributed to a defence-related dataset. The advertised contents remain unverified.

Not established
Authentic files, a new intrusion, active access, a completed transaction, unique affected people or a shared operator.

Evidence card B16 — 6 Jul 2026

AshleyWood2022 | Forum | Forum | English

ORIGINAL

Full information [...] Database [...] South Korea 150K

Note. The source chronology is ambiguous; the displayed date does not establish a new intrusion.

Held
A retained post describes database sale claim, attributed to an automotive sales platform. The advertised contents remain unverified.

Not established
Authentic files, a new intrusion, active access, a completed transaction, unique affected people or a shared operator.

Evidence card B17

23 Aug 2026

updap | Forum | Forum | English

ORIGINAL

This is a partial data with dumped files from the company

Note. Advertisement or source assertion. Older extortion-listing overlap leaves the original incident date unresolved.

Held

A retained post describes business and employee-document release claim, attributed to a pharmaceutical-sector organisation. The advertised contents remain unverified.

Not established

Authentic files, a new intrusion, active access, a completed transaction, unique affected people or a shared operator.

Evidence card B18

9 Sep 2026

REDX | Forum | Forum | English

ORIGINAL

Estimated Records: [quantity withheld] (reported)

Note. Advertisement or source assertion; not independently authenticated.

Held

A retained post describes subscriber database sale claim, attributed to a telecommunications organisation. The advertised contents remain unverified.

Not established

Authentic files, a new intrusion, active access, a completed transaction, unique affected people or a shared operator.

Evidence card B19

7 Oct 2026

updap | Forum | Forum | English

ORIGINAL

Customers database Total Records: +1m unique records

Note. Advertisement or source assertion; not independently authenticated.

Held

A retained post describes customer database release claim, attributed to an e-commerce organisation. The advertised contents remain unverified.

Not established

Authentic files, a new intrusion, active access, a completed transaction, unique affected people or a shared operator.

Evidence card B20

17 Oct 2026

updap | Forum | Forum | Chinese and Korean annotations

ORIGINAL

[recruitment records] 第 7,806 行 [teaching records] 第 1902 行 [staff records] 第 1,569 行

TRANSLATION

Recruitment, teaching and staff samples carry row labels 7,806, 1902 and 1,569.

Note. Row labels do not establish total records or unique people; older sample dates remain relevant.

Held

A retained post describes recruitment and staff database sample, attributed to an education-sector organisation. The advertised contents remain unverified.

Not established

Authentic files, a new intrusion, active access, a completed transaction, unique affected people or a shared operator.

Evidence card B21 8 Nov 2026

DataJava Forum Forum English

ORIGINAL

this is an admin-side export rather than a scrape.

Note. Advertisement or source assertion; not independently authenticated.

Held

A retained post describes CRM administrator and member-data sale, attributed to a digital-services organisation. The advertised contents remain unverified.

Not established

Authentic files, a new intrusion, active access, a completed transaction, unique affected people or a shared operator.

Evidence card B22 10 Nov 2026

DataJava Forum Forum English

ORIGINAL

Access: full admin account in [an e-commerce administration environment].

Note. Advertisement or source assertion; not independently authenticated.

Held

A retained post describes administrator access and customer-record sale, attributed to an education-services organisation. The advertised contents remain unverified.

Not established

Authentic files, a new intrusion, active access, a completed transaction, unique affected people or a shared operator.

Evidence card B23 17 Nov 2026

thisversace Forum Forum English

ORIGINAL

Databases From Korea [a consumer-services organisation] 17.11.2026

Note. The visible sample includes older registration and login dates.

Held

A retained post describes member database circulation, attributed to a consumer-services organisation. The advertised contents remain unverified.

Not established

A new incident on the title date, current account validity, a reliable population count or authentic origin.

Evidence card B24 21 Nov 2026

tet Forum Forum English

ORIGINAL

Total records : 43.19M Price : 500 $

Note. An advertisement, with the exact source time unresolved. Repetitive sample patterns raise authenticity questions without establishing fabrication.

Held

A financial-services dataset advertisement claims 43.19M records and asks 500 USD. The quantity is an advertised record count, not verified people or payments.

Not established

Authenticated files, active access, valid payments, a completed sale or 43.19M affected people.

Source: [S1].

The age of a sample can establish that some included material is older; it cannot establish the age of every row in the advertised file. A title dated in 2026 likewise cannot establish a new incident. Preserve both limits.

A separate 2026-03-23 post advertises VPN access associated with a maritime or logistics organisation for 10,000 USD. Identity, active access and a completed transaction are unverified. Nearby channel names do not establish the seller's affiliation. [S1]

A repeated academic-infrastructure offer observed on 2026-10-13 asks 300 USD and describes privileged host access. The advertised privilege, asset relationship and live access remain unverified. Repetition does not establish another intrusion or a completed transaction. [S1]

Repeated public-transport website access advertisements appear across September and October. They do not establish valid access, aviation operations or flight-system access. Owners should reconcile the advertised asset with the particular web application before deciding scope or containment. [S1]

An earlier maritime-themed offer dated 2026-01-17 asks 50,000 USD. Its relationship to the later access advertisement, access validity and any transaction remain unverified. Municipal website-access advertisements likewise require asset-specific validation; they do not establish government-wide access. [S1]

4.5 Recent activity: 2026-11-08 through 2026-11-22

Card	Date	Role	Evidence status
B07	2026-11-12	a defence-sector supplier	Advertisement or circulation; contents unverified
B08	2026-11-19	an energy-sector organisation	Advertisement or circulation; contents unverified
B21	2026-11-08	a digital-services organisation	Advertisement or circulation; contents unverified
B22	2026-11-10	an education-services organisation	Advertisement or circulation; contents unverified
B23	2026-11-17	a consumer-services organisation	Advertisement or circulation; contents unverified
B24	2026-11-21	a financial-services dataset	Advertisement or circulation; contents unverified

The administrator offers, technical documents, procurement records and older member material describe different claims. They are not added into affected people or connected to a single operator. [S1]

A 2026-11-16 advertisement lists a municipal website among several international entries. It does not establish the same access as earlier offers, a new intrusion date or operator-wide scope. Treat the particular advertised asset as a separate validation task. [S1]

The recent section describes publications and offers. It does not infer when information was first obtained. Where a post's chronology is inconsistent with earlier observations, it is not used as evidence of a fresh attack in this interval.

KEY TAKEAWAYS

01

Keep offered access, advertised information and confirmed incidents separate.

02

Resolve claimed units and provenance before sizing impact.

03

Treat a recent publication as a validation prompt, not proof of a recent intrusion.

CHAPTER 05

Public incidents and targeting by sector

05

THIS CHAPTER ANSWERS

What did organisations and authorities actually report, and how does that change the response?

2

clocks beside every case: the event and its disclosure

5.1 Sector response map 47
5.2 Early-year incidents and campaign warnings 48
5.3 Administrator, developer and software-supply-chain campaigns 49
5.4 Consumer services and public-sector campaign reporting 52
5.5 Criminal extortion and the AI claim 54
5.6 Recent activity: 2026-11-08 through 2026-11-22 55
5.7 Recent technical advisories are not victim incidents 61
5.8 Follow-ups and exclusions 61
5.9 The decision across sectors 62

CHAPTER 05

Public incidents and targeting by sector

IN SHORT

Public evidence spans ransomware, phishing, business-application exposure and supplier dependencies. Campaign notices and policy announcements are distinct from confirmed incidents. Recent disclosures also include an accidental document release and earlier activity newly reported in November. Use the case's established mechanism and affected information to choose the owner, and retain unresolved scope beside every response decision.

5.1 Sector response map

The rows combine distinct evidence types without merging them into incident totals. Unverified claims remain labelled. Related services and small sectors are grouped to avoid unsupported comparisons.

Sector	Supported example	Evidence type	First response
Public administration	QR lures, impersonation and a shared-mail investigation	Official campaign notices and disclosure	Verify workflow, sessions and service scope
Finance and insurance	Dated sector reports, assessment-system exposure and separate access advertisements	Official reporting plus unverified claims	Review interfaces and validate accounts
Education and research	Teaching, research and administrative portal disclosures	Official notices and attributed reporting	Preserve access logs and reconcile record categories
Industry and defence	Technical-document offers; developer and administrator lures	Claims and official campaign warnings	Engage engineering and privileged-access owners
Energy and infrastructure	Personal/procurement-data claims and a separate public disclosure	Claim and official account kept separate	Reconcile affected systems and information
Communications and consumer services	Streaming-service investigation and fake installer distribution	Regulator and CERT reporting	Review database access and customer messaging
Health and life sciences	Healthcare data offer and official ransomware warnings	Unverified claim and campaign evidence	Separate clinical continuity from information impact
Transport and travel	Booking information reused in payment messages	Official warning	Verify payment requests through known contacts
Business suppliers	Training and shared-service access disclosures	Company statements reported by press	Identify controller records and supplier evidence

5.2 Early-year incidents and campaign warnings

CASE I

I Education-group disruption, with the data scope still developing

Education and business services

Official disclosure; scope qualified

OFFICIAL ACCOUNT	A company notice published on 2026-01-12 describes abnormal internal-system activity detected on 2026-01-10. It reports isolation and an investigation into suspected ransomware. [S49][S50]
LATER REPORTING	A 2026-01-14 report describes a company update acknowledging some stolen data while customer-information inclusion remained unresolved. Large membership figures are not a confirmed exfiltration count. [S47]
RESPONSE	Test restoration and customer-data assessment as separate workstreams. Keep the earliest discovery, later technical finding and evolving population distinct in communications.

Bottom line

Follow the stated mechanism and information scope; preserve date, population and attribution limits in the response.

Additional disclosure: clinical imaging availability

National reporting on 2026-01-27 describes a hospital's 2026-01-26 ransomware incident affecting image-reading workflows, with restoration that afternoon. At publication, it reported no patient-data disclosure or surgery and treatment interruption. These are the dated report's scope statements. [S104]

CASE J

J Government-themed QR codes move the decision to a phone

Government-themed impersonation

Official campaign account; local extent unresolved

OFFICIAL ACCOUNT	KISA's 2026-01-10 notice describes QR-code lures impersonating government and think-tank personnel. The intended outcomes include malicious mobile-app installation or credential entry. [S19]
LIMIT	The notice establishes detected campaign behaviour, without enumerating a national victim population or proving that the impersonated bodies were entered.

RESPONSE	Verify document and payment workflows through known contacts. Apply the same scrutiny to a QR destination as to a clickable email link, and provide an approved reporting route for mobile users.

Bottom line

Follow the stated mechanism and information scope; preserve date, population and attribution limits in the response.

KISA's 2026-01-06 notice also describes forum-associated indications involving domestic websites. Its February warning focuses on ransomware risks affecting healthcare, education and ICT. These are campaign observations and warnings, rather than a count of distinct confirmed organisations. [S18][S20]

5.3 Administrator, developer and software-supply-chain campaigns

K

CASE K

Useful-looking utilities target privileged users

Administrator and developer tools

Official campaign account; local extent unresolved

OFFICIAL ACCOUNT	KISA's 2026-03-11 notice describes malicious installers impersonating common administrator and developer utilities, distributed through public code-hosting services and promoted through search results. [S21]
LIMIT	The notice does not establish that every user who viewed a repository installed the software, or enumerate affected Korean organisations.
RESPONSE	Use approved acquisition routes for privileged utilities. Review unexpected installer, script and outbound activity on administrator workstations, and validate exposed sessions where corroborating evidence exists.

Bottom line

Follow the stated mechanism and information scope; preserve date, population and attribution limits in the response.

CASE L

L ■ A global developer campaign receives an official Korean warning

Software supply chain

Official campaign account; local extent unresolved

OFFICIAL ACCOUNT	The 2026-04-01 warning concerns developer-tool and package-supply-chain propagation. The 2026-05-20 notice adds further activity to that account. [S23][S27]
COUNTING BOUNDARY	The later notice is an update to the campaign. An official Korean advisory about a global event does not establish a Korean victim total or a separate local incident on each publication date.
RESPONSE	Development owners should identify relevant dependencies, build credentials and release permissions. Where an exposed secret is confirmed, replace and revoke it, then inspect access and build integrity.

Bottom line

Follow the stated mechanism and information scope; preserve date, population and attribution limits in the response.

CASE M

M ■ A familiar messaging installer is impersonated

Consumer software impersonation

Official campaign account; local extent unresolved

OFFICIAL ACCOUNT	KISA's 2026-04-15 notice describes fake download pages and information-stealing malware. It estimates roughly 560 malicious downloads between 2026-02-10 and 2026-04-14. [S24]
LIMIT	Downloads do not identify unique people or successful infections. Impersonation does not establish an intrusion into the legitimate product provider.
RESPONSE	Confirm the software's acquisition route, inspect endpoint activity and validate sessions after corroborated malware exposure. Provide staff with a known installation source.

Bottom line

Follow the stated mechanism and information scope; preserve date, population and attribution limits in the response.

CASE N

N Email-led ransomware against smaller businesses

Small and medium businesses

Official campaign account; local extent unresolved

OFFICIAL ACCOUNT	KISA's 2026-04-16 notice describes increased ransomware harm at domestic small and medium businesses, including malicious document attachments and impersonated installation guidance. [S25]
LIMIT	The notice identifies a threat pattern without providing a national denominator or establishing a single operator behind every case.
RESPONSE	Combine attachment and endpoint controls with an isolated restoration test. Include business email and identity recovery, rather than testing files alone.

Bottom line

Follow the stated mechanism and information scope; preserve date, population and attribution limits in the response.

CASE Q

Q AI-tool impersonation and developer credentials

Developer tools

Official campaign account; local extent unresolved

OFFICIAL ACCOUNT	KISA's 2026-07-16 notice describes repositories and pages impersonating AI development tools, with malicious download links. A companion warning concerns exposed developer credentials. [S30][S31]
SUPPORTING CONTEXT	PIPC's June guidance explains the personal-data consequences of exposed cloud and collaboration credentials. It is prevention guidance, rather than an incident count. [S36]
RESPONSE	Review approved development-tool sources, repository secrets and cloud roles. Removing a visible secret from a file does not revoke its authority; replacement and access review are necessary where exposure is established.

Bottom line

Follow the stated mechanism and information scope; preserve date, population and attribution limits in the response.

Additional disclosure: service restoration and later ransomware classification

ActionPower's Daglo service notice, published on 2026-03-27, dates a security anomaly to 2026-03-22 around noon. It describes protective service shutdown and restoration of all functions by 2026-03-23 at 08:00. [S98]

Yonhap's 2026-04-09 report quotes the company's later classification of the event as ransomware. The company said its investigation found no indication of user personal-information, recording or core-company-data disclosure. It acknowledged old, discarded and some employee-held sample material. [S99]

These are the company's qualified findings, reported with the stated investigative support. They do not establish zero exposure. National reporting also connects the service to ActionPower; it does not authenticate every tracker label or claimed file volume. [S100]

The March monitoring posts repeat a Crypto24 claim. The claimant label remains separate from the company's confirmed event and information-scope account. Different channel repetitions do not create additional incidents. [S1]

Service owners should preserve restoration times, identify the material actually disclosed and revoke relevant access according to their own evidence. A subsequent classification should update the incident record without rewriting the original notice.

5.4 Consumer services and public-sector campaign reporting

CASE O

Database access and a separate secondary-fraud warning

Consumer services

Official disclosure; scope qualified

OFFICIAL ACCOUNT	PIPC's 2026-06-04 notice describes a streaming provider's report following database access detected on 2026-06-02. The regulator's notice does not finalise the affected population. [S35][S51]
BOUNDARY	Some fields were encrypted, but that does not establish that every exposed field was protected or that all information was unusable.
RESPONSE	Establish the actual records and encryption context, restrict the access path and assess notification. KISA's separate warning about compensation and refund lures supports trusted-channel customer advice. [S28]

Bottom line

Follow the stated mechanism and information scope; preserve date, population and attribution limits in the response.

CASE R

R

A joint warning describes more than one delivery route

Cross-sector campaign

Official campaign account; local extent unresolved

OFFICIAL ACCOUNT	A 2026-07-30 joint notice by Korean cyber, intelligence, police and financial-security bodies describes recruitment or resume phishing and smaller websites used as malware-distribution footholds. [S32]
ATTRIBUTION BOUNDARY	The notice's state-backed framing belongs to those sources. It does not assign every component to a named group or establish a shared operator for the report's criminal advertisements.
RESPONSE	Protect recruitment and document workflows, review unexpected website changes and correlate endpoint behaviour with account activity. Do not infer state attribution from a Korean-language lure alone.

Bottom line

Follow the stated mechanism and information scope; preserve date, population and attribution limits in the response.

A separate public-sector training disclosure, reported in July, concerns access beginning in 2025 and continuing into February 2026. The ministry's account left the exact exposed content unresolved. Turkish reporting supplies additional language coverage, rather than another incident or a final population total. [S52][S53]

KISA's September warning describes public-agency and financial-company impersonation using alleged legal violations, criminal involvement or breach compensation. This is a campaign against recipients, rather than proof of entry into the impersonated institutions. [S55]

Additional disclosure: sensitive information in an asset-handling workflow

The National Tax Service's 2026-03-01 apology concerns original press photographs supplied during a 2026-02-26 briefing. The agency confirmed that the photographs contained sensitive virtual-asset information and that coins left the taxpayer's wallet. It requested a police investigation. [S101]

National reporting describes a token quantity and nominal valuation with material liquidity uncertainty. This report does not adopt that quoted valuation as realised net loss. A reported return account also remained under verification in the accepted follow-up. [S102][S103][S105]

This is an accidental sensitive-information disclosure and custody-control case. It is separate from earlier reports about other seized assets. Communications and asset-custody teams should independently review publication material for secrets before release and preserve an approved evidence copy.

Additional disclosure: business documents across two exposure windows

National reporting describes an entertainment group's account of external access during 2026-09-12–2026-09-13 and 2026-10-03–2026-10-05. The described routes concerned document-preview functionality and expense processing, rather than an established common campaign. [S111][S112]

The reports attribute the exposure of some internal documents and personal information to the company's notice. The described populations include some current and former employees and partner personnel. Categories vary by person, and an affected-person total is not established.

This account does not establish that the external software supplier was itself attacked or identify a particular vulnerability. Application owners should inventory preview and export functions, establish which records they can reach and preserve evidence for each exposure window.

Additional disclosure: a separately confirmed university portal event

Yonsei University's 2026-10-22 notice confirms portal information exposure during two windows on 2026-10-20 and 2026-10-21. It describes university identifiers, contact and affiliation information, and account-management metadata. Fields vary by person; the notice supplies no affected-person total. [S117]

The university describes blocking access routes, reporting to authorities and notifying affected members. Dailysecu and NewsPim corroborate the portal disclosure. The information categories do not establish raw-password disclosure or privileged shell access. [S118][S119]

No opened source connects this portal event to earlier access-sale advertisements. Account owners should follow the confirmed information scope and notification, while treating unverified offers as separate validation tasks.

5.5 Criminal extortion and the AI claim

W

CASE W

Police allegations span two calendar years

Multi-sector extortion allegations

Press-reported account; scope qualified

REPORTED POLICE ACCOUNT	MBC's 2026-10-26 report describes allegations involving roughly 90 organisations and more than 8.2 million records during September 2025–October 2026. [S43]
CHRONOLOGY	Police reportedly assessed that intensive generative-AI use began in late August, followed by an alleged acceleration in activity. That does not make every earlier alleged intrusion AI-driven.
RELATIONSHIP LIMIT	The account does not establish that these suspects caused the entire financial-sector disclosure population or every advertisement in this report.

RESPONSE	Prioritise authorisation, exposed accounts and evidence preservation according to the actual access route. AI-related descriptions should not displace the ordinary controls that prevent or reveal access.

Bottom line

Follow the stated mechanism and information scope; preserve date, population and attribution limits in the response.

KISA's October response warning likewise emphasises externally reachable applications, access controls, exposed credentials and information-transfer monitoring.

Its November network-attached storage (NAS) warning supports separate backups and controlled external access. Neither supplies a complete national victim total. [S33][S34]

5.6 Recent activity: 2026-11-08 through 2026-11-22

The closing period contains separate disclosures and updates. Dates below identify the relevant event or publication, rather than a common campaign.

Disclosure	Established scope	Event or discovery	Boundary
Financial Security Institute	Assessment-service forms and information	Detected 2026-11-09; disclosed 2026-11-10	Categories are not unique people; Case P, Chapter 9
University teaching service	24,011 records in the reported official account	Discovered 2026-11-12; notice 2026-11-13	Password and national-ID exclusions belong to that account
Employee-training service	Unauthorised cloud access; provisional population	Access 2026-11-09; reported to the regulator 2026-11-11	Approximate initial scope remains provisional
Public voucher service	API-related personal-information access	Detected 2026-11-13; press account 2026-11-16	No reported voucher theft at publication
Research-university portals	Three disclosed record populations	Attack 2026-11-13; notices 2026-11-19 and 2026-11-20	Records can overlap; Case U
Additional closing-day disclosures	Education, shared-mail, energy, supplier and logistics disclosures	Publications through 2026-11-22; underlying dates differ	Separate cases and updates; details and qualifications below

S

CASE S

Teaching-service information, with explicit exclusions

Education

Press-reported account; scope qualified

REPORTED OFFICIAL ACCOUNT	Yonhap reports a university's apology concerning a server used for teaching operations. The university said it identified 24,011 records involving student and staff identifiers and contact details. [S40]
LIMIT	The university's account excluded passwords and unique national identifiers at that time. The figure is not a count of all students or a finding that every campus system was affected.
RESPONSE	Preserve service access evidence, reconcile the affected records and provide trusted-channel advice about impersonation. Review the particular teaching service's privileges and supplier relationships.

Bottom line

Follow the stated mechanism and information scope; preserve date, population and attribution limits in the response.

T

CASE T

API access does not establish payment theft

Public payment-related service

Press-reported account; scope qualified

REPORTED OFFICIAL ACCOUNT	A public voucher-service operator attributed information access to an API authentication weakness. Its November statement reported 3,083 affected customers. [S41]
LIMIT	The operator said it had not identified voucher-balance theft or unauthorised payments at publication. Its suspicion about AI use remains the operator's assessment.
RESPONSE	Test the actual authorisation boundary and review information queries separately from transaction records. Preserve both information-access and payment evidence before declaring the outcome.

Bottom line

Follow the stated mechanism and information scope; preserve date, population and attribution limits in the response.

CASE U

U An additional portal changes the record total

Research and education

Official disclosure; scope qualified

OFFICIAL ACCOUNT	A research university's 2026-11-19 notice describes a 2026-11-13 intrusion, with 19,500 account-ID/encrypted-password records and 478 account-ID/email/affiliation records. [S44][S76]
UPDATE	Its 2026-11-20 notice adds 25,551 administrative-portal records. The arithmetic total is 45,529 records, rather than an established count of unique people. [S48]
RESPONSE	Reconcile people across applications, assess credential protection and preserve the successive notices. A later scope revision should update the response without erasing the first disclosure's evidence and timing.

Bottom line

Follow the stated mechanism and information scope; preserve date, population and attribution limits in the response.

CASE V

V Employee training exposes a supplier dependency

Employee training

Press-reported account; scope qualified

REPORTED ACCOUNT	Asia Economy reports a company's confirmation of unauthorised cloud access and the privacy regulator's receipt of a report. The story dates access to 2026-11-09 and reporting to the regulator to 2026-11-11. [S45]
LIMIT	An approximately 70,000-user figure was provisional. It should not become a final unique-person count or a separate incident for each corporate training customer.
RESPONSE	Employers should identify the records their training provider holds, confirm the relevant tenant and obtain evidence for their own privacy and staff-protection decisions.

Bottom line

Follow the stated mechanism and information scope; preserve date, population and attribution limits in the response.

CASE X

X

A university's additional notice expands categories without a new count

Education

Official disclosure; scope qualified

OFFICIAL ACCOUNT	A university's 2026-11-18 notice describes approximately 180,000 records, including approximately 25,000 with resident-registration numbers. It dates the event to 2026-11-16 and discovery to 2026-11-17. [S57]
UPDATE	Its 2026-11-22 notice adds academic and instructor-related information. It gives no additional population or deduplicated total. National reporting corroborates the earlier notice. [S56][S73][S74]
RESPONSE	Reconcile the newly identified categories with the earlier population and update advice for the actual information involved. Do not add an unspecified expansion to an invented total.

Bottom line

Follow the stated mechanism and information scope; preserve date, population and attribution limits in the response.

CASE Y

Y

Shared email access and the date of the public explanation

Public services

Official disclosure; scope qualified

OFFICIAL ACCOUNT	A public-service operator's explanation concerns abnormal access to approximately 300 administrative email accounts. It describes a path through local-government networks and a single-sign-on weakness. [S60]
CHRONOLOGY	The official explanation says the Ministry of the Interior and Safety received notification on 2026-11-09. National reporting appeared on 2026-11-16; the official web explanation was posted on 2026-11-17. A later article does not date a new attack. [S60][S61]
LIMIT	Investigation continued. The account does not establish that all public-sector mail was accessed or identify a common actor behind unrelated disclosures.
RESPONSE	Review authentication dependencies, relevant sessions and mailbox access records together. Separate the account population from messages, recipients and any later verified information exposure.

Bottom line

Follow the stated mechanism and information scope; preserve date, population and attribution limits in the response.

CASE Z

Z

Two energy-company service populations, not one deduplicated total

Energy and procurement

Press-reported account; scope qualified

REPORTED DISCLOSURE	National reporting on 2026-11-22 describes a company's disclosure concerning customer and procurement services, detected on 2026-11-20. The two reported system-user populations were 650,487 and 869,761. [S58][S78][S79]
COUNTING BOUNDARY	Their arithmetic sum is 1,520,248. It is not a verified deduplicated population across the two systems; information categories differ by record and person.
CLAIM BOUNDARY	The report's separate procurement-data advertisement remains unverified. Publication timing and overlapping themes do not establish that the offered file matches the disclosed information.
RESPONSE	Reconcile identities across the services, assess the actual exposed categories and preserve the successive statements. Customer protection should follow those facts, rather than an actor's title or the largest possible sum.

Bottom line

Follow the stated mechanism and information scope; preserve date, population and attribution limits in the response.

The following additional disclosures broaden the supplier and service picture without establishing a common campaign.

Disclosure	Supported distinction	First response	Sources
Startup-program supplier	The 818 program participants are a subset of the supplier-wide 20,028 population	Confirm the controller's actual records and processor notice	[S67][S68]
Logistics chatbot	Abnormal automated access was identified; actual information exposure and population remained unresolved	Preserve queries and validate the possible information scope	[S80][S81]
Regional university services	Library, employment, document and research-administration services appear in distinct disclosures	Identify the specific application and data owner	[S71]

Disclosure	Supported distinction	First response	Sources
School transport	Approximately 9,900 guardian-contact entries were reported; affected pupils and schools remained under assessment	Warn through trusted channels and reconcile the population	[S75]
Outsourced staff training	A financial institution's employee information was affected through a training provider; no core-bank access is established	Confirm the supplier tenant and staff-protection action	[S69]
Insurance processor	A report describes 66 customers in an October processor incident, disclosed through a November notice	Validate records and notification responsibilities	[S70]

The logistics notice is a possible-exposure account. It is not presented as a confirmed information-loss population. The startup supplier's web posting and press disclosure also carry different dates; the described discovery occurred earlier.

For the public-sector training incident, ministry briefings distinguish February recognition, subsequent analysis and later notification. The stored-information population is not a confirmed exfiltrated-person count. The report makes no legal-violation finding from that chronology. [S62][S63]

Additional recent disclosure: customer-support information at a contractor

MBC and Newsis report a financial service's 2026-11-15 account of customer-support contractor access on 2026-11-12. The described information depended on the customer's consultation history; the affected records and population remained under investigation. [S106][S107]

A separate provider report describes abnormal activity in some support systems and says information scope varies by client and person. The provider and client accounts concern different views of the contractor disclosure. Neither supports an all-users population or a general finding of realised phishing harm. [S108]

The account does not establish access to core transaction or wallet systems. Reconcile the actual consultation fields and affected records, then update trusted-channel customer guidance and suspicious-message handling according to those facts.

A November report quotes a manufacturer acknowledging a security incident involving an advertising-data vendor for its North American service business. Preliminary vendor work suggested some company information may have been affected; the investigation continued. This is not a blanket denial of impact. [S116]

An N0n-labelled listing and a separate 2026-11-22 Hyflock manufacturing claim remain distinct assertions. They do not establish the same affected entity, a common incident or two verified intrusions. The vendor account does not establish access to the manufacturer's own systems. [S1][S2]

5.7 Recent technical advisories are not victim incidents

The Java advisory published during the closing fortnight warrants an asset review. It does not establish a Korean organisation was attacked through the vulnerability. PIPC's warning focuses on preventing large personal-data exposure through linked systems and bulk access. [S11][S12][S13][S39]

The following release strings concern CVE-2026-114938. They are software versions, not network addresses. NVD records affected Oracle Java and GraalVM products, and also lists some Siemens industrial-edge and security-management products. KISA's current advisory supplies the corresponding fixed versions and distribution-specific guidance.

Product family	Affected listed release	Fixed listed release
Java 8 Enterprise Performance Pack	8u511b33-perf	8u513-perf
Oracle Java SE 17 / GraalVM JDK 17	17.0.21.0.3	17.0.21.1
Oracle Java SE 21 / GraalVM JDK 21	21.0.13.0.3	21.0.13.1
Oracle Java SE 25	25.0.5.0.3	25.0.5.1
Oracle Java SE 27	27.0.1.0.3	27.0.1.1
GraalVM Enterprise Edition	21.3.20.0.3	21.3.20.1

Earlier releases in a branch may also require attention. The exact distribution, package, hardware conditions and service runtime matter. Follow the relevant vendor's current guidance, then verify the running service after restarting or redeploying it.

NVD's Oracle-provided CVSS 3.1 score is 8.1. Scores quoted under a different CVSS version should not be substituted without naming the scale. A severity score does not establish observed exploitation or exposure at a particular organisation. [S12]

5.8 Follow-ups and exclusions

Publication	Correct interpretation	Treatment
July sanctions concerning three companies	Underlying incidents occurred in 2024	Regulatory context, not new 2026 attacks [S37]
November industrial-group sanction	Underlying intrusion occurred in July 2022	Enforcement context only [S38]
November education-office document notice	Accidental, limited-circulation disclosure concerning May submissions	Information-governance example, not hacking [S42]
Reposted older retail and member material	A 2026 post can contain earlier records	Recirculation, not a newly dated intrusion [S1]
Global developer and VPN advisories	Korean warning does not enumerate Korean victims	Defensive context with local extent unresolved [S23][S29]

The company's primary notice governs the January education-group discovery chronology. Translated or repeated reporting does not create a separate incident. [S49]

5.9 The decision across sectors

The cases show why a single category such as data breach is too coarse for response planning. A clinical service, a document repository, a training tenant and an assessment portal hold different information and support different business processes.

Ask what was reached, which privilege allowed it, what information was accessible and what service depends on the same identity. Those questions connect the technical finding to containment, continuity and privacy decisions.

Do not wait for an actor's final attribution to preserve evidence or close a verified access path. Equally, do not turn an advertisement or an unconfirmed population into a company finding. Use the action plan to assign both urgency and evidential responsibility.

KEY TAKEAWAYS

01

Keep event, detection, disclosure and enforcement dates distinct.

02

Reconcile applications and record populations before estimating affected people.

03

Let established access and business consequences determine the response owner.

CHAPTER 06

Hacktivism, DDoS and service continuity

06

THIS CHAPTER ANSWERS

How should a defender distinguish a disruption claim from a demonstrated service impact?

3

separate questions: reachability, data access and operational effect

6.1 Chronology without assumed causation 64
6.2 Claim against confirmation 65
6.3 An absence of confirmation has a narrow meaning 65
6.4 Additional actor claims and what they do not establish 66
6.5 Communications that survive changing evidence 67
6.6 Response ownership 67

CHAPTER 06

Hacktivism, DDoS and service continuity

IN SHORT

A website claim, a moment of unreachability and an operational interruption require different evidence. The retained material does not establish a common operator behind separate availability and data claims. Political slogans do not supply that missing link. Compare public claims with your own service telemetry, confirm any physical-process implication with the operator, and prepare a factual status message with a stated update time.

6.1 Chronology without assumed causation

10 Jan 2026	**KISA** QR impersonation warning; campaign behaviour, not a victim total
20 Mar 2026	**KISA** Hacktivist attempts described; service impact not established for every claim
4 Jun 2026	**PIPC** Streaming-service incident investigation; population not finalised
30 Jul 2026	**Joint agencies** State-backed campaign assessment; attribution remains the sources'
10 Nov 2026	**Financial Security Institute** Assessment-system disclosure following detection on 2026-11-09
12 Nov 2026	**Forum seller** Technical-document offer; contents unverified
17 Nov 2026	**Public-service operator** Shared-email explanation posted online; earlier notification and reporting are separate dates
19 Nov 2026	**Forum seller** Procurement-data offer; not authenticated
20 Nov 2026	**University** Additional portal records; not a unique-person total
22 Nov 2026	**National reporting** Energy-company disclosure; two system populations, not a deduplicated total

Sources: [S1][S6][S18][S19][S22][S32][S35][S48][S58][S60].

The timeline separates actor statements, third-party relays and official disclosures. A publication date does not establish when access began. Two items close together in time do not establish shared infrastructure or coordination.

6.2 Claim against confirmation

Question	Actor material	Evidence needed	Defender statement
Was a site unavailable?	A claim or external availability result	Service and upstream telemetry for the interval	State affected services and confirmed duration
Was information obtained?	Advertised files or screenshots	Access records and a validated sample	State verified categories and remaining uncertainty
Was a physical process affected?	An interface image or control claim	Operator records and process readings	Distinguish display access from a process change
Who was responsible?	Alias, flag or political slogan	Source-supported attribution evidence	Attribute the assessment and its confidence

A claimant may report a large target list while an operator confirms a narrower service problem. Those measures should not become a ratio. An availability result also cannot establish theft, persistence or responsibility for a separate incident.

6.3 An absence of confirmation has a narrow meaning

KISA's 2026-03-20 warning describes RipperSec attempts concerning Korean government and defence-sector targets. It does not establish successful disruption of every service in an actor's target list. The warning is official campaign context rather than independent validation of every claimed outcome. [S22]

RipperSec

Hacktivist activity described by KISA | The source's campaign framing; no independent state attribution

IN SOUTH KOREA, 2026

2026-03-20

KISA warning describes attempts concerning Korean government and defence-sector targets

CLAIMED TARGETS

Broad government and defence-sector roles, as stated by the source

SEEN IN PUBLIC REPORTING

[S22] Official campaign warning

OUR ASSESSMENT

The warning establishes reported attempts, not successful disruption of every named service. Compare any relevant claim with the responsible operator's service records.

CONFIDENCE

High for the existence of the warning; specific outcomes unresolved

The useful operational distinction remains the same when claims are sparse. A defender should be able to determine whether the public website, authentication service, customer transaction or internal process is affected. A single status indicator cannot answer all four.

For industrial operators, a screenshot of an interface warrants confidential validation with the owner. It does not justify announcing unsafe operations. Any intervention in production equipment must follow the operator's safety and change procedures.

6.4 Additional actor claims and what they do not establish

The retained RipperSec-labelled channel contains scheduled targeting notices and separate assertions about service availability, accounts and control interfaces. A scheduled target and time establish an announced intention, rather than a completed attack. [S1]

Observed post dates	Broad role or theme	Retained assertion	Evidence boundary
2026-01-15	Telecommunications-related host	An actor asserts host access	Host ownership and provider-wide access are unestablished
2026-02-05–2026-02-21	Energy, agricultural and administrative interfaces	Control or administration access is asserted; some posts refer to videos	The retained text establishes neither control nor a physical-process effect
2026-02-20	Several database targets	A channel asserts possession of database material	Files, origin and separate intrusion counts remain unverified
2026-02-22–2026-03-04	Travel, financial, commerce, public-data and energy websites	Channel posts assert unavailable services or give status links	Continuous downtime and business interruption are not demonstrated
2026-02-24	A public-facing website	A separate actor claims defacement	No independently verified page or service impact is established
2026-03-17	Several public-facing targets	Another channel posts an operation list with status links	A target list does not establish successful attacks against every target
2026-04-13–2026-05-23	Public-service websites	Additional channel relays assert disruption or repeat target lists	Relays and status links do not independently establish operational impact

These are distinct assertions, with original event dates and effects unresolved. Product names in a control-interface claim do not establish that the product vendor was attacked. Shared rhetoric does not establish a state relationship. [S1]

For an owner receiving a relevant interface claim, validate the asset and access route confidentially. Preserve authentication and operator records before deciding whether the claim concerns a public display, administration or an actual process change.

6.5 Communications that survive changing evidence

Prepare separate message templates for a claim under investigation, a confirmed service interruption and a confirmed personal-data event. Each should identify the affected service, the facts established, the mitigation underway and the next update time.

Communications staff need access to a technical evidence owner and a privacy decision owner. They should avoid repeating actor traffic volumes, slogans or claimed victim totals as company findings. Where an attribution is unresolved, say so plainly.

Agree with providers how incident records and mitigation telemetry will be preserved. A business continuity exercise should also test the fallback when an identity provider or customer messaging channel is unavailable.

6.6 Response ownership

Decision	Owner	Evidence before escalation
Activate mitigation	Network and service operations	Confirmed abnormal traffic or service degradation
Restrict an account	Identity and incident response	Account match and suspicious activity
Announce a data event	Privacy and communications	Applicable duty and verified or legally relevant suspected scope
Change a physical process	Responsible operator	Process evidence and approved safety action
Attribute publicly	Designated leadership	Reviewed source-supported assessment

The purpose is to preserve service and accuracy together. Teams can act urgently on their own telemetry while keeping a third party's unverified narrative outside the factual status message.

KEY TAKEAWAYS

01

Reachability, data access and physical impact are different propositions.

02

Political framing does not establish responsibility.

03

Rehearse mitigation, evidence preservation and a timed status update together.

CHAPTER 07

Actors, campaigns and relationships

07

THIS CHAPTER ANSWERS

Which actor assessments are supported, and which defensive behaviours matter regardless of attribution?

73

South Korea ransomware listings in Ransompedia

7.1 Relationship map 70
7.2 Reply-based phishing and attributed espionage 71
7.3 Domestic campaign research without blanket attribution 72
7.4 Recent commercial lures remain relevant 73
7.5 Ransomware and extortion 73
7.6 Criminal personas and evidence boundaries 79

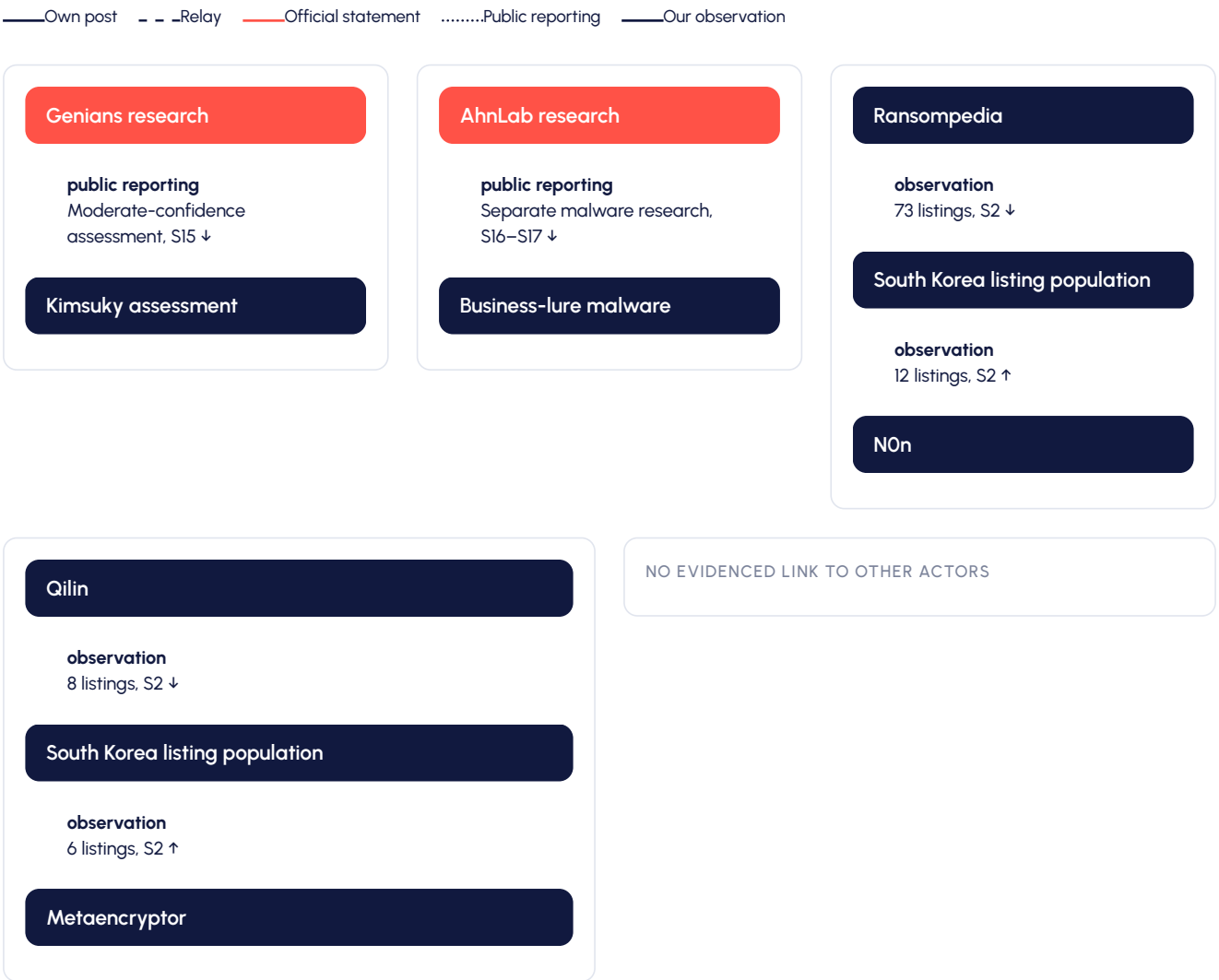
CHAPTER 07

Actors, campaigns and relationships

IN SHORT

Separate three tracks: source-attributed espionage research, extortion listings and criminal-market personas. Genians assigns moderate confidence to a Kimsuky connection in its seminar-lure research. Ransompedia records multiple claimant labels, without establishing unique operators. An alias can recur without proving common ownership of every advertisement. Use the documented behaviour to prioritise identity, endpoint and recovery controls, and preserve attribution uncertainty in every escalation.

7.1 Relationship map



The map separates publishers, actor labels and the listing population. A source's attribution is not an independent finding by this report. An own-data listing edge records a claim in the retained source, rather than an intrusion confirmed by the named organisation.

No edge connects an underground seller to a state-attributed campaign without a concrete shared element. A shared language, victim sector or publication week is insufficient. Similar advertised quantities also do not establish that sellers possess the same file.

7.2 Reply-based phishing and attributed espionage

Kimsuky

Espionage assessment attributed to Genians | North Korea-linked, as assessed by Genians with moderate confidence

IN SOUTH KOREA, 2026

2026-11-16
Research publication describing earlier correspondence and tool evolution

CLAIMED TARGETS

Policy and security professionals, as described by the source

SEEN IN PUBLIC REPORTING

[S15] Genians assesses the campaign with moderate confidence and retains imitation as an alternative.

OUR ASSESSMENT

Correlate trusted-workflow correspondence, endpoint behaviour and account evidence. No link to the report's unrelated market advertisements is established.

CONFIDENCE
Source attribution: moderate; national victim extent unresolved

Genians published its NodeLinkRAT research on 2026-11-16. It describes September correspondence impersonating a parliamentary aide and requesting seminar honorarium paperwork. The first message omitted its attachment; a later reply supplied the malicious archive. Genians attributes the campaign to the North Korea-linked Kimsuky group with moderate confidence. [S15]

The source explicitly preserves the possibility of imitation. Its account, phishing-kit and infrastructure overlaps support an association, while commonly abused services cannot establish responsibility alone. This report adopts neither a stronger confidence nor a wider victim population.

The defensive consequence is to retain email-thread context and endpoint events together. A requested attachment can feel more legitimate than an unsolicited one. Verify unexpected payment or identity paperwork through a known channel, and investigate a document-themed archive that launches a script interpreter.

The publication date is recent; the described correspondence occurred earlier. The report therefore treats this as recent disclosure of earlier activity, rather than a new attack dated to the closing fortnight.

7.3 Domestic campaign research without blanket attribution

AhnLab's domestic October review, published on 2026-11-20, describes spearphishing, shortcut files and a Hangul-document lure. The source says shortcuts had the largest share in its observed October population. Its public article does not provide a national denominator. [S14]

The article's actor tags do not assign every described delivery chain to one group. The report therefore uses the mechanisms for defensive planning and does not attribute the whole population to Kimsuky.

For security operations, connect the document or archive event to child processes, persistence and subsequent outbound activity. Legitimate remote-management software or cloud services can appear in a malicious chain. Their presence alone does not justify a malicious verdict.

The matrix and table are behavioural crosswalks, an analyst interpretation of the cited research. Technique definitions were checked against MITRE ATT&CK. They are not attribution models or claims that every listed behaviour occurred at every Korean target. [S90]

TECHNIQUES NAMED IN THE VENDOR RESEARCH, BY TACTIC

Execution	Persistence	Exfiltration
T1204.002 Malicious File: document-themed shortcut, analyst crosswalk [S14][S15][S90]	T1053.005 Scheduled Task: reported recurring task, analyst crosswalk [S14][S15][S90]	T1567.002 Cloud Storage: reported information transfer, analyst crosswalk [S15][S90]
T1059.001 PowerShell: reported script chain, analyst crosswalk [S14][S15][S90]		

Analyst behavioural crosswalk; identifiers checked against MITRE; not a vendor attribution or victim count. [S90]

Behaviour	Defensive surface	Initial question	Source
Targeted document correspondence	Mail and endpoint	Did the sender's workflow match a known business request?	[S14][S15]
Shortcut launching scripts	Process telemetry	Did a document-themed file start an interpreter?	[S14][S15]
Scheduled persistence	Endpoint changes	Who created the task and what behaviour followed?	[S14]
Cloud-assisted data transfer	Proxy and endpoint	Is the transfer expected for this user and process?	[S15]
Browser-data collection	Endpoint and identity	Do account or session alerts corroborate the process chain?	[S14]

7.4 Recent commercial lures remain relevant

AhnLab's November research also describes procurement-themed malware delivery. Its 2026-11-12 notice concerns a quotation archive associated with SnakeKeylogger. Its 2026-11-13 notice concerns a purchase-order document associated with XLoader. These are separate vendor observations. [S16][S17]

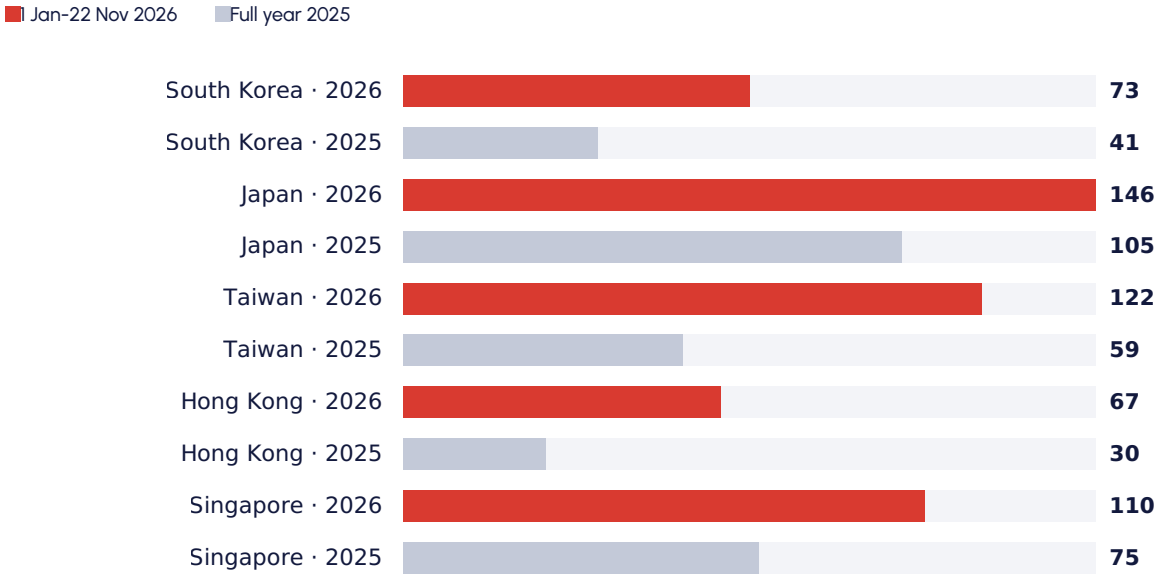
[GROUP commercial-malware]

Purchasing and accounts-payable teams should not rely on the apparent relevance of an attachment. Security operations should be able to identify document or archive applications launching unexpected scripts, then inspect account and session activity on the same endpoint.

A finding of malware on an employee endpoint does not establish that the corporate network was entered. Conversely, a document-themed lure can warrant investigation before a data-sale advertisement appears. External market visibility and internal endpoint visibility serve different purposes.

7.5 Ransomware and extortion

South Korea has fewer visible listings than three selected regional peers



Source: Brandefense Ransompedia listing claims [S2]. 2026 covers 1 January-22 November, closing day partial; 2025 is the full year. Unequal periods and source visibility do not establish a national risk ranking.

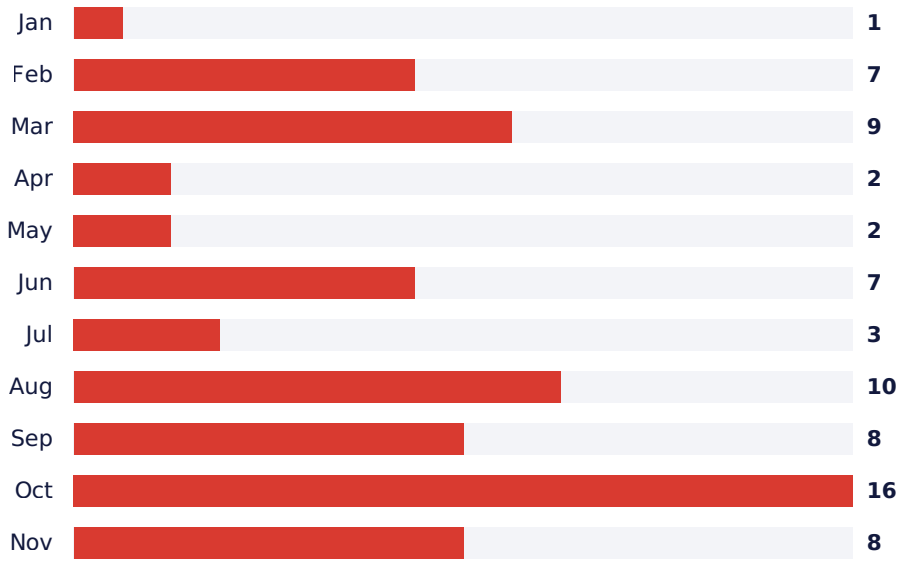
Comparison countries were selected as examples to provide context only; they do not imply a ranking or political assessment.

Ransompedia records 73 South Korea listings in the requested window, against 41 for all of 2025. The partial-year and full-year totals describe visibility in the same snapshot; they are not a matched-duration growth rate. [S2]

Comparator	Window listings	Full-year 2025	Why included
South Korea	73	41	Report country
Japan	146	105	Nearby industrial and supplier economy
Taiwan	122	59	Semiconductor and export context
Hong Kong	67	30	Regional financial-services context
Singapore	110	75	Regional finance, trade and digital services

The peers differ in size, industrial composition and publication visibility. The figures do not rank national security or estimate the chance that an organisation will be attacked. Country labels are used for the comparison without a political inference.

October carries the largest South Korea listing total in this snapshot

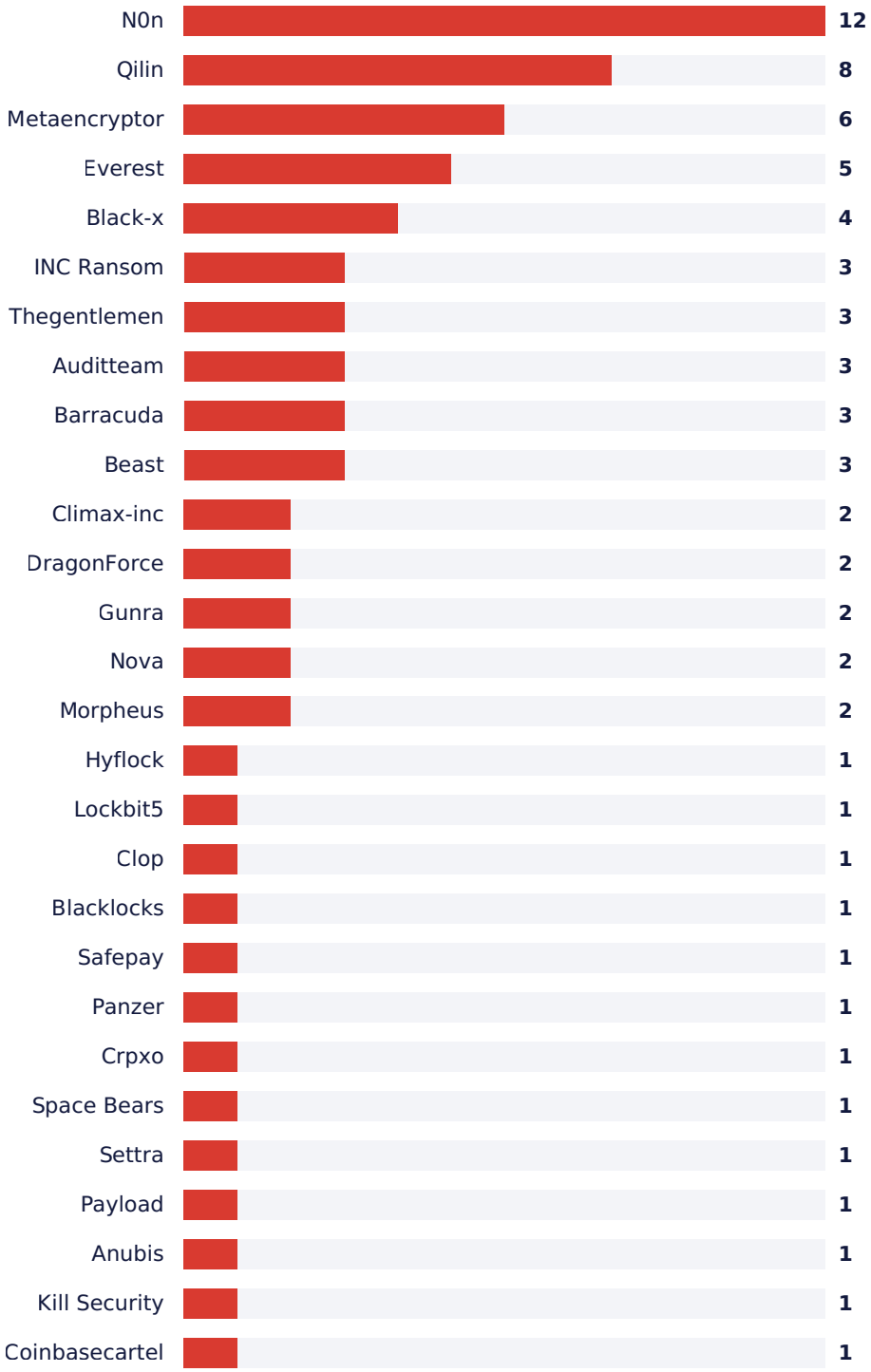


Source: Brandefense Ransompedia listing claims [S2]. 2026 covers 1 January–22 November, closing day partial; 2025 is the full year. Unequal periods and source visibility do not establish a national risk ranking.

Month	Listings	Month	Listings
January	1	July	3
February	7	August	10
March	9	September	8
April	2	October	16
May	2	November to cut-off	8
June	7	Total	73

October's 16 listings are a publication observation, not a measure of intrusion starts. A group can list material after a long delay. November is partial and must not be compared with a complete month as a rate.

The leading three claimant labels account for 26 of 73 listings



Source: Brandefense Ransompedia listing claims [S2]. 2026 covers 1 January–22 November, closing day partial; 2025 is the full year. Unequal periods and source visibility do not establish a national risk ranking.

N0n accounts for 12 listings, Qilin for 8 and Metaencryptor for 6. Together they represent 26 of 73, or 35.6%. The other 47 listings carry other labels. These names identify claims, rather than unique people or independently established affiliates. [S2]

Ransomware claimant labels

Extortion listing population | No state attribution assessed

IN SOUTH KOREA, 2026

2026

73 South Korea listings in the requested window

CLAIMED TARGETS

Listing-labelled sectors; no named victims here

SEEN IN PUBLIC REPORTING

[S2] Ransompedia records the dated listing population.

OUR ASSESSMENT

N0n, Qilin and Metaencryptor account for 26 of 73 listings. Prepare recovery and disclosure; listing status does not establish a confirmed incident.

CONFIDENCE

High for retained listing counts; underlying assertions remain claims

N0n

Extortion listing label | No state attribution assessed

IN SOUTH KOREA, 2026

2026

12 South Korea listings in the requested window

CLAIMED TARGETS

As labelled in the retained listing population; no named victims here

SEEN IN PUBLIC REPORTING

[S2] Own-data listing snapshot

OUR ASSESSMENT

The label supports preparation for extortion, information-impact assessment and recovery. It does not establish a unique operator, encryption, a completed payment or a verified information transfer.

CONFIDENCE

High for the retained count; underlying claim outcomes unverified

Qilin

Extortion listing label | No state attribution assessed

IN SOUTH KOREA, 2026

2026

8 South Korea listings in the requested window

CLAIMED TARGETS

As labelled in the retained listing population; no named victims here

SEEN IN PUBLIC REPORTING

[S2] Own-data listing snapshot

OUR ASSESSMENT

The label supports preparation for extortion, information-impact assessment and recovery. It does not establish a unique operator, encryption, a completed payment or a verified information transfer.

CONFIDENCE

High for the retained count; underlying claim outcomes unverified

Metaencryptor

Extortion listing label | No state attribution assessed

IN SOUTH KOREA, 2026

2026

6 South Korea listings in the requested window

CLAIMED TARGETS

As labelled in the retained listing population; no named victims here

SEEN IN PUBLIC REPORTING

[S2] Own-data listing snapshot

OUR ASSESSMENT

The label supports preparation for extortion, information-impact assessment and recovery. It does not establish a unique operator, encryption, a completed payment or a verified information transfer.

CONFIDENCE

High for the retained count; underlying claim outcomes unverified

The largest industry label is manufacturing, with 19 of 73 listings. Labels can be broad or inaccurate. Use the pattern to include production, supplier and engineering-data scenarios in exercises, rather than to calculate a national manufacturing incident rate.

7.6 Criminal personas and evidence boundaries

Persona	Retained role	Boundary
FantancyHacker	Lending-data advertising	File origin, exclusive sale and population unverified
Solonik	Database-themed posts	Mixed row units and hosting/tenant attribution unresolved
zSenior	Privileged-access offer	Source thread challenges proof; no database theft established
0xCAFE	Multi-system information bundle	Several services do not establish separate intrusions
TunaFish	Remote-access advertisement	Active access and a completed transaction unverified
HighWayToShell	Cloud-administrator offer	No established link to the other insurer offer
taltikgoo	Technical-document offer	Supplier relationships do not establish customer incidents
Noiem	Personal/procurement-data offer	Categories overlap; official-file identity unverified
DataJava	Recent administrative/data offers	Similar presentation is a provenance lead, not proof of one backend

The practical question is what each retained post establishes. A seller can advertise data, a buyer can request access, and another account can relay the same title. None of those roles by itself establishes original theft, a successful sale or continuing access.

For threat-intelligence teams, keep persona, venue, claimed dataset and observed post as distinct records. Any relationship assessment should explain its concrete evidence and its limit. The report's case cards preserve those distinctions beside the quoted material.

KEY TAKEAWAYS

01

Preserve Genians' moderate-confidence attribution and imitation alternative.

02

Treat ransomware labels as claims and test recovery against the relevant business impact.

03

Correlate trusted-workflow lures with endpoint and identity evidence before attributing an incident.

CHAPTER 08

Fraud, identity and the secondary-use problem

THIS CHAPTER ANSWERS

How can circulating information create harm without a new intrusion at the organisation receiving a fraudulent request?

4

workflows to test: recovery, onboarding, payment and supplier contact

8.1 Advertisements show demand and supply claims 82
8.2 Payment-card material: a narrow view 82
8.3 Secondary fraud in official warnings 83
8.4 Prices are assertions rather than transaction evidence 84
8.5 Four workflows worth testing 84
8.6 Link security and customer operations 85

CHAPTER 08

Fraud, identity and the secondary-use problem

IN SHORT

Criminal-market material and official warnings point to the reuse of identity and relationship information. A believable message can quote a real booking, workplace or customer detail. That does not establish the sender's authority. Card material is a narrow observation with no national-loss interpretation. Test account recovery and payment changes against accurate personal information, verify supplier messages through known contacts, and route corroborated fraud to the responsible team.

8.1 Advertisements show demand and supply claims

The retained offers describe personal information, account-related records, customer contacts and administrative access. Some sellers present several services in one bundle; others request material rather than claim possession. These observations support workflow testing, without establishing a completed transaction. [S1]

An offer of identity data, a request for accounts and a service promising verification should remain separate observations. They can describe complementary capabilities without showing that one operator acquired or combined them.

For a defender, the useful question is whether a process treats a known personal detail as a secret. Names, contact information and an accurate business relationship can make an approach persuasive. Additional authentication and a trusted callback route should determine authority for a risky change.

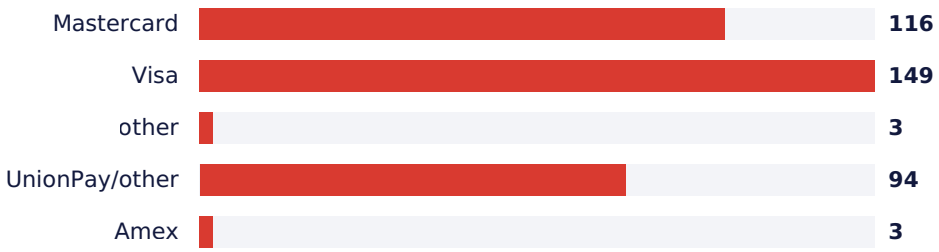
8.2 Payment-card material: a narrow view

SCOPE OF THE CARD FIGURES

These figures describe payment-card records in the retained post corpus. They do not measure national card exposure, card theft or fraud loss, and do not represent Brandefense's wider card coverage.

The retained post evidence contains 365 distinct payment-card records across 424 posts, associated with 187 issuer prefixes. These are corpus observations; validity, origin and fraud loss remain unresolved. They do not measure national card exposure or Brandefense's wider card coverage. [S4]

Card-brand counts concern the retained post evidence only



Source: retained post payment-card aggregate evidence [S4]. Card records are not unique cardholders, losses or national prevalence.

These observations should not be joined to official breach totals or interpreted as evidence of a particular bank's intrusion. An issuer's investigation should depend on its own authorisation and fraud signals. Reissuance or customer restrictions require validation under issuer policy.

8.3 Secondary fraud in official warnings

KISA's May warning describes stolen travel-booking details being reused in hotel impersonation and payment-reconfirmation messages. A June warning anticipates compensation and refund phishing following a streaming-service disclosure. The first describes reported reuse; the second includes anticipated secondary abuse. Neither supplies a national fraud-loss total. [S26][S28]

The police-authored 2026-03-27 republication warns about travel-refund, impersonation, investment, romance and donation lures. National reporting on 2026-03-23 distinguished reported attempts from realised harm. These are preventive scenarios, rather than verified loss figures. [S109][S110]

The distinction between observed and anticipated secondary abuse matters. A warning that a refund scam may follow a disclosure is preparation advice. It does not establish that every warned-of scam occurred or caused a measured loss.

For customer communications, state which details a legitimate organisation will never ask a person to provide through an unsolicited message. Offer a trusted way to verify a claim without using the sender's link or telephone number.

8.4 Prices are assertions rather than transaction evidence

Offer	Asking price	Evidence boundary
Remote administrative access, Case E	898 USD	One advertisement; usable access and sale unverified
Business-system datasets	900–1,000 USD	Selected seller offers; files and transactions unverified
Recent administrator/customer-data offer	4,500 USD	Advertised access and population unverified
Recent CRM-related offer	4,550 USD	Claimed administrative export, not verified access

These are separate advertised items in the retained posts. They are not a representative price distribution. [S1]

An asking price can describe the seller's presentation and target audience. It does not establish market value, file authenticity, demand at that price or a completed transaction. Prices for access, records, subscriptions and services are not interchangeable units.

Similarly, an advertised quantity may refer to rows, orders, files or accounts. A dataset can contain several records about one person or information from several organisations. Preserve the seller's stated unit and the uncertainty instead of converting the quantity to victims.

8.5 Four workflows worth testing

Workflow	Test condition	Owner	Completion evidence
Account recovery	Caller knows accurate personal and relationship details	Identity and customer operations	Risky change requires independent verification
Onboarding	Applicant presents plausible identity information from an exposed file	Fraud and compliance	Additional checks address the actual risk
Payment change	Message quotes a real supplier invoice or booking	Finance and service owner	Known-contact confirmation precedes change
Staff support	Request cites internal names and assessment documents	Help desk and security	Privileged change requires an approved route

Use synthetic cases and authorised exercises. The goal is to find a process that confuses knowledge with authority, without circulating real affected people's information.

8.6 Link security and customer operations

An incident team may establish the technical scope before it understands the customer relationship. A contact centre may see suspicious approaches before security sees a matching advertisement. Both need a way to exchange relevant facts without spreading unnecessary personal information.

Record what the customer or staff member received, which relationship detail was accurate, and which action the message requested. Keep that report separate from assumptions about where the information originated.

When a new disclosure changes the verified categories, update fraud monitoring and customer advice. Closure should include a check that the affected workflow remains safe, rather than ending when the original application returns to service.

KEY TAKEAWAYS

01

Accurate personal information does not establish authority.

02

Keep advertised quantities and narrow card observations out of national-loss estimates.

03

Test recovery, payment and supplier workflows with synthetic cases and accountable owners.

CHAPTER 09

Banking and financial services

09

THIS CHAPTER ANSWERS

How should financial organisations connect application security, identity validation and customer protection?

37

firms in the FSC's dated disclosure population

9.1 Universe and separation 87
9.2 A dated official disclosure population 87
9.3 Assessment-service evidence 88
9.4 Put business interfaces into the asset inventory 89
9.5 Customer and staff protection 89
9.6 Management questions 89

CHAPTER 09

Banking and financial services

IN SHORT

The financial-sector evidence concerns distinct applications, reporting populations and information categories. The FSC described 40 cases involving 37 firms during a stated period. A separate November disclosure concerns the Financial Security Institute's assessment service. Neither should become a claim that core banking systems or all customer credentials were accessed. Review external interfaces and support applications, preserve access evidence, and bring customer-protection teams into the incident decision.

9.1 Universe and separation

The selected portfolio contains 25 banking and payment domains and 25 insurance and capital-markets domains. These cells include different functions and may include related groups. They do not represent 50 independently validated banks or issuers.

The banking and payment cell has 24 of 25 domains with device associations, 23 with historical credential records and 15 with a current credential listing. Its device associations total 55,600, including 152 employee-classified and 55,448 other associations. Historical credential records total 150,216. [S3]

The separate insurance and capital-markets cell has 25 of 25 domains with device associations, 24 with historical credential records and 17 with a current listing. It has 21,508 device associations, including 107 employee-classified and 21,401 other associations, and 92,116 historical credential records. [S3]

Card attribution does not locate the source of theft. Issuers should validate relevant signals against their own account, endpoint and fraud evidence before assigning an incident.

Payment-card material in the retained post corpus is a separate, narrow observation (§8.2). It does not measure national card exposure, card theft or fraud loss. It should not be used to attribute an intrusion to a bank or connect an advertisement to an official incident.

9.2 A dated official disclosure population

The FSC's 2026-11-05 statement reports 40 cases involving 37 financial firms between 2026-09-30 and 2026-11-03. It describes approximately 473,000 personal-information entries. The same statement says customer account passwords had not been reported stolen at that time. [S5]

The boundary matters. Personal information can support convincing impersonation without containing a usable banking password. Customer notices and fraud monitoring should address that route while technical investigators establish which application and accounts were involved.

The FSC also describes intended inspections and rule changes. A planned measure is not proof of completed inspection or enacted legislation. Chapter 10 separates the current reporting guidance from announced policy work.

The FSC's 2026-10-14 statement explicitly confirms Streami among the financial-company incidents. National reporting identifies Streami as Gopax's operator. The regulator was still investigating routes and relationships; its aggregate findings should not be assigned wholesale to this organisation. [S113][S114]

Later reporting on 2026-11-18 describes an expanded affected-person scope and dates the underlying event to 2026-09-08. That follow-up attributes its account to supervisory material; the underlying document is not established here. No initial estimate is presented as final, and no funds-loss inference follows. [S115]

9.3 Assessment-service evidence

P

CASE P

Assessment data and transaction systems are different

Financial security services

Official disclosure; scope qualified

OFFICIAL ACCOUNT	The Financial Security Institute disclosed abnormal external access to its continuous-assessment system, detected on 2026-11-09. It blocked access and began an investigation. [S6]
REPORTED SCOPE	The institute described approximately 200 administrative forms, 300 personal-data entries within forms and 350 system-user entries. These are categories that can overlap, not a unique-person total.
BOUNDARY	The institute said the system did not process general customers' financial transactions. Its stated scope excluded financial-system architecture and specified sensitive customer information at that time.
CORROBORATION	Yonhap reported the institute's disclosure. That supports named discussion of this public case without establishing facts beyond the institute's account. [S7]
RESPONSE	Financial firms should identify documents supplied to assessment and support services, confirm recipient access, preserve relevant records and assess impersonation risk for affected staff.

Bottom line

Follow the stated mechanism and information scope; preserve date, population and attribution limits in the response.

An assessment service can hold useful social-engineering information even when it does not operate a payment platform. The response should follow the exposed categories and business relationships, rather than assuming the most sensitive possible system was involved.

9.4 Put business interfaces into the asset inventory

The first review should cover interfaces that expose personal information or permit changes to workflow state. Include partner access, support portals, staff applications, training and assessment services. An application with a small user population can still hold privileged information.

For each interface, record an accountable owner, the authentication mechanism, permitted objects and export capability. Test access with appropriately authorised accounts. A successful login test is insufficient if one user can request another user's record.

Give incident responders a way to identify both the account and the object accessed. Log retention should support a meaningful review of access, exports and administrative changes. Preserve records before routine rotation removes them.

9.5 Customer and staff protection

Evidence	Risk to validate	Joint owners	Initial action
Staff contact information disclosed	Convincing internal impersonation	Security and human resources	Warn staff through a trusted channel
Customer identity information disclosed	Recovery and call-centre impersonation	Fraud and customer operations	Tighten risky recovery decisions
Active credential corroborated	Unauthorised account use	Identity and incident response	Revoke relevant sessions and contain
Unusual payee or device change	Transaction abuse	Digital banking and fraud	Apply appropriate verification
A processor's notice	Shared records and notification duties	Procurement, privacy and business owner	Confirm scope and preserve evidence

These are conditional response paths, not findings that the listed harms occurred. The customer-protection decision should be proportionate to the verified categories and the remaining uncertainty.

9.6 Management questions

The board should ask whether external business interfaces have owners and whether unauthorised object access can be detected. It should also ask whether the customer contact plan is ready before the investigation produces a final number.

The CISO should report unresolved applications and evidence gaps with dates and owners. Fraud leadership should demonstrate that known identity information cannot, by itself, approve an account recovery or a payment change.

KEY TAKEAWAYS

01

Keep official reports, selected-domain signals and card material separate.

02

Review support and partner applications alongside transaction platforms.

03

Link verified information categories to account, staff and customer protection.

CHAPTER 10

Regulatory and national response

10

THIS CHAPTER ANSWERS

Which current duties and announced measures should a Korean organisation distinguish?

72 hours

stated period in PIPC's conditional breach-reporting guidance

10.1 Current personal-data reporting guidance 92
10.2 September changes and the later certification provision 92
10.3 Financial-sector announcements are dated policy evidence 93
10.4 Applicability before a clock starts 94
10.5 Exercise the reporting workflow 94

CHAPTER 10

Regulatory and national response

IN SHORT

Incident response must distinguish personal-data reporting, notification to affected people and sector supervision. PIPC describes changes effective in September, including notification of possible leakage and a wider incident scope. A separate certification provision has a later start. The FSC's November programme includes planned measures rather than a completed legal transition. Have privacy counsel confirm applicability, name the decision owner, and preserve the awareness record and initial evidence.

10.1 Current personal-data reporting guidance

PIPC's guidance states that a controller must report within 72 hours where one of its listed conditions applies. Those conditions include at least 1,000 affected data subjects, sensitive or unique identifying information, or leakage through unlawful external access. [S9]

That final condition matters for smaller incidents. A controller should not assume that a figure below 1,000 removes every reporting obligation. The legal assessment concerns the event, information categories and access route as well as the population.

The guidance identifies KISA as a designated reporting institution. It separately directs financial institutions and relevant credit-information businesses to the FSS for the appropriate route. The same page distinguishes personal-credit information under a different statute. [S9]

This report gives a decision aid, not legal advice. Counsel should confirm the current legislation, applicable exceptions, sector rules and reporting procedure for the particular entity. Record when relevant facts became known; do not substitute an actor's publication date for organisational awareness.

10.2 September changes and the later certification provision

PIPC's 2026-09-10 announcement states that revised law and implementing provisions take effect on 2026-09-11. It describes notification of possible leakage, expanded information in notices and inclusion of forgery, alteration or damage, including ransomware. [S10]

The announcement also describes stronger governance responsibilities for senior management and privacy officers. It does not make every detail of the implementing conditions interchangeable with the short public summary. Organisations should obtain the controlling text for their own applicability decision.

The separate mandatory ISMS-P provision is described as taking effect on 2027-07-01. Its later commencement must not be presented as a requirement already in force at the report cut-off. [S10]

Instrument	Verified status	Immediate management task
PIPC breach-reporting guidance	Conditional reporting period and routes described	Confirm event, information and entity scope
September privacy changes	Effective date 2026-09-11 stated by PIPC	Update notification and governance procedures
Possible-leak notification	Introduced under the September framework	Obtain counsel's trigger and content checklist
Mandatory ISMS-P provision	Later commencement 2027-07-01 stated	Determine applicability and implementation plan
Sector financial requirements	Separate financial reporting route identified	Verify FSS and other applicable obligations

The absence of confirmed exfiltration does not, by itself, close every notification question. The new possible-leak framework is especially relevant where unlawful access is known but the affected individuals cannot yet be fully identified.

10.3 Financial-sector announcements are dated policy evidence

The FSC's November programme proposes wider scrutiny of external business interfaces and clearer management accountability. It also describes planned changes to supervision, information sharing and evaluation requirements. [S5]

The statement says a digital-finance safety bill is planned for the first quarter of 2027. This report treats that as intended legislation. It does not state that the bill was enacted or that an announced timetable demonstrates implementation.

For a financial firm, the useful near-term response is to maintain an asset register covering externally accessible business applications and their accountable executives. Preserve the evidence needed to explain which system was reached and which information was affected.

10.4 Applicability before a clock starts

Organisation	Decision to prepare	Accountable functions
Personal-data controller	Reporting conditions, subject notice and awareness record	Privacy, legal and incident response
Financial institution	Financial reporting route plus other applicable privacy duties	Compliance, privacy and CISO
Processor or business supplier	Contractual alert, evidence preservation and controller assistance	Procurement, legal and service owner
Public body	Competent technical and privacy chan-nels	Security office and privacy officer
Overseas provider serving Korea	Local applicability and accessible reporting procedure	Legal and local representative where applicable

A supplier contract should say who sends the first incident alert and who can provide access records. It should not require a final forensic conclusion before every relevant alert reaches the controller.

Maintain a decision log covering awareness, known facts, uncertainties, legal assessment and subsequent updates. A changing population estimate should lead to controlled updates, rather than an undocumented replacement of the initial record.

10.5 Exercise the reporting workflow

Use a scenario in which a support service reports unlawful access but cannot yet identify every affected person. Require the privacy team to decide which duties need assessment, the service owner to explain the records held, and responders to preserve evidence.

Then introduce a second fact: encrypted account information or internal assessment documents were involved. The exercise should show how the organisation changes its customer-protection and reporting decisions without claiming an unsupported final total.

Completion means a dated applicability record, an owner for each channel and a tested update process. Merely naming a regulator in a policy document is insufficient.

KEY TAKEAWAYS

01

Assess reporting and subject-notification duties separately.

02

Keep current requirements distinct from later commencement dates and proposed legislation.

03

Record awareness, preserve evidence and test the initial-notice workflow.

CHAPTER 11

Outlook and conditional scenarios

11

THIS CHAPTER ANSWERS

Which judgements justify preparation, and what evidence would change them?

4

conditional planning scenarios with explicit triggers

11.1 Key judgements 97
11.2 What would change the assessment 98
11.3 Four planning scenarios 98
11.4 Signals that are insufficient by themselves 99

CHAPTER 11

Outlook and conditional scenarios

IN SHORT

The evidence supports preparation for identity abuse, peripheral-application exposure, extortion and trusted-workflow phishing. It does not supply a national attack probability or establish a common attacker behind the recent disclosures. Treat the scenarios below as planning assumptions. Change priorities when internal evidence, official updates or validated samples change the proposition, and fund the controls that can be demonstrated in an exercise.

11.1 Key judgements

Judgement	Confidence	Basis and limit
Peripheral applications belong in critical security reviews	High for the disclosed response need	Financial and assessment-service disclosures; not a national architecture census
Identity information can support credible follow-on impersonation	Medium as a planning judgement	Exposed categories and official warning themes; realised losses are not measured here
Extortion readiness deserves continued investment	High for the visible listing population	73 listings; unpublished incidents and confirmed outcomes unresolved
Trusted correspondence remains an important phishing surface	High for the cited campaigns	Official and vendor descriptions; no national frequency estimate
The recent disclosures share one attacker	Not established	Temporal proximity supplies no concrete link

Confidence attaches to each proposition. A source's confidence about one campaign cannot be transferred to another incident merely because both involved Korean-language correspondence.

11.2 What would change the assessment

Current position	New evidence	Decision affected
A data advertisement remains unverified	A sample matches protected internal records and access evidence	Escalate investigation and assess notification
A credential association needs validation	Active privileged account and suspicious session match	Contain the account and related sessions
Separate recent incidents have no established link	Concrete shared infrastructure or a source-supported campaign assessment	Revisit coordination and hunting scope
A vendor describes an earlier campaign	New activity in the organisation's own telemetry	Move from historical comparison to active response
An official population is provisional	Controller publishes a supported revision	Update impact and customer-protection decisions

The table avoids a common forecast error: turning an advertisement into an expected loss. An external signal can justify a validation task without establishing the likelihood or size of harm.

11.3 Four planning scenarios

Scenario A: an external application exposes information. If the organisation finds an unauthorised object-access path in a customer, staff or partner application, treat the affected data and privileges as the scope to establish. Preserve access evidence, restrict the path safely and involve privacy staff. The signal is a validated access-control failure, rather than a high post count.

Scenario B: identity data is reused for payment or recovery fraud. If customers receive messages quoting genuine relationship details, confirm whether information was exposed and whether the contact is fraudulent. Warn through a trusted channel and strengthen risky recovery or payee-change checks. Accurate biographical information should not establish authority.

Scenario C: extortion threatens continuity and engineering information. If a credible claim or internal detection concerns production-support or engineering systems, activate both recovery and information-impact work. Test the minimum safe service with independent recovery credentials. A public listing alone does not establish encryption or physical-process manipulation.

Scenario D: a trusted workflow delivers a malicious file. If correspondence about a seminar, recruitment, purchasing or support request produces an unexpected archive or shortcut, correlate the thread with endpoint behaviour. Investigate script execution and account activity together. A familiar subject or a requested attachment does not establish legitimacy.

11.4 Signals that are insufficient by themselves

A flag, language or political slogan does not establish nationality. An alias match does not establish one operator. A recent post does not establish a recent intrusion. A large row count does not establish unique affected people.

Likewise, the absence of a listing does not show that an organisation avoided extortion. The absence of a public attribution does not show that a campaign lacked a sponsor. These gaps limit inference rather than supplying an alternative conclusion.

For executives, review the scenarios against actual service dependencies and the evidence available to responders. Select a small set of measurable exercises. Revise the plan when those exercises or new incident facts identify a more consequential gap.

KEY TAKEAWAYS

01

Treat scenarios as conditional preparation, not predictions.

02

Revisit decisions when the underlying proposition changes.

03

Fund validation, customer protection and recovery evidence that a business owner can review.

CHAPTER 12

Action plan

12

THIS CHAPTER ANSWERS

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

18

actions with accountable owners and closure evidence

12.1 Ninety-day action schedule 101
12.2 Scorecard targets 103
12.3 By role 104
12.4 How Brandefense can help 104

CHAPTER 12

Action plan

IN SHORT

Begin with the information and services the organisation actually controls. Establish alert ownership, validate active account evidence and review external business interfaces. Then test supplier notification, customer recovery decisions and service restoration. The plan is a sequence, not permission to delay an active response. Report completed evidence, unresolved dependencies and dated remedial actions to the board by day 90.

12.1 Ninety-day action schedule

1Days 1–30

Establish a route for relevant credential, device and data-offer alerts, internally or through a provider

OWNER
CISO and threat intelligence

COMPLETION EVIDENCE
Named source, recipient and first reviewed alert

Validate new credential alerts against active accounts, privilege and sessions

OWNER
Identity operations

COMPLETION EVIDENCE
Dated disposition for each alert

Inventory external customer, partner and staff applications, including supporting services

OWNER
Application and business owners

COMPLETION EVIDENCE
Service, data, owner and interface register

Test authorisation on sensitive objects and bulk exports using approved accounts

OWNER
Application security

COMPLETION EVIDENCE
Evidence of permitted and rejected access

Assess current Java advisories against actual service runtimes and supported vendor packages

OWNER
Infrastructure and application owners

COMPLETION EVIDENCE
Runtime inventory and patch or mitigation record

Confirm privacy and sector-reporting triggers, channels and awareness records

OWNER
Legal, privacy and compliance

COMPLETION EVIDENCE
Approved applicability and initial-notice checklist

Identify critical suppliers holding records or administrative access

OWNER

Procurement and data owners

COMPLETION EVIDENCE

Supplier evidence contact and incident-alert route

2Days 31–60

Prioritise phishing-resistant MFA for privileged and remote users

OWNER

Identity and business owners

COMPLETION EVIDENCE

Coverage record and tested recovery route

Detect document or archive workflows launching unexpected scripts and persistence

OWNER

SOC and endpoint engineering

COMPLETION EVIDENCE

Reviewed authorised simulation and alert evidence

Verify legitimate mail senders before staged DMARC enforcement

OWNER

Messaging

COMPLETION EVIDENCE

Alignment review, approved policy and rollback route

Test customer recovery and payee changes against a caller with accurate personal information

OWNER

Fraud and customer operations

COMPLETION EVIDENCE

Synthetic case rejected or gap remediated

Test supplier evidence transfer and provisional notification

OWNER

Procurement, privacy and incident response

COMPLETION EVIDENCE

Timed exercise record and agreed updates

Restore one essential service with protected backups and separate credentials

OWNER

Infrastructure and business continuity

COMPLETION EVIDENCE

Integrity check and business acceptance against recovery target

3Days 61–90

Exercise a simultaneous service interruption and data claim

OWNER

CISO and communications

COMPLETION EVIDENCE

Factual status message, evidence owner and update time

Reconcile privileged tokens and secrets exposed in a confirmed event

OWNER
Identity and development

COMPLETION EVIDENCE
Revocation, replacement and access review records

Close certificate, renewal and public-service configuration exceptions

OWNER
Network and service owners

COMPLETION EVIDENCE
Successful recheck or dated approved exception

Exercise notification where affected people are initially uncertain

OWNER
Privacy, legal and business owners

COMPLETION EVIDENCE
Trigger assessment, initial content and update decision

Report the scorecard and remaining service dependencies

OWNER
CISO to board

COMPLETION EVIDENCE
Evidence-linked board record with dated owners

New evidence of active unauthorised access enters incident response immediately. The day ranges organise improvement work; they do not replace regulatory deadlines or the organisation's severity process.

12.2 Scorecard targets

The targets below are suggested management commitments. Set stricter targets where the service, law or internal policy requires them. An exception should identify the compensating control, owner and review date.

Measure	Suggested target	What counts as evidence
Relevant alert route	In place by day 30	Recipient and first alert reviewed
New relevant identity alerts	Every alert has a dated disposition	Account and session evidence
External sensitive applications	Every application has an accountable owner	Reviewed service and data register
Privileged and remote users	Phishing-resistant MFA or a dated migration plan by day 60	Coverage and recovery test
Critical supplier alert routes	Tested by day 60	Timed message and evidence transfer
Essential-service restoration	Meets the approved recovery target or has a dated fix	Business acceptance and integrity check
Notification exercise	Completed by day 90	Awareness, trigger and update record

A successful backup job does not demonstrate restoration. A deployed alert does not demonstrate that the right team receives it. A completed policy document does not demonstrate that an incident decision can be made under time pressure.

12.3 By role

Role	First decision	Evidence to request
Board	Which essential service and data relationship needs an exercise?	Business-owned recovery and notification results
CISO	Which external signals can be validated now?	Alert dispositions and unresolved dependencies
SOC	Which workflow and identity events must be connected?	Thread, process, persistence and session evidence
Identity	Which active account or token carries material privilege?	Ownership, activity and revocation record
Application owner	Can a user access only authorised objects?	Tested access and export boundaries
Fraud	Can accurate personal information authorise a risky change?	Synthetic recovery and payee-change results
Privacy and legal	Which facts start each duty?	Applicability and awareness decision log
Procurement	Can a critical supplier provide timely evidence?	Tested contacts and contractual alert route
Communications	Which facts can be stated now?	Verified service and data scope with update time

12.4 How Brandefense can help

Brandefense combines Cyber Threat Intelligence, Digital Risk Protection and External Attack Surface Management. External intelligence can help an organisation identify relevant credential offers, impersonation material and public exposure signals for review.

The operational value comes from connecting an external signal to an accountable internal owner. Historical records and criminal claims still require validation. A platform observation does not replace the organisation's incident, privacy or business-continuity decision.

Request a demo to discuss the domains, brands, services and alert workflows relevant to your organisation.

KEY TAKEAWAYS

01

Establish ownership and validate active evidence first.

02

Demonstrate supplier response, phishing resistance and restoration through exercises.

03

Report closure evidence and dated exceptions to the board by day 90.

APPENDICES

Appendices

A–D

THIS CHAPTER ANSWERS

What can a reader conclude from each evidence population?

5

populations with separate units and limits

Appendix A. Scope, evidence and limitations 107

Appendix B. Evidence register 110

Appendix C. Sources 111

Appendix D. Glossary 116

Appendix A. Scope, evidence and limitations

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

A.1 Observation window

Post dates use UTC; public-source dates retain the calendar stated by their publisher.

The requested observation window is 2026-01-01 through 2026-11-22, based on post publication time. Recent activity covers 2026-11-08 through 2026-11-22. Evidence reflects material available when checked on 2026-11-22; the cut-off day was still in progress.

Public disclosures retain their own event, detection and publication dates. A recent disclosure can describe an earlier intrusion. Policy and enforcement developments are labelled separately and do not increase a count of new attacks.

A.2 Evidence populations

Population	Unit	Appropriate conclusion	Main limit
Underground material	Retained post or advertisement	What was offered, requested or asserted	Authenticity and outcome require corroboration
Ransomware listings	Published criminal claim	Visibility in the dated snapshot	Not confirmed intrusion or unique organisation count
Selected-domain observations	Domain and configuration observation	Validation or configuration task	Not independent entities or national prevalence
Public disclosures	Source's stated event and scope	Confirmed or attributed facts within that scope	Estimates and investigation findings can change
Vendor campaign research	Researcher's observed activity	Behaviour and attributed assessment	Local victim extent and attribution can remain unresolved

These populations are not added together. Similar wording or matching totals do not establish overlap. A post mentioning South Korea can be a global price list, ordinary discussion or reporting about another country.

A.3 Exposure and configuration observations

The selected 250-domain portfolio covers ten merged sectors with 25 candidates in each. It is purposive and does not reproduce an official national ranking. Legal-entity independence and ownership remain limitations where not established.

The national Atlas headline is 54 out of 100 for the selected 250-domain portfolio. This report publishes no organisation or sector ratings and no grade distribution. Exposure records are cumulative snapshots dated 2026-11-22; lookalike candidates concern the preceding 30 days. [S3]

DNS, mail-policy and web observations concern the named service and date. An unavailable observation remains unknown. A certificate or policy record cannot establish successful intrusion, and an unobserved configuration element does not prove that no equivalent control exists elsewhere.

A.4 Criminal claims and chronology

Case cards state the claim, observed chronology, established evidence, alternatives and proportionate response. Authentic quotations are redacted to remove victim identifiers, personal information and contact value.

Some retained posts have inconsistent chronology, while others quote older threads or show sample dates from earlier years. Such records can establish circulation of a claim but are not used to date a fresh intrusion.

A fresh advertisement does not establish a fresh intrusion. A repost, a reply and an original theft are different events. Where origin, freshness or file identity is unresolved, the report preserves that uncertainty.

A.5 Payment-card scope

Payment-card figures concern payment-card records in the retained post corpus. They do not represent Brandefense's wider card coverage or measure national card exposure, card theft or fraud loss.

A.6 Ransomware and comparisons

The report compares South Korea with Japan, Taiwan, Hong Kong and Singapore for industrial, financial and digital-service context. The peers' different scale and visibility prevent a risk ranking.

The full-year 2025 figures are context for the partial 2026 window. They are not a matched-period baseline. Industry and country labels describe the listing population and can remain imprecise.

A.7 Source coverage

The public-source evidence includes Korean and English official notices, organisation disclosures, national reporting and vendor research. Russian and Turkish reporting was also considered where relevant. Each cited external fact is tied to a supporting passage and a verification date.

Official-source evidence is uneven across the window. Some original notices are unavailable in the accepted evidence. Where the account rests on press reporting of an official statement, that relationship is explicit and any unqualified original-confirmation claim is avoided.

The report does not claim a complete census of cyber incidents affecting South Korea. Unpublished events, inaccessible original notices and private investigations remain outside what the available evidence can establish.

Post-level coverage has gaps. Counts describe retained evidence; the wider population of relevant posts is not established.

A.8 Names and neutrality

Unverified targets use broad role labels that can describe several organisations. An organisation is named as an affected party only where official confirmation and wide reporting support that choice. Source addresses identifying a withheld party are represented by the publisher's root with an article-withheld notice.

Actor rhetoric does not become the authors' framing. State attributions remain the cited source's assessment, at its stated confidence. No position on political disputes, governments, elections or foreign relations is implied.

A.9 Confidence and action

High confidence can attach to the existence of a retained advertisement while its contents remain unverified. A confirmed disclosure can establish information access without settling the actor or every affected person.

Recommendations are conditional where the evidence is conditional. A validation task can begin before a claim is confirmed. Disruptive containment, public statements and notification decisions should follow the organisation's own evidence and applicable duties.

Appendix B. Evidence register

The post cards are shown in Chapter 4. They reproduce source assertions, not verified outcomes.

Card	Date	Venue	Alias	Language	Location
B01	2026-03-11	Forum	FantancyHacker	Korean	Chapter 4
B02	2026-01-14	Forum	Solonik	English	Chapter 4
B03	2026-03-11	Forum	zSenior	English	Chapter 4
B04	2026-04-26	Forum	0xCAFE	English	Chapter 4
B05	2026-04-28	Forum	TunaFish	English	Chapter 4
B06	2026-08-23	Forum	HighWayToShell	English	Chapter 4
B07	2026-11-12	Forum	taltikgoo	English	Chapter 4
B08	2026-11-19	Forum	Noiem	English	Chapter 4
B09	2026-01-13	Forum	Solonik	English	Chapter 4
B10	2026-03-01	Forum	INDOHAXSEC	English	Chapter 4
B11	2026-03-10	Forum	ZeusHacking	Korean	Chapter 4
B12	2026-03-30	Forum	GlitchX	English	Chapter 4
B13	2026-03-31	Forum	xorcat	English	Chapter 4
B14	2026-04-03	Forum	Grubder	English	Chapter 4
B15	2026-05-28	Forum	Forum participant	English	Chapter 4
B16	2026-07-06	Forum	AshleyWood2022	English	Chapter 4
B17	2026-08-23	Forum	updap	English	Chapter 4
B18	2026-09-09	Forum	□RED✘□	English	Chapter 4
B19	2026-10-07	Forum	updap	English	Chapter 4
B20	2026-10-17	Forum	updap	Chinese and Korean annotations	Chapter 4
B21	2026-11-08	Forum	DataJava	English	Chapter 4
B22	2026-11-10	Forum	DataJava	English	Chapter 4
B23	2026-11-17	Forum	thisversace	English	Chapter 4
B24	2026-11-21	Forum	tet	English	Chapter 4

Appendix C. Sources

External source passages were verified on 2026-11-22–2026-11-23; individual verification dates appear below. The evidence cut-off remains 2026-11-22. Own-source evidence has no public download. Article addresses are withheld where required by the naming policy.

S1: Odin by Brandefense. South Korea country-tagged post counts and retained research corpus, publication window 2026-01-01–2026-11-22. Verified on 2026-11-22.

S2: Brandefense Ransompedia. Listing snapshot for South Korea and four regional comparators, read 2026-11-22. Verified on 2026-11-22.

S3: Odin by Brandefense. Brandefense Atlas exposure ratings, device and credential associations, current listings and selected-domain configuration observations, dated 2026-11-22. Verified on 2026-11-22.

S4: Brandefense Blackhole. Payment-card aggregate evidence for the retained post corpus. Verified on 2026-11-22.

S5: FSC. Financial-sector incidents and response. 2026-11-05. https://www.fsc.go.kr/eng/pr010101/88092?curPage=1. Verified on 2026-11-23.

S6: FSI. Financial Security Institute assessment-system breach. 2026-11-10. https://www.fsec.or.kr/bbs/detail?bbsNo=12144&menuNo=69. Verified on 2026-11-22.

S7: Yonhap. FSI breach reported nationally. 2026-11-10. https://en.yna.co.kr/view/AEN20261110010651315. Verified on 2026-11-22.

S8: DataReportal. Digital 2027 South Korea; October and late-2026 estimates. 2026-11. https://datareportal.com/reports/digital-2027-south-korea. Verified on 2026-11-23.

S9: PIPC. Personal-data breach reporting guidance. current guidance. https://pipc.go.kr/np/default/page.do?mCode=D030040000. Verified on 2026-11-22.

S10: PIPC. Revised privacy law and decree effective September 11. 2026-09-10. https://pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=12459. Verified on 2026-11-22.

S11: KISA / KrCERT/CC. Java security update advisory and FAQ. 2026-11-18;updated2026-11-20. https://www.boho.or.kr/kr/bbs/view.do?bbsId=B0000133&menuNo=205020&nttId=72313&pageIndex=1. Verified on 2026-11-22.

S12: NIST NVD. CVE-2026-114938 record. 2026-11-17. https://nvd.nist.gov/vuln/detail/CVE-2026-114938. Verified on 2026-11-23.

S13: Oracle. November2026 Critical Security Patch Update;Java risk matrix. 2026-11-17. https://www.oracle.com/security-alerts/cspunov2026.html. Verified on 2026-11-22.

S14: AhnLab ASEC. October2026 domestic APT activity review. 2026-11-20. https://asec.ahnlab.com/ko/96683/. Verified on 2026-11-22.

S15: Genians Security Center. NodeLinkRAT campaign research. 2026-11-16. https://www.genians.co.kr/en/blog/threat_intelligence/nodelinkrat. Verified on 2026-11-23.

S16: AhnLab ASEC. Purchase-order document phishing associated with XLoader. 2026-11-13. https://asec.ahnlab.com/ko/96512/. Verified on 2026-11-22.

S17: AhnLab ASEC. Quotation archive phishing associated with SnakeKeylogger. 2026-11-12. https://asec.ahnlab.com/ko/96494/. Verified on 2026-11-22.

S18: KISA. Forum-linked attacks on domestic websites. 2026-01-06. https://www.krcert.or.kr/kr/bbs/view.do?bbsId=B0000133&menuNo=205020&nttId=71932. Verified on 2026-11-22.

S19: KISA. Government and think-tank impersonation QR phishing. 2026-01-10. https://www.krcert.or.kr/kr/bbs/view.do?bbsId=B0000133&menuNo=205020&nttId=71936. Verified on 2026-11-22.

S20: KISA. Ransomware prevention warning. 2026-02-04. https://www.krcert.or.kr/kr/bbs/view.do?bbsId=B0000133&menuNo=205020&nttId=71960. Verified on 2026-11-22.

S21: KISA. Utilities impersonation targeting IT staff. 2026-03-11. https://www.krcert.or.kr/kr/bbs/view.do?bbsId=B0000133&menuNo=205020&nttId=71998. Verified on 2026-11-22.

S22: KISA. Hacktivism and geopolitical threat warning. 2026-03-20. https://www.krcert.or.kr/kr/bbs/view.do?bbsId=B0000133&menuNo=205020&nttId=72005. Verified on 2026-11-22.

S23: KISA. Developer supply-chain diffusion warning. 2026-04-01. https://www.krcert.or.kr/kr/bbs/view.do?bbsId=B0000133&menuNo=205020&nttId=72014. Verified on 2026-11-22.

S24: KISA. KakaoTalk installer impersonation. 2026-04-15. https://www.krcert.or.kr/kr/bbs/view.do?bbsId=B0000133&menuNo=205020&nttId=72027. Verified on 2026-11-22.

S25: KISA. Midnight/Endpoint ransomware against SMEs. 2026-04-16. https://www.krcert.or.kr/kr/bbs/view.do?bbsId=B0000133&menuNo=205020&nttId=72028. Verified on 2026-11-22.

S26: KISA. Travel-reservation data reused for phishing. 2026-05-12. https://www.krcert.or.kr/kr/bbs/view.do?bbsId=B0000133&menuNo=205020&nttId=72049. Verified on 2026-11-22.

S27: KISA. Second developer supply-chain warning. 2026-05-20. https://www.krcert.or.kr/kr/bbs/view.do?bbsId=B0000133&menuNo=205020&nttId=72059. Verified on 2026-11-22.

S28: KISA. OTT-breach follow-on fraud warning. 2026-06-03. https://www.krcert.or.kr/kr/bbs/view.do?bbsId=B0000133&menuNo=205020&nttId=72078. Verified on 2026-11-23.

S29: KISA. Firewall/VPN credential-abuse warning. 2026-06-21. https://www.krcert.or.kr/kr/bbs/view.do?bbsId=B0000133&menuNo=205020&nttId=72105. Verified on 2026-11-22.

S30: KISA. AI-development-tool impersonation. 2026-07-16. https://www.krcert.or.kr/kr/bbs/view.do?bbsId=B0000133&menuNo=205020&nttId=72133. Verified on 2026-11-22.

S31: KISA. Developer credential exposure warning. 2026-07-16. https://www.krcert.or.kr/kr/bbs/view.do?bbsId=B0000133&menuNo=205020&nttId=72132. Verified on 2026-11-22.

S32: KISA/NIS/KNPA/FSI joint. State-backed attacks on Korean nationals and businesses. 2026-07-30. https://www.krcert.or.kr/kr/bbs/view.do?bbsId=B0000133&menuNo=205020&nttId=72144. Verified on 2026-11-22.

S33: KISA. Financial and private-sector incident response warning. 2026-10-03. https://www.krcert.or.kr/kr/bbs/view.do?bbsId=B0000133&menuNo=205020&nttId=72207. Verified on 2026-11-22.

S34: KISA. NAS ransomware warning. 2026-11-03. https://www.krcert.or.kr/kr/bbs/view.do?bbsId=B0000133&menuNo=205020&nttId=72267. Verified on 2026-11-22.

S35: PIPC. OTT-service breach investigation. 2026-06-04. https://pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=12147. Verified on 2026-11-22.

S36: PIPC. Cloud/developer secret-management warning. 2026-06-15. https://pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C010010000&nttId=12179. Verified on 2026-11-22.

S37: PIPC. Three companies sanctioned for 2024 breaches. 2026-07-08. https://pipc.go.kr/ (article URL withheld). Verified on 2026-11-22.

S38: PIPC. Industrial-group enforcement concerning a 2022 incident. 2026-11-12. https://pipc.go.kr/ (article URL withheld). Verified on 2026-11-22.

S39: PIPC. Java-related mass-leak prevention warning. 2026-11-18. https://pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=12660. Verified on 2026-11-22.

S40: Yonhap. University teaching-system breach. 2026-11-14. https://www.yna.co.kr/ (article URL withheld). Verified on 2026-11-22.

S41: Yonhap. Regional-voucher platform API authorization incident. 2026-11-16. https://www.yna.co.kr/ (article URL withheld). Verified on 2026-11-22.

S42: Yonhap. Education-office accidental legal-document disclosure. 2026-11-21. https://www.yna.co.kr/ (article URL withheld). Verified on 2026-11-22.

S43: MBC quoting Seoul police. Multi-company extortion arrests. 2026-10-26. https://imnews.imbc.com/ (article URL withheld). Verified on 2026-11-22.

S44: University official. Research-equipment and IT-service portal compromise. 2026-11-19. https://postech.ac.kr/eng/news-center/university_announcement.do?article.offset=0&articleLimit=10&articleNo=56081&mode=view. Verified on 2026-11-23.

S45: Asia Economy. Employee-training platform unauthorized cloud access. 2026-11-12. https://view.asiae.co.kr/ (article URL withheld). Verified on 2026-11-23.

S47: BleepingComputer. Education-group ransomware update. 2026-01-14. https://www.bleepingcomputer.com/news/security/south-korean-giant-kyowon-confirms-data-theft-in-ransomware-attack/amp/. Verified on 2026-11-22.

S48: University official. Second university-portal breach notice. 2026-11-20. https://postech.ac.kr/ (article URL withheld). Verified on 2026-11-22.

S49: Company official. Education-group cyber incident disclosure. 2026-01-12. https://www.kyowon.co.kr/Media/News_detail?iscont=&nttid=1255&page=1&searchcolumn=&searchpreface=+&searchpreface2=&searchpreface3=&searchword=. Verified on 2026-11-22.

S50: Yonhap. Education-group incident nationally reported. 2026-01-12. https://www.yna.co.kr/view/AKR20260112036251030. Verified on 2026-11-22.

S51: Yonhap. OTT provider acknowledges unauthorized-access leak. 2026-06-03. https://www.yna.co.kr/amp/view/AKR20260603014100017. Verified on 2026-11-22.

S52: SBS via Daum. Public-sector training-system access disclosure. 2026-07-20. https://v.daum.net/v/20260720140004721. Verified on 2026-11-22.

S53: TRT Haber / Anadolu. Turkish coverage of public-sector training incident. 2026-07-22. https://www.trthaber.com/haber/dunya/guney-korede-10-bin-disisleri-personelinin-verilerinin-sizdirildigi-iddia-edildi-951857.html. Verified on 2026-11-22.

S55: KISA. Agency and financial-company impersonation mail. 2026-09-29. https://www.boho.or.kr/kr/bbs/view.do?bbsId=B0000133&menuNo=205020&nttId=72202. Verified on 2026-11-22.

S56: University official notice. Additional personal-data breach notice. 2026-11-22. https://www.jj.ac.kr/ (article URL withheld). Verified on 2026-11-22.

S57: University official notice. First personal-data breach notice. 2026-11-18. https://www.jj.ac.kr/jj/community/notice01.do?articleNo=535802&mode=view. Verified on 2026-11-22.

S58: Etoday. Utility customer and procurement data disclosure. 2026-11-22. https://www.etoday.co.kr/ (article URL withheld). Verified on 2026-11-22.

S60: National Information Resources Service. Administrative email abnormal-access explanation. 2026-11-17. https://www.nirs.go.kr/ncia_MJS/board/dev/board/board.jsp?id=data_201&idx=4779&mode=view. Verified on 2026-11-23.

S61: Yonhap. Unauthorized access to approximately 300 public-service email accounts. 2026-11-16. https://www.yna.co.kr/ (article URL withheld). Verified on 2026-11-22.

S62: Ministry of Foreign Affairs. Ministry briefing on a public-sector training incident. 2026-07-21. https://www.mofa.go.kr/www/brd/m_4078/view.do?page=1&seq=368855. Verified on 2026-11-22.

S63: Ministry of Foreign Affairs. Ministry briefing on a public-sector training incident. 2026-07-23. https://www.mofa.go.kr/ (article URL withheld). Verified on 2026-11-22.

S67: Ministry of SMEs and Startups. Private AI supplier personal-data breach explanation. 2026-11-20. https://www.mss.go.kr/ (article URL withheld). Verified on 2026-11-23.

S68: Yonhap. Startup-program participants in AI supplier breach. 2026-11-13. https://www.yna.co.kr/ (article URL withheld). Verified on 2026-11-22.

S69: Yonhap. Financial-institution outsourced-training disclosure. 2026-09-28. https://www.yna.co.kr/ (article URL withheld). Verified on 2026-11-22.

S70: Yonhap Infomax. Insurer customer data exposed at a claims processor. 2026-11-22. https://news.einfomax.co.kr/ (article URL withheld). Verified on 2026-11-23.

S71: Yonhap. Regional universities report distinct system exposures. 2026-11-18. https://www.yna.co.kr/ (article URL withheld). Verified on 2026-11-22.

S73: JoongAng Ilbo. University discloses approximately 180,000 records. 2026-11-20 (search metadata; body lacks timestamp). https://www.joongang.co.kr/article/25480425. Verified on 2026-11-22.

S74: Financial News / Newsis. University online liberal-arts service breach. 2026-11-19. https://www.fnnews.com/ (article URL withheld). Verified on 2026-11-22.

S75: Segye Ilbo. University and school-transport disclosures. 2026-11-19. https://m.segye.com/ (article URL withheld). Verified on 2026-11-22.

S76: Dailysecu. Research-university portal breach: initial notice corroboration. 2026-11-20. https://www.dailysecu.com/news/articleView.html?idxno=209629. Verified on 2026-11-23.

S78: Yonhap. Utility customer and procurement disclosure scope. 2026-11-22. https://www.yna.co.kr/ (article URL withheld). Verified on 2026-11-22.

S79: Newsis. Utility confirms customer and procurement data breach. 2026-11-22. https://www.newsis.com/ (article URL withheld). Verified on 2026-11-22.

S80: CJ Logistics. Possible personal-data exposure notice. 2026-11-18. https://www.cjlogistics.com/ko/newsroom/notice/NR_00001412. Verified on 2026-11-22.

S81: Edaily. Logistics chatbot abnormal-access investigation. 2026-11-18. https://www.edaily.co.kr/News/Read?mediaCodeNo=257&newsId=04336166645647032. Verified on 2026-11-22.

S90: MITRE ATT&CK. Technique definitions for the analyst behavioural crosswalk. current reference. https://attack.mitre.org/techniques/T1204/002/ https://attack.mitre.org/techniques/T1059/001/ https://attack.mitre.org/techniques/T1053/005/ https://attack.mitre.org/techniques/T1567/002/. Verified on 2026-11-22.

S91: NIST. Digital identity guidance: phishing resistance. Current reference. https://pages.nist.gov/800-63-4/sp800-63b/authenticators/. Verified on 2026-11-22.

S92: OWASP. Object-level authorisation definition. Current reference. https://api-security.owasp.org/editions/2023/en/0xa1-broken-object-level-authorization/. Verified on 2026-11-22.

S93: KISA. ISMS-P certification overview. Current reference. https://www.kisa.or.kr/1050602. Verified on 2026-11-22.

S94: IETF. RFC 9989 DMARC. Current reference. https://www.rfc-editor.org/rfc/rfc9989.html. Verified on 2026-11-22.

S95: IETF. RFC 6376 DKIM. Current reference. https://www.rfc-editor.org/rfc/rfc6376.html. Verified on 2026-11-22.

S96: IETF. RFC 7208 SPF. Current reference. https://www.rfc-editor.org/rfc/rfc7208.html. Verified on 2026-11-22.

S97: Microsoft. Shell Links overview. Current reference. https://learn.microsoft.com/en-us/windows/win32/shell/links. Verified on 2026-11-22.

S98: Daglo. Service security-anomaly notice. 2026-03-27. https://daglo.ai/page/330ca999-eeb2-8056-ae72-c18f3c954ee4. Verified on 2026-11-22.

S99: Yonhap. Company investigation updates a March service incident. 2026-04-09. https://www.yna.co.kr/view/AKR20260409116200017. Verified on 2026-11-22.

S100: Newsis. Service-provider follow-up and information-scope statement. 2026-04-15. https://mobile.newsis.com/view/NISX20260414_0003591185. Verified on 2026-11-22.

S101: National Tax Service. Official apology concerning sensitive information in press photographs. 2026-03-01. https://s.nts.go.kr/nts/na/ntt/selectNttInfo.do?mi=2201&nttSn=1349387. Verified on 2026-11-22.

S102: Yonhap. Press-photo disclosure and uncertain asset valuation. 2026-02-27. https://www.yna.co.kr/amp/view/AKR20260227180500002. Verified on 2026-11-22.

S103: Newsis. Photo-disclosure explanation and valuation limits. 2026-02-28; updated2026-03-01. https://nwww.newsis.com/view/NISX20260228_0003530566. Verified on 2026-11-22.

S104: Yonhap. Hospital image-workflow interruption and restoration. 2026-01-27. https://www.yna.co.kr/ (article URL withheld). Verified on 2026-11-22.

S105: Yonhap. Investigation of an unverified asset-return account. 2026-03-01. https://www.yna.co.kr/ (article URL withheld). Verified on 2026-11-22.

S106: MBC. Contractor customer-support information disclosure. 2026-11-15. https://imnews.imbc.com/ (article URL withheld). Verified on 2026-11-22.

S107: Newsis. Support-service notice and consultation-dependent scope. 2026-11-15. https://nwww.newsis.com/ (article URL withheld). Verified on 2026-11-22.

S108: Yonhap. Provider account of support-system access and varying client scope. 2026-11-14. https://www.yna.co.kr/ (article URL withheld). Verified on 2026-11-22.

S109: Korean National Police, official Korea.kr republication. Police-authored fraud-prevention warning. 2026-03-27. https://www.korea.kr/multi/visualNewsView.do?newsId=148961591. Verified on 2026-11-22.

S110: Newsis. Police warning distinguishes attempts from realised harm. 2026-03-23. https://www.newsis.com/ (article URL withheld). Verified on 2026-11-23.

S111: CBS NoCut News. Approval and expense-document disclosure across two windows. 2026-11-03 05:00. https://www.nocutnews.co.kr/ (article URL withheld). Verified on 2026-11-22.

S112: Yonhap. Business-document access and reported company response. 2026-11-02 16:07. https://www.yna.co.kr/ (article URL withheld). Verified on 2026-11-22.

S113: Financial Services Commission. Regulator confirms financial-company incidents and unresolved relationships. 2026-10-14. https://www.fsc.go.kr/ (article URL withheld). Verified on 2026-11-23.

S114: NewsPim. Financial intermediary disclosure and remaining scope questions. 2026-10-29 10:35. https://www.newspim.com/ (article URL withheld). Verified on 2026-11-23.

S115: Edaily. Later financial-disclosure scope reporting. 2026-11-18 16:22:38. https://www.edaily.co.kr/ (article URL withheld). Verified on 2026-11-23.

S116: Dailysecu. Manufacturing-related extortion claim and preliminary vendor response. Published2026-11-15 16:02:03+09:00; modified2026-11-16 20:06:57+09:00. https://www.dailysecu.com/ (article URL withheld). Verified on 2026-11-22.

S117: Yonsei University Information and Communications Office. University portal information-exposure notice. 2026-10-22. https://www.yonsei.ac.kr/bbs/sc/58/944433/artclView.do. Verified on 2026-11-22.

S118: Dailysecu. Portal-disclosure scope and response reporting. Article discusses October22 notice; exact article publication not independently established in this pass. https://www.dailysecu.com/news/articleView.html?idxno=209012. Verified on 2026-11-22.

S119: NewsPim. Portal-disclosure inquiry and separate exposure windows. Published2026-10-22 17:56; modified2026-11-02 14:11. https://www.newspim.com/news/view/20261022001356. Verified on 2026-11-22.

S120: IETF. RFC 6797: HTTP Strict Transport Security (HSTS). 2012-11. https://www.rfc-editor.org/rfc/rfc6797.html. Verified on 2026-11-23.

S121: W3C. Content Security Policy Level 3. 2026-10-27 (Working Draft). https://www.w3.org/TR/2026/WD-CSP3-20261027/. Verified on 2026-11-23.

S122: IETF. RFC 8659: DNS Certification Authority Authorization (CAA) Resource Record. 2019-11. https://www.rfc-editor.org/rfc/rfc8659.html. Verified on 2026-11-23.

S123: IBM. What is Customer Relationship Management (CRM)? https://www.ibm.com/think/topics/crm. Verified on 2026-11-23.

S124: IBM. What is network attached storage? https://www.ibm.com/think/topics/network-attached-storage. Verified on 2026-11-23.

Appendix D. Glossary

Term	Plain meaning
Account recovery	The process used to restore access when a user cannot sign in
API	A software interface through which applications request information or actions
Atlas headline	A national portfolio exposure figure; not an attack probability
Authentication	Checking the identity presented by a user or service
Authorisation	Deciding which information or actions that identity may access
Blackhole	Brandefense's intelligence source used for the retained post material
CAA	Certification Authority Authorization: a DNS record specifying which certificate authorities may issue certificates for a domain [S122]
CRM	Customer relationship management: software for managing interactions with current and potential customers [S123]
CSP	Content Security Policy: a browser policy controlling which resources a page may fetch or execute [S121]
Cloud administrator	An identity with management privileges in a cloud environment
Combolist	A collection of login identifiers and passwords from different sources
Controller	The party responsible for deciding the purposes and means of personal-data processing
Credential	Information or a token used to authenticate an account
Device association	An external observation linking a device's records with a service or domain
DKIM	A mail-signing mechanism using a domain's published verification key
DMARC	A domain policy for handling mail that fails specified authentication checks
DNSSEC	DNS signatures and validation links used to check the authenticity of DNS data
DS record	A parent-zone record linking a domain's DNSSEC keys to its parent
ERP	Enterprise resource planning software used to manage business processes

Term	Plain meaning
Exfiltration	Unauthorised transfer of information out of a controlled environment
HSTS	HTTP Strict Transport Security: a website policy directing browsers to use secure connections [S120]
HWP	A Hangul word-processing document format; a document-themed name does not establish a safe file
Infostealer	Malware designed to collect information such as stored account data
ISMS-P	A Korean certification framework covering information security and personal-information protection
LNK	A Windows shortcut file that can start a program or another action
MFA	Multi-factor authentication, requiring more than one type of sign-in evidence
NAS	Network-attached storage: a device providing shared file storage over a network [S124]
Object authorisation	Checking whether a particular identity may access the particular record or object requested
Phishing-resistant MFA	Authentication bound to the legitimate service, reducing credential-relay risk
Processor	A party handling personal data on behalf of a controller
Ransompedia	Brandefense's ransomware-listing source; a listing records a criminal claim
Recovery target	The business-approved service and time objectives used to judge restoration
Session	An authenticated interaction that can remain usable after the initial sign-in
SPF	A domain's declaration of systems authorised to send its email
SSO	Single sign-on, where an authentication service grants access to multiple applications
Stealer log	Information recorded by malware on an affected device
Supplier tenant	A customer-specific environment within a shared service
TLS	Encryption and authentication used to protect a network connection

Term	Plain meaning
Token	A credential representing an identity, session or delegated permission
TLP:CLEAR	A sharing label permitting public distribution, subject to other applicable duties

The glossary explains terms used in the report. It does not assign a threat actor or establish that an organisation suffered a particular outcome.

Technical terminology references: [S91][S92][S93][S94][S95][S96][S97].

About this report

Prepared by Odin by Brandefense as the Brandefense Country Report · South Korea 2026. The report prioritises retained own-source evidence and source-checked public disclosures, while preserving each population's limits.

The English master is the reference edition. The Korean edition is translated from it with AI assistance and carries a visible notice. Both editions preserve the same numbers, evidence IDs, source references and defensive decisions.

Recommendations describe conditional defensive actions. They do not state that any organisation has or has not implemented a control. This package does not claim a complete census of cybercrime affecting South Korea.

© 2026 Brandefense. All rights reserved.

ABOUT BRANDEFENSE

Attackers See You First. We make sure you do.

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

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

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

GARTNER PEER INSIGHTS
4.7 / 5

COVERAGE
3 pillars
CTI, DRPS, EASM

MONITORING
24 / 7
Open, deep and dark web

REQUEST A DEMO

Request A Demo. See what attackers see.

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

Request a demo →

AWARDS

Recognised Around The World. Technology and trust.

Selected awards recognising Brandefense technology and innovation.



Top InfoSec Innovator

2026



Deloitte Technology Fast 500 EMEA

2024



Global InfoSec Awards

2025



Cybersecurity Excellence Awards

2025

See Brandefense In Action.

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

Request a demo →

BRANDEFENSE

See what attackers see. Before they act.

UNITED STATES

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

TÜRKIYE

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

BRANDEFENSE.IO