BRANDEFENSE COUNTRY REPORT · MALAYSIA 2026

Brandefense Malaysia Cyber Threat Landscape Report 2026

Identity, supplier dependencies and underground claims

Odin by Brandefense

Research window: 1 January–22 November 2026

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

250

selected organisation-domain entries across 11 sector cells

8,748–9,196

relevant posts in the retained Malaysia-tagged set

87

Malaysian ransomware leak-site listings in the reporting window

35

banking and finance entries in the selected portfolio

CONTENTS

Contents

01	Executive summary	04
	Report map	08
02	Malaysia's digital and threat context	09
03	National exposure: a portfolio of 250 selected domains	14
04	What we see on the dark web	23
05	Incidents and claims by sector	34
06	Hacktivism and DDoS	46
07	Threat actors	51
08	The fraud economy	58
09	Banking and finance deep dive	65
10	Regulatory and national response	70
11	Outlook	75
12	Action plan	79
A	Appendix A. Scope and evidence	86
B	Appendix B. Evidence register	89
C	Appendix C. Sources	90
D	Appendix D. Glossary	93
	About this report	95

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

About this edition

AI-assisted analysis and drafting. The report distinguishes retained observations, actor assertions and public accounts. The English edition is the master text.

CHAPTER 01

Executive summary

01

THIS CHAPTER ANSWERS

Which evidence should leaders act on first?

55 of 249

assessed entries had a credential listed for sale when checked

1.1 Five findings for leaders 05

1.2 Four decisions for leaders 06

1.3 The year in numbers 06

CHAPTER 01

Executive summary

IN SHORT

Current identity evidence deserves the first validation decision. Of 249 assessed portfolio entries, 55 had a credential listed for sale when checked; one selected entry remains unknown. Public accounts describe distinct service and supplier boundaries. Underground advertisements remain claims, while recent official warnings distinguish payment, account and device responses. Assign identity, continuity and fraud owners, validate the relevant evidence and record what closes each action.

1.1 Five findings for leaders

1. Current listings require account validation. Of 249 assessed entries, 55 had a credential listed for sale when checked on 22 November. The national Atlas headline is 48/100. One of 250 selected entries has no usable exposure result. These are portfolio observations, not national prevalence or confirmed current account access. [S1][S2]

The same assessed population has 485,462 recorded device associations and 3,686,480 historical credential-record associations. Neither total is a count of people or new 2026 incidents. Validate account status, evidence dates and device ownership before deciding the response.

2. The underground volume needs a coverage boundary. Brandefense Blackhole recorded 782,224 Malaysian-tagged posts during the reporting window. The retained country-tag material contains 25,355 distinct posts, so the report does not treat that retained view as the entire tagged population. A country reference does not establish targeting. [S3]

The recent 8–22 November view contains 922 tagged posts, including eight tagged forum posts. A separate forum view contains 14 posts; these populations overlap and are not added. Advertised volumes, dates and possession claims require separate corroboration.

3. Extortion publications remain separate from incident confirmation. Ransompedia contains 87 Malaysian listings dated within the window, including six dated 8–22 November. Qilin appears on 18 listings and The Gentlemen on 12. These labels describe source publications; they do not establish entry routes, active access or nationally distinct incidents. [S4]

4. Service and supplier boundaries determine continuity decisions. Public accounts distinguish interrupted terminal services, credit-reporting access and support-file questions. They also distinguish public websites from financial services. Preserve each source's stated boundary and date, then test the actual business dependency and its recovery evidence. [S5][S6][S7][S8]

5. Fraud response depends on what a user submitted or ran. November MyCERT advisories describe an assistance-themed payment-information lure and a free-laptop messaging-account lure. The June script advisory describes a different endpoint decision. Establish the user's action, then route card, account and device questions to the relevant owners. [S9][S10][S11]

1.2 Four decisions for leaders

1. Give every relevant current credential listing an identity owner and a dated disposition. Validate active status and corroborating activity before declaring account access.
2. Test an authenticated fallback for credit, trading, logistics and other external dependencies. Close the exercise with reconciled transactions and a business-owner return-to-service decision.
3. Separate payment-card, messaging-account and endpoint intake. Determine which information was submitted and whether a file ran before choosing the response.
4. Map notification readiness to the actual entity and activity. Preserve detection, assessment and service-restoration dates, and have legal validate the applicable duty.

1.3 The year in numbers

782,224

Malaysian-tagged Blackhole posts dated within the reporting window

WHAT IT IS NOT

National incidents or affected people

25,355

Distinct posts in the retained country-tag view

WHAT IT IS NOT

The full tagged population

922

Tagged posts dated 8–22 November

WHAT IT IS NOT

Distinct newly affected organisations

250

Selected organisation-domain entries

WHAT IT IS NOT

A national census or independent legal-entity count

249

Entries with usable Atlas exposure observations

WHAT IT IS NOT

Complete exposure coverage of the selected portfolio

55 / 249

Assessed entries with a current credential listing

WHAT IT IS NOT

Confirmed active accounts or intrusions

48/100

National Atlas headline for assessed entries

WHAT IT IS NOT

A sector rating or national prevalence estimate

485,462

Recorded device associations across assessed entries

WHAT IT IS NOT

Unique people or newly affected devices

3,686,480

Historical credential-record associations

WHAT IT IS NOT

Unique active passwords

199 / 250

Selected domains with completed passive observations

WHAT IT IS NOT

A complete national hygiene assessment

87

Ransompedia Malaysian listings in the reporting window

WHAT IT IS NOT

Independently confirmed incidents

1,244

Distinct Malaysian-attributed payment cards

WHAT IT IS NOT

National card theft or fraud loss

Figures retain their own populations and dates. They must not be added to produce a national incident or victim total. [S3][S1][S12][S4][S13]

KEY TAKEAWAYS

01

Validate current account evidence before escalating a claim into an incident finding.

02

Maintain distinct identity, supplier, service and fraud response owners.

03

Require completion evidence and preserve unknown outcomes in the board record.

Report map

Twelve chapters, five reader routes. Begin with the question that matches your role, then follow the evidence to its validation owner.

Board and executives	Which decisions deserve resources and what demonstrates completion?	01 03 11 12
CISO and security leads	Which evidence is ours and which response comes first?	03 05 07 09 10 12
SOC and threat intelligence	What was observed, what was claimed and what supports the relationship?	04 06 07 08 A B
Fraud and customer protection	Which user action determines the payment, account or device response?	04 08 09 12
Legal and communications	Which service boundary and notification duty can we support?	05 06 10 12

Chapter	It answers
1 Executive summary	Which findings and decisions matter first
2 Context	Which identity, supplier and service dependencies shape the evidence
3 Selected portfolio	What 250 selected-domain observations can and cannot establish
4 Dark web	Which offers and recent posts deserve validation
5 Sectors	Which reported boundaries matter to each sector
6 Hacktivism and DDoS	What claims establish and how to validate impact
7 Actors	Which relationships and listing observations are supported
8 Fraud economy	How to route payment, account and endpoint decisions
9 Banking	How financial-service and customer boundaries differ
10 Regulation	Which entity, activity, trigger and effective date applies
11 Outlook	Which conditional scenarios and change signals to plan for
12 Action plan	Who should act and what completion evidence the board needs

CHAPTER 02

Malaysia's digital and threat context

02

THIS CHAPTER ANSWERS

Which dependencies explain the incidents in this report, and what should Malaysian organisations protect together?

4

recurring boundaries: identity, suppliers, public websites and operational services

2.1 High household connectivity expands the service boundary 10

2.2 A service can fail outside the organisation that customers recognise 10

2.3 Customer information and current access are different propositions 11

2.4 Messaging lures cross the customer and workplace boundary 11

2.5 Public websites and operational systems need separate status statements 12

2.6 Official warnings and legal duties serve different purposes 12

CHAPTER 02

Malaysia's digital and threat context

IN SHORT

Malaysia's public reporting describes several different problems: criminal data offers, phishing, vulnerable public websites and interruptions to financial and logistics services. They require different evidence and different owners. An affected supplier does not establish access to every customer system. An actor's data advertisement does not establish a new intrusion. Map critical service and data dependencies, then test the identity and recovery controls at each boundary.

2.1 High household connectivity expands the service boundary

DOSM's ICT release published on 23 April 2026 reported internet access in 97.1% of households for reference year 2025. This is a household-access measure. The same release reported internet use by 98.3% of individuals aged 15 and above. The metadata defines the survey population and use period. Neither figure is a 2026 observation, and the denominators are not interchangeable. [S14] [S15]

For defenders, high household access gives customer-facing digital processes broad relevance. It does not measure exposure to a particular campaign. The useful planning question is whether customers and staff can recognise and report a suspicious transaction, message or account request through an established route.

A digital service also depends on the information and providers around it. Authentication, customer support, payment processing and recovery can have different owners. The incidents in this report make those boundaries concrete without suggesting that one connectivity figure explains their frequency.

2.2 A service can fail outside the organisation that customers recognise

The 2026 cases show why an organisation's own network is only part of its operational boundary. A technology-services group acknowledged an incident affecting part of its IT environment. A container terminal reported interruption and phased recovery. A credit-reporting provider disclosed unauthorised access in one business environment. The disclosed scopes differ, but each creates decisions for connected organisations. [S16][S5][S6]

For a customer-facing organisation, the practical question is which transaction or dataset depends on that environment. A supplier relationship alone does not establish that the customer was affected. Conversely, an unaffected internal network does not settle whether customer information held elsewhere was accessed. The response should trace the relevant data and service, then preserve the distinction in communications.

A useful dependency map identifies the provider, the business process, the data exchanged and the alternative operating mode. It should also name the person who can confirm the provider's statement. A contract list without these details leaves the operational question unanswered when a service stops.

The report therefore treats supplier exposure as a boundary to validate. It does not infer a single supply-chain campaign from unrelated incidents. Shared business consequences do not establish shared infrastructure, entry routes or operators.

2.3 Customer information and current access are different propositions

On 21 June, reporting of an MKN and NACSA statement said circulating personal-data claims were believed to concern incidents before 2022. The statement distinguished those claims from current platforms and referred to continuing investigation. That is the authorities' assessment at that date. It does not establish the origin of every file advertised later. [S17]

This distinction matters for identity and fraud teams. An advertisement published in 2026 can describe information obtained earlier. A recent post date is evidence of recent advertising, not necessarily recent acquisition. The report retains the post date while separately recording any claimed or independently established data date.

Older identity information can still be relevant when a fraudster uses it to make a message convincing. That is a defensive scenario, not a finding that a particular advertised dataset was used. Organisations should test how much their recovery and customer-verification processes depend on static personal information.

Password and session decisions need a different test. A historical association does not show whether an account remains active, whether its owner changed the password, or whether a session is usable. Current validity and ownership must be established before a disruptive response. Identity teams should retain a reasoned disposition rather than treating every historical record as a live incident.

2.4 Messaging lures cross the customer and workplace boundary

MyCERT's June warning described malicious Windows scripts delivered through WhatsApp Desktop or Web. The advisory concerned a document-style lure and remote-management installation after execution. It did not describe a vulnerability in the mobile messaging application. [S11]

The November advisories described different outcomes. An aid-themed portal sought identity, card and one-time-password information. A free-laptop lure sought messaging-account login codes and a two-step password. The communication channel was similar, but the assets at risk differed. [S9][S10]

For defenders, the first question should be what the user did. Receiving a message, opening a page, submitting an identity number, entering a payment-card number and running a script are separate events. Each requires a proportionate response. A single generic instruction to reset every password can miss the relevant asset.

The workplace boundary is equally important. A staff member can use a personal messaging account on a work device. That possibility warrants an endpoint and account check where the evidence supports it. It does not establish that the employer's systems or customer database were accessed.

2.5 Public websites and operational systems need separate status statements

A late-June NC4 alert described attacks involving a vulnerable content-management extension. The vendor published an update and guidance for older installations. Separately, November reporting quoted a bank's statement that a corporate-website issue did not affect banking services, deposits or customer information. These are distinct episodes with different source accounts. [S18][S19][S8]

The shared defensive lesson is to define the service boundary before describing impact. A public website, customer authentication, transaction processing, file sharing and core databases are different assets. A website claim should prompt relevant checks without becoming a claim about every connected system.

The health-sector case also distinguishes support-file access from patient-service availability (Case H). Its limits belong beside the claim rather than in a remote footnote. [S7]

Communications teams should prepare a service matrix before an incident. Each row needs a current state, the evidence supporting it, the responsible owner and a timestamp. This makes a narrow statement easier to defend and update than a broad claim that everything is safe.

NACSA separately assessed a cloud-productivity disruption as more likely technical or infrastructure-related than a cyberattack. This report keeps that account outside its eight-event case set. The notice does not settle unrelated claims, and a technical explanation does not remove the need to test service continuity. [S20]

2.6 Official warnings and legal duties serve different purposes

MyCERT advisories identify campaigns and practical response steps. NACSA and NC4 provide national coordination and alerts. BNM and the personal-data regulator have separate supervisory roles. A warning about a campaign is not itself a finding that every recipient is affected. Chapter 10 distinguishes the relevant obligations and effective dates. [S11][S18][S9][S10]

The same separation applies to official reassurance. On 18 November, a minister described circulating dark-web claims as unverified and potentially old. The report attributes that statement to its source and date. It does not use it to cancel individual incidents acknowledged elsewhere during the year. [S21]

For a CISO, the practical objective is a record that can support both technical decisions and notification assessment. That record should state what is known, what remains unverified, which data or services are involved and when the organisation became aware. Legal and operational teams can then apply the relevant duty to the same facts.

KEY TAKEAWAYS

01

Supplier incidents, public websites and operational platforms require separate impact boundaries.

02

Recent advertising does not establish recent theft or current account access.

03

Route messaging incidents by the action taken and the asset disclosed, then validate the appropriate service or account.

CHAPTER 03

National exposure: a portfolio of 250 selected domains

THIS CHAPTER ANSWERS

What does the selected portfolio tell us, and which conclusions remain outside its evidence?

250

selected organisation-domain entries across 11 sector cells

3.1 Universe card 15

3.2 Separate a published policy from its actual effect 16

3.3 TLS and homepage observations answer narrow questions 18

3.4 Current listings and historical associations require separate validation 18

3.5 Lookalikes, documents and mentions are investigation leads 21

3.6 Turn the chapter into a validation queue 21

CHAPTER 03

National exposure: a portfolio of 250 selected domains

IN SHORT

Of 249 assessed portfolio entries, 55 had a credential listed for sale when checked. The national Atlas headline is 48/100. One of the 250 selected entries has no usable exposure result. Passive observations cover 199 entries. These are selected-domain results, not national prevalence. Validate current listings with identity owners, then review dated device and credential associations.

3.1 Universe card

The portfolio supplies a defined denominator for the chapter. Related brands, group companies and local services can overlap. A selected domain is not necessarily an independent legal entity. [S2]

Item	Definition
Population	250 organisation-domain entries across 11 sector cells
Selection	Purposive public-knowledge portfolio of public bodies, financial services, major businesses and essential services
Unit	One selected primary domain for each portfolio entry
Domain observations	245 entries supplied a DNS response; five supplied no response in the retained observations
Ownership	Domain responses and ordinary page content do not establish independent legal ownership
Comparison	Descriptive results for this portfolio; no national prevalence or sector-security ranking
Overlap	Related organisations, brands and service populations can overlap
Date	Public observations and the selection register are dated 22 November 2026

A domain without a response is an unknown observation. It is not evidence that an organisation is inactive, insecure or absent. The five entries remain in the portfolio denominator, while control-specific results retain the denominator that could actually be assessed.

The sector cells provide descriptive groupings. They are not a claim that the report represents every organisation or service within a sector.

Sector	Portfolio entries	Reading limit
Government	40	Different bodies and service activities
Banking and finance	35	Includes more than licensed banks or card issuers
Insurance	15	Selected insurers and related services
Energy and utilities	20	Different energy and public-service activities
Transport and logistics	20	Different modes and supporting services
Telecom and technology	20	Network and technology-service businesses
Education	25	Selected institutions and related groups
Healthcare	15	Provider and group relationships can overlap
Retail and holdings	25	Brands and parent groups can overlap
Manufacturing and industry	20	Selected industrial and consumer businesses
Hospitality and media	15	Combined descriptive cell for service businesses
Total	**250**	**Selected entries, not national prevalence**

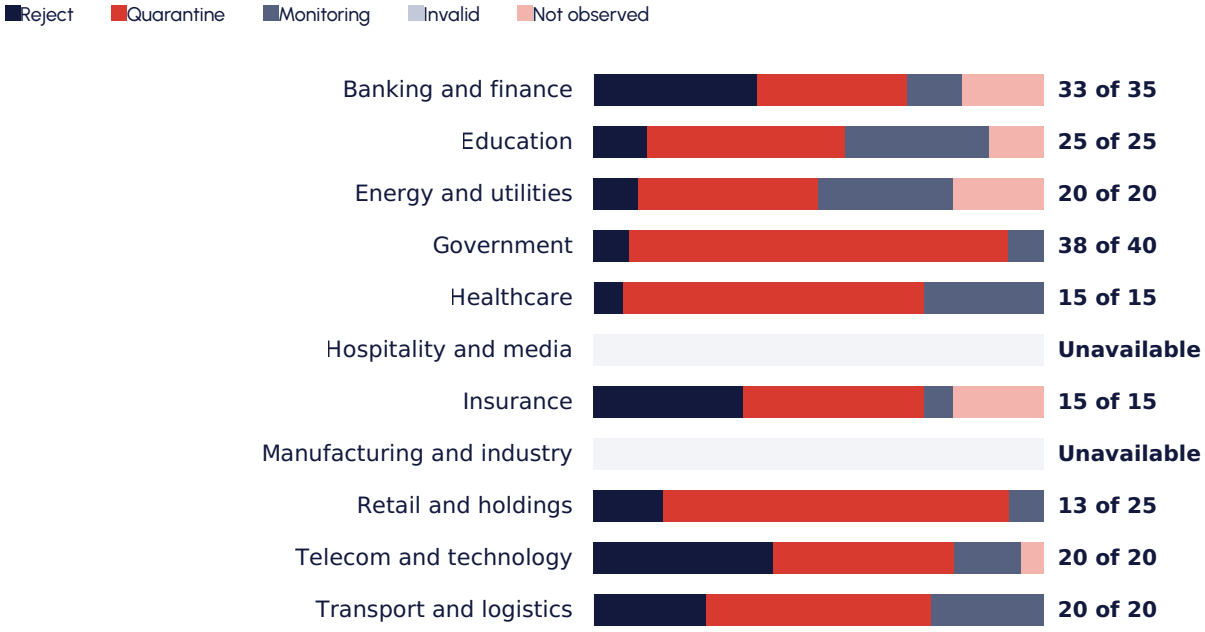
3.2 Separate a published policy from its actual effect

The mail-domain result concerns an observed published policy. A rejection or quarantine policy is a useful configuration finding. It does not establish that every message is subject to the policy or that every impersonation route is blocked. The report therefore avoids treating policy presence as universal enforcement. [S12]

The practical next step is validation with the messaging owner. The owner should determine which legitimate senders use the domain, whether intended messages are authenticated and what exceptions remain. A configuration change is complete when the service still works as intended and the result is supported by records.

A non-observed signing record is similarly limited. It does not establish that the organisation signs no mail. A DNSSEC delegation record is not a validation of the entire trust chain. These distinctions prevent a control-presence table from becoming a broader security verdict.

Published mail policies vary across the selected portfolio



Source: passive observations, 22 November 2026 [S12]. 199 entries have passive results; each sector retains its own denominator. Published policy does not establish enforcement; unavailable results do not establish absent controls.

Completed passive observations cover 199 of 250 selected domains. Of 245 domains that supplied a DNS response, 46 lack a completed passive observation; five selected domains supplied no DNS response. These unavailable results remain unknown. [S12]

Observation	Result	Denominator
Published DMARC rejection policy	41	199 completed observations
Published DMARC quarantine policy	106	199 completed observations
Published monitoring policy	35	199 completed observations
No DMARC policy observed	17	199 completed observations
SPF record observed	181	199 completed observations
DKIM signing record observed	136	199 completed observations
DNSSEC delegation record observed	60	199 completed observations
Valid / invalid / unresolved TLS	158 / 10 / 31	199 completed observations
Homepage answered / inconclusive	150 / 49	199 completed observations
HSTS observed	110	150 answering homepages

Unavailable sector control results remain unknown. The incomplete passive coverage does not support a complete national hygiene assessment.

3.3 TLS and homepage observations answer narrow questions

A TLS observation concerns the connection and certificate result at the stated date. A valid result does not establish that the application is patched. An invalid result differs from an unresolved observation, and both differ from a homepage that simply did not answer.

Homepage-header results use responding pages as their denominator. They should not be divided by every selected domain when some pages did not respond. A missing or inconclusive result remains unknown rather than becoming a failed control.

The service owner should validate a reported configuration finding against the intended service. That includes confirming whether the selected domain is the right entry point and whether the observation concerns a parent, subsidiary or shared service. The report's selected-domain boundary does not resolve those organisational relationships.

3.4 Current listings and historical associations require separate validation

A current credential-market listing, a historical credential record and an infected-device association are different signals. They should not be added into a count of people or incidents. An association can require investigation without establishing the account's current validity or the device's ownership.

Of 249 assessed entries, 55 had a credential listed for sale when checked on 22 November 2026. One selected entry has no usable exposure result. The selected portfolio contains 250 entries, so the listing status of that remaining entry is unknown. [S1]

The national Atlas headline is **48/100** for the 249 assessed entries. Only the national rating is published. Sector tables contain observed signals, with separate selected and assessed denominators. They provide no sector rating or national prevalence estimate.

Observed exposure signals across the selected sectors

	Device associations	Employee devices	Credential history	Current listings	Listing history	Documents
Banking and finance (35)	86%	66%	86%	26%	23%	74%
Education (25)	96%	96%	96%	44%	44%	96%
Energy and utilities (20)	95%	80%	95%	20%	20%	55%
Government (40)	92%	85%	95%	20%	20%	68%
Healthcare (15)	93%	87%	87%	7%	7%	67%
Hospitality and media (15)	80%	60%	80%	13%	13%	47%
Insurance (15)	100%	67%	100%	27%	27%	67%
Manufacturing and industry (19)	63%	53%	89%	5%	5%	58%
Retail and holdings (25)	88%	80%	100%	20%	20%	84%
Telecom and technology (20)	90%	85%	95%	25%	25%	75%
Transport and logistics (20)	90%	85%	95%	25%	25%	70%

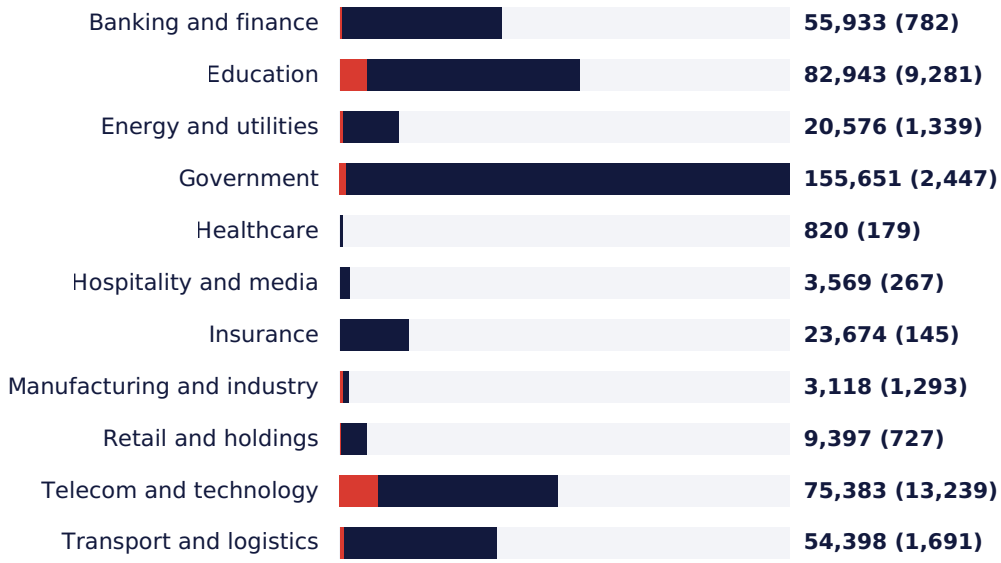
Current credential listings by sector (coral). Denominators are assessed entries. Source: Brandefense exposure observations, 22 November 2026 [S1][S2]. 250 selected entries, 249 assessed. Cumulative associations can overlap; they are not unique people or new incidents.

Observation	Result	Limit
Assessed entries / selected entries	249 / 250	One entry unavailable
Entries with current credential listings	55 / 249	Account validity unverified
Entries with historical credential records	231 / 249	Historical records, not unique people
Entries with device associations	221 / 249	Ownership and present status unverified
Entries with employee-classified devices	193 / 249	Classification needs owner validation
Entries with document associations	176 / 249	Confidentiality unverified

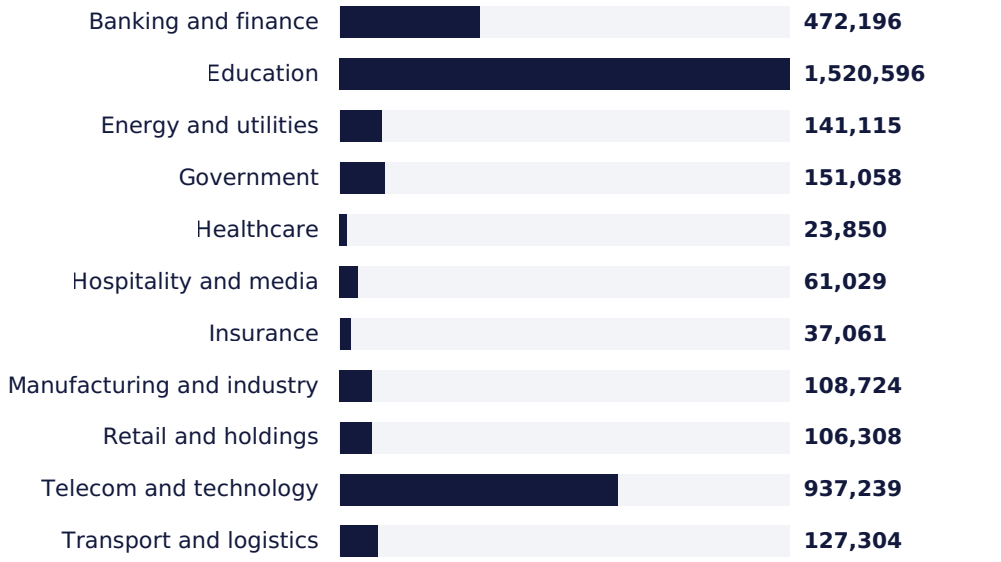
Device and credential associations by sector

Employee-classified Other (not employee-classified)

Device associations (employee subset in parentheses)



Historical credential-record associations (separate scale)



Source: Brandefense exposure observations, 22 November 2026 [S1][S2]. 250 selected entries, 249 assessed. Cumulative associations can overlap; they are not unique people or new incidents.

The assessed entries have 485,462 recorded device associations, including 31,390 employee-classified associations. Other device associations are not established as customer-owned. Cross-domain overlap is possible. These are cumulative source observations, not devices newly affected during 2026. [S1]

Historical credential-record associations total 3,686,480: 900,247 breach-database records, 1,216,827 stealer-log lines and 1,569,406 combolist entries. Stealer logs are records produced by information-stealing malware. Combolists are compiled username/password combinations. [S57] These records are not unique accounts, active passwords or confirmed incidents. No ownership or freshness conclusion follows from the total alone.

Education accounts for 1,520,596 credential-record associations; telecom and technology account for 937,239. Those totals describe this selected portfolio. They do not compare the security of the two sectors. Staff, student, customer and shared-service relationships need separate validation.

Document associations total 4,318. Publication context and confidentiality remain unverified. Similar content or repeated references can span domains, so this is not a count of unique confidential files.

An organisation receiving a current listing should first identify the relevant account and its status. If the account is active, the identity team should review appropriate sign-in and session evidence. A privileged or remote-access account can require urgent action under the organisation's own incident plan.

Historical records need their dates and remediation context. A disabled account with no relevant recent activity differs from a currently used account with corroborating activity. The record should state which proposition was validated and what evidence supports the decision.

Device associations need the same care. An employee-associated record can guide a staff-device investigation. Other associations do not automatically belong to customers. The service owner and endpoint team should establish ownership and relevance before drawing that conclusion.

3.5 Lookalikes, documents and mentions are investigation leads

A similar-looking name is not evidence that a domain is malicious. A document mentioning an organisation is not evidence that the document is confidential. A post naming a country or company is not necessarily an attack against it. Each proposition needs the relevant context.

Lookalike observations cover 19 October–18 November 2026, separately from the reporting cut-off. There are 33,811 candidate associations across 178 assessed entries. Similar names can be unrelated; these are not confirmed phishing sites. Other exposure counters describe the records held when checked on 22 November. [S1]

For a potential impersonation domain, the first questions concern purpose, hosting context and observed use. For a document, the owner should identify the information classification and legitimate publication context. For a post, the analyst should distinguish a generic mention, an advertisement and a specific access assertion.

3.6 Turn the chapter into a validation queue

A useful queue separates configuration validation from incident investigation. Public policy findings belong with the service owner. Current account evidence belongs with identity and incident response. Supplier or data-access propositions need the relevant business and privacy owners.

The queue should record the asset, evidence date, proposition, owner, next action and completion condition. It should preserve unknown results instead of silently dropping them. This makes the chapter useful without asking the reader to treat a purposive portfolio as a national security measurement.

KEY TAKEAWAYS

01

The 250 entries define a selected-domain portfolio, not 250 independently verified legal entities.

02

Published policies, TLS results and homepage responses have different assessed denominators.

03

Validate each finding with the relevant owner and retain unknown outcomes as unknown.

CHAPTER 04

What we see on the dark web

04

THIS CHAPTER ANSWERS

What do Malaysian data and access advertisements establish, and which claims need a separate investigation?

8,748–9,196

relevant posts in the retained Malaysia-tagged set

4.1 Volume describes source visibility 24

4.2 The offers overlap 26

4.3 Six advertisements, six bounded propositions 27

4.4 Circulation is evidence of an offer, not its origin 32

4.5 Additional claims stay visible without becoming a total 32

CHAPTER 04

What we see on the dark web

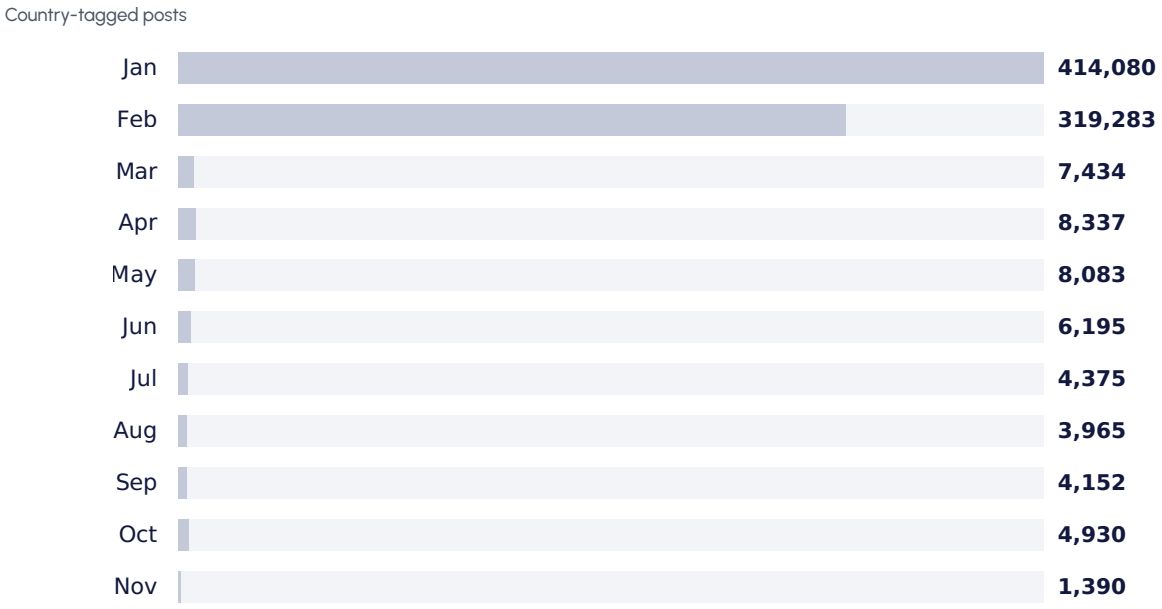
IN SHORT

The source records 782,224 Malaysia-tagged posts during 1 January–22 November 2026. The retained tagged set contains 25,355 posts, including a relevant range of 8,748–9,196. These are post populations, not incident or victim totals. Advertisements offer consumer information, financial data and business access. Repetition and seller assurances do not establish authenticity or fresh compromise. Use the evidence cards to scope validation, identify the responsible owner and define what would justify escalation.

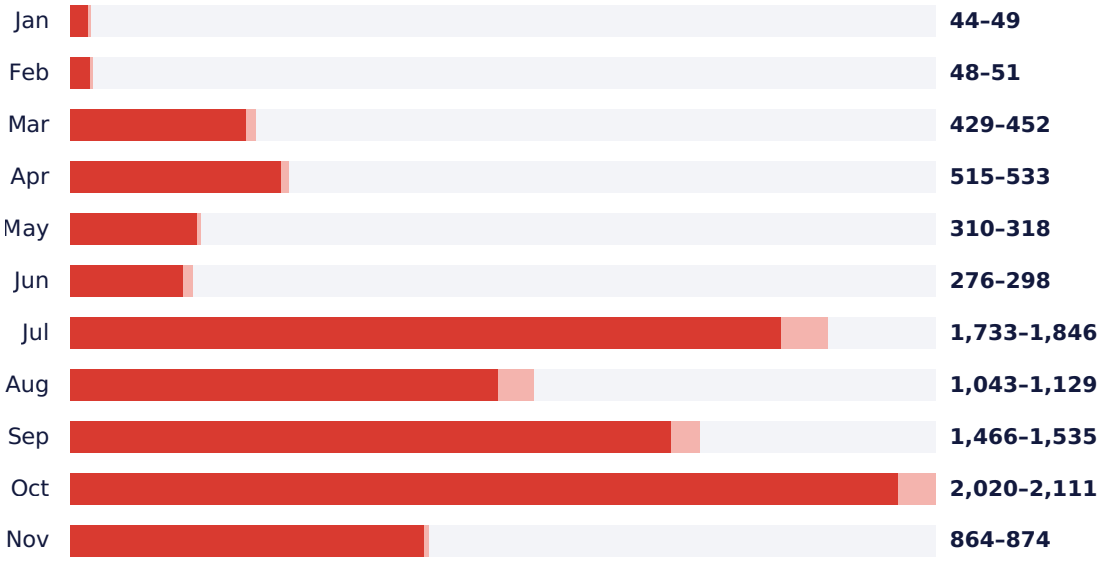
4.1 Volume describes source visibility

Post counts do not measure Malaysian incident prevalence. The 782,224 source count and 25,355 retained tagged posts describe different coverage populations. Neither is a census of attacks. A country reference can concern a market, a claimed dataset, a news report or an advertised service. [S3]

Monthly post volumes have uneven coverage and do not establish threat growth



Relevant-post range (separate scale; uneven coverage)



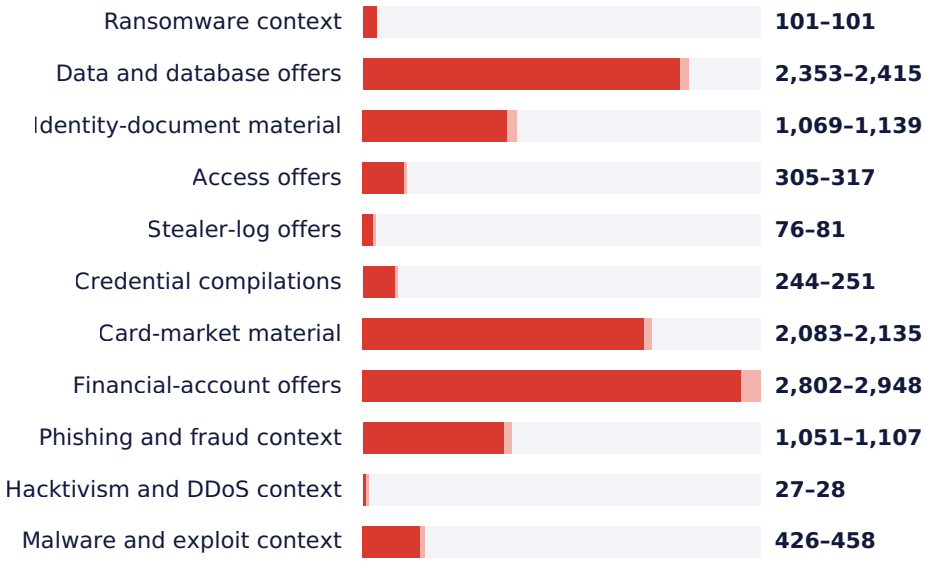
Source: Brandefense Blackhole, Malaysia-tagged posts, 1 January–22 November 2026; November partial [S3]. Retained material has uneven coverage; posts and overlapping themes are not confirmed incidents.

January and February dominate the source's tagged count, while later months contribute more of the relevant retained material. That contrast cannot establish a rise in successful attacks. Source composition and coverage differ across the period. November ends on 22 November and is an incomplete month. [S3]

The relevant retained range is 8,748–9,196 posts. Its bounds describe uncertainty in this post population. They do not estimate hidden incidents, unique people or the probability that an advertisement is genuine. The same underlying offer can appear in several posts, languages or venues. [S3]

4.2 The offers overlap

Financial-account and data offers recur across overlapping post themes



Source: Brandefense Blackhole, Malaysia-tagged posts, 1 January–22 November 2026; November partial [S3]. Retained material has uneven coverage; posts and overlapping themes are not confirmed incidents.

Observed theme	Relevant retained posts	Evidence limit
Financial-account offers	2,802–2,948	Advertised availability does not establish usable accounts or bank-system access
Data and database offers	2,353–2,415	A title and sample fields do not establish origin or valid records
Card-market material	2,083–2,135	Posts are separate from the narrow card observations in Chapter 9
Identity-document material	1,069–1,139	Document validity and affected-person counts remain separate questions
Phishing and fraud context	1,051–1,107	Promotion and reporting do not establish a completed fraud
Access offers	305–317	Privilege descriptions are seller claims until validated
Credential compilations	244–251	Geographic labels do not establish an organisational incident

The rows overlap and must not be added. A single post can offer account access, identity material and payment services. The source records content under these themes, without confirming that an advertised transaction occurred. Chapter 8 considers fraud propositions; Chapter 9 gives the separately scoped card figures. [S3]

English and Chinese-language material both contribute substantially to the retained set. The relevant upper-bound counts are 3,897 English-labelled posts and 3,519 Chinese-labelled posts. Language does not identify an operator's nationality or establish state direction. Native wording also matters when an automated translation changes a commercial term into an allegation. [S3]

4.3 Six advertisements, six bounded propositions

The following cases use authentic redacted passages from retained posts. They illustrate different validation questions. They are not six confirmed breaches, and their source dates are posting dates. Quantities and identifying details have been withheld rather than presented as verified impact. [S3]

A

CASE A

A public-sector data offer needs provenance evidence

Evidence card B01 | 9 Jan 2026 | Retained forum advertisement | Public sector

Claim unverified

CLAIM	A 9 January forum advertisement offered sensitive information under a Malaysian public-sector label.
HELD	The advertisement and its wording are retained. It establishes that a claim was published.
ALTERNATIVES	The offer could concern old material, repackaged information, inaccurate labelling or authentic records. The post does not resolve those possibilities.
LIMITS	Authenticity, acquisition date, completeness and current access are unverified. No organisation confirmation is established by this source.
RESPONSE	The security and privacy owners should assess field relevance against authorised records, then investigate any corroborated access or disclosure boundary.

Bottom line

Validate provenance and the relevant disclosure boundary before accepting a public-sector label.

B

CASE B

A financial-sector label does not establish bank access

Evidence card B02 | 8 May 2026 | Retained forum advertisement | Financial services

Claim unverified

CLAIM	A forum post dated 8 May advertised a database associated with a Malaysian financial institution.
HELD	The title, sector claim and redacted sample section are retained.

ALTERNATIVES	Customer information can originate from several relationships. A financial-sector label does not identify which system, if any, supplied it.
LIMITS	The source does not establish authenticity, affected-account count, current access or institutional confirmation.
RESPONSE	The fraud and security teams should test the claimed data boundary through authorised evidence before taking disruptive account actions.

Bottom line

Establish the relevant data boundary before inferring access to a financial institution.

Evidence card B01 — 9 Jan 2026

Seller persona | Retained forum advertisement | Forum | English

ORIGINAL

i have [REDACTED_ORGANISATION] OF MALAYSIA data databse i.e confidential, sensitive

Note. Authentic redacted excerpt. Seller-stated quantities and identifying details withheld. Posting date is not an incident date.

Held

The retained forum advertisement and its wording.

Not established

Authenticity, source of the information, current access, completeness, and a confirmed incident.

Evidence card B02 — 8 May 2026

Seller persona | Retained forum advertisement | Forum | English

ORIGINAL

[REDACTED_ORGANISATION], Malaysia Database

Note. Authentic redacted excerpt. Seller-stated quantities and identifying details withheld. Posting date is not an incident date.

Held

The retained advertisement, a financial-sector label, and a redacted sample section.

Not established

Database authenticity, provenance, affected account count, or compromise of the institution.

C

CASE C

Consumer information and account activity are separate claims

Claim unverified

Evidence card B03 | 23 Aug 2026 | Retained forum advertisement | Consumer information

CLAIM	A forum advertisement dated 23 August offered Malaysian consumer information and asserted that associated messaging accounts were active.
HELD	The advertisement and its mixed English and Chinese headings are retained.
ALTERNATIVES	Circulating contact lists, inaccurate account checks and repackaged material could produce similar advertising.
LIMITS	Consent, origin, freshness, unique-person count and account validity remain unverified. No organisational incident follows from the post alone.

RESPONSE	Privacy and fraud owners should assess the stated field categories and relevant impersonation scenarios without contacting advertised individuals or treating every entry as valid.

Bottom line

Assess contact-data provenance and lure scenarios without treating advertised accounts as validated.

D

CASE D

A freshness promise is an assertion about age

Evidence card B04 | 6 Sep 2026 | Retained forum advertisement | Financial marketing

Claim unverified

CLAIM	A 6 September forum post offered Malaysian financial-marketing information and asserted that records were sourced within 30 days.
HELD	The advertisement contains a claimed age and a seller-stated quantity.
ALTERNATIVES	The date may describe packaging, a seller's receipt or repeated promotion rather than original acquisition.
LIMITS	Neither the claimed age nor the quantity is independently established. The offer does not identify a confirmed institutional incident.
RESPONSE	The business and privacy owners should establish lawful data provenance and assess relevant lure scenarios before accepting the seller's description of freshness.

Bottom line

Validate the claimed acquisition period separately from the posting date.

Evidence card B03 — 23 Aug 2026

Seller persona | Retained forum advertisement | Forum | English

ORIGINAL

This is a database of property owners in Malaysia who are active on WS Rows: [record count withheld]

Note. Authentic redacted excerpt. Seller-stated quantities and identifying details withheld. Posting date is not an incident date.

Held
The retained advertisement and its mixed English/Chinese sample headings.

Not established
Consent, provenance, freshness, unique-person count, account validity, or an organisational incident.

Evidence card B04 — 6 Sep 2026

Seller persona | Retained forum advertisement | Forum | English

ORIGINAL

FRESH DATABASE [record count withheld] Malaysia Crypto & Forex Leads All records sourced within 30 days.

Note. Authentic redacted excerpt. Seller-stated quantities and identifying details withheld. Posting date is not an incident date.

Held
The retained advertisement, claimed count, and claimed age.

Not established
The supplied count, claimed age, accuracy, consent, provenance, or a named organisation incident.

CASE K

K

A November customer-data offer does not date an intrusion

Claim unverified

Evidence card B05 | 19 Nov 2026 | Retained forum advertisement | Consumer business

CLAIM	A forum advertisement dated 19 November offered customer records under a Malaysian consumer-business label.
HELD	The forum title and a redacted sample section are retained.
ALTERNATIVES	The advertisement may describe earlier circulation, another source relationship or an inaccurately labelled product.
LIMITS	Authenticity, exact record count, current compromise and incident date are unverified. Posting near the cut-off does not establish a new November intrusion.
RESPONSE	The security and privacy owners should define the claimed customer-data boundary and escalate when authorised comparison or access evidence supports it.

Bottom line

A November advertisement does not establish a November intrusion.

CASE L

L

Administrator access is an advertised capability

Evidence card B06 | 1 Feb 2026 | Retained forum advertisement | Private-sector businesses

Claim unverified

CLAIM	A Russian-language seller post dated 1 February advertised access associated with Malaysian businesses and claimed administrator privileges.
HELD	One retained post contains two Malaysia-labelled entries and the privilege claim.
ALTERNATIVES	The entries may concern unrelated access, stale access or inaccurate descriptions. A shared seller does not establish one intrusion or operator.
LIMITS	Access validity, persistence, ownership, affected systems and incident dates remain unverified. Identifying business and system details are withheld.
RESPONSE	The identity and infrastructure owners should review relevant privileged accounts, sessions and remote access using internal evidence before accepting the advertised capability.

Bottom line

Review privileged access using internal evidence; the seller claim is not validation.

Evidence card B05 — 19 Nov 2026

Seller persona | Retained forum advertisement | Forum | English

ORIGINAL

[REDACTED_ORGANISATION] Shopping & Customer Database

Note. Authentic redacted excerpt. Seller-stated quantities and identifying details withheld. Posting date is not an incident date.

Held
The retained forum title and a redacted sample section.

Not established
Authenticity, current compromise, exact record or person count, incident date, or institutional confirmation.

Evidence card B06 — 1 Feb 2026

Seller persona | Retained forum advertisement | Forum | Russian

ORIGINAL

Доступ Malaysia [identifying details withheld] Domain Admin

TRANSLATION

Access Malaysia [identifying details withheld] Domain Admin

Note. Authentic redacted excerpt. Seller-stated quantities and identifying details withheld. Posting date is not an incident date.

Held
A single seller post with two entries labelled Malaysia and a claim of administrator privileges.

Not established
Access validity, persistence, true ownership, affected systems, incident date, or a shared operator behind different advertised entries.

4.4 Circulation is evidence of an offer, not its origin

A retained forum discussion challenges the provenance of a Malaysian consumer-data advertisement. The challenge is useful counterevidence to an unqualified freshness narrative, but it does not establish that the challenger is correct. Both assertions require their own evidence. [S3]

A Chinese-language advertisement includes Malaysia in a multi-country menu and promises active, high-quality material. Those words describe the seller's assurances. They do not establish data quality, nationality, possession or a completed sale. Repeated catalogues can keep a proposition visible without demonstrating a new acquisition. [S3]

Evidence card B07 — 10 Feb 2026

Forum participant | Retained forum discussion | Forum | English

ORIGINAL

All your sample data can be found in publicly available databases.

Note. Published assertion only; no independent confirmation of the offered material.

Held
A provenance challenge in the retained thread.

Not established
Whether the data was repackaged, overlap size, freshness, or which participant is correct.

Evidence card B09 — 8 Mar 2026

Seller persona | Retained channel post | Telegram | Chinese

ORIGINAL

全网低价包活出售 顶级质量 先到先得欢迎咨询

TRANSLATION

Sold at low prices across the network, guaranteed active. Top quality, first come first served; inquiries welcome.

Note. Published assertion only; no independent confirmation of the offered material.

Held
The advertisement and its claims of low prices, availability and quality.

Not established
Data validity, activity, provenance, nationality, any named organisation incident or common operator.

Chinese-language catalogue variants also advertise a Malaysia-labelled banking-user product among unrelated foreign offers. The shortened menu is a data-sale lead. It does not establish a named bank incident, a validated dataset or a common operator behind similar wording. The catalogue family remains a mention rather than another confirmed case. [S3]

4.5 Additional claims stay visible without becoming a total

Further retained posts contain role-based mentions concerning public-sector, education, healthcare, technology, travel and industrial organisations. Some posts describe re-uploads or an earlier data period. Others concern query services, credential catalogues or claimed records whose Malaysian association is uncertain. These mentions do not establish additional confirmed incidents. [S3]

A title repeated in another venue is evidence of circulation. It does not independently confirm the dataset, establish a second incident or identify the first seller. Likewise, an advertised query service does not establish access to a government system. A person appearing in a claimed dataset does not necessarily identify its source organisation.

For an affected organisation, the first useful output is a scoped proposition: the claimed fields, source date, relevant internal boundary and evidence needed to validate it. The investigation should preserve both corroborating and contradictory findings. Escalation should follow that evidence, with a named owner for account, privacy and continuity decisions.

KEY TAKEAWAYS

01

Relevant retained post counts describe source visibility, not a national incident total.

02

Data, access and freshness claims require separate validation, even when advertisements repeat.

03

Assign an owner and closure evidence to each relevant proposition before escalating a claimed impact.

CHAPTER 05

Incidents and claims by sector

THIS CHAPTER ANSWERS

Which service boundaries did public reporting identify, and what first response does each sector need?

6

sector perspectives, with the evidence status retained

5.1 How to read the sector examples 35
5.2 Technology suppliers: distinguish possible access from confirmed misuse 38
5.3 Financial services: trading availability and data impact are separate 38
5.4 Consumer payment services: reconcile the return to normal 39
5.5 Telecommunications: isolated disclosure does not establish network entry 39
5.6 Logistics: recovery must include connected workflows 40
5.7 Credit reporting: one environment is not the entire data estate 41
5.8 Healthcare: support files require their own access boundary 42
5.9 Public-service transactions: integrity can require investigation without an outage 43
5.10 Public-facing services: a website event does not identify an entry route elsewhere 43
5.11 Airline supplier notice: possible customer impact is not confirmed carrier-system access 44
5.12 Public displays need a vendor-access and isolation plan 44
5.13 Protective action does not establish a completed incident finding 45

CHAPTER 05

Incidents and claims by sector

IN SHORT

Public reporting describes supplier, website, trading, credit-reporting, logistics and support-file incidents. Confirmation of an incident does not confirm an actor's identity, an advertised record count or an alleged entry route. Some reports describe precautionary restrictions rather than established theft. Use the sector examples to identify your service boundary, ask for the supporting evidence and assign the first validation step.

5.1 How to read the sector examples

This chapter separates an organisation's acknowledgement, an authority's account and an actor's claim. They can concern the same episode without establishing the same proposition. An organisation can confirm unauthorised access while the volume advertised by a seller remains unverified. A restriction imposed during investigation can also protect services that were not affected.

The cases below retain generic target labels. The label is a privacy choice, not a statement about an organisation's importance. Dates identify the reported chronology. They do not establish the date on which data was first obtained unless a source says so.

The first-response column is a recommendation for organisations with a comparable dependency. It does not imply that the organisation in the case failed to perform that action. The report does not infer national sector prevalence from these examples.

Technology services

OBSERVED OR REPORTED

Incident affecting part of a supplier's IT environment; documents potentially accessed

STATUS AND LIMIT

Company notice; possible data access, no confirmed misuse at notice date

FIRST RESPONSE

Identify the documents and relationships within the affected environment

Banking and finance

OBSERVED OR REPORTED

Website disruption, broker restrictions and credit-reporting interruption

STATUS AND LIMIT

Separate events; do not combine their service or data scopes

FIRST RESPONSE

Validate authentication, transactions and public-site status separately

Logistics

OBSERVED OR REPORTED

Terminal interruption followed by phased recovery

STATUS AND LIMIT

Operator incident described in industry reporting; group and theft claims remain separate

FIRST RESPONSE

Test manual processing and the evidence required before reopening interfaces

Healthcare

OBSERVED OR REPORTED

Limited support-file platform access in November

STATUS AND LIMIT

Official account quoted in reporting; no actor or data volume established

FIRST RESPONSE

Check file scope, external sharing and account privileges

Public services

OBSERVED OR REPORTED

Content-management extension attacks and aid-themed phishing

STATUS AND LIMIT

Official technical alerts; phishing does not establish access to impersonated systems

FIRST RESPONSE

Prove fixed extension state and protect identity-verification routes

Consumer services

OBSERVED OR REPORTED

Job-task, assistance and messaging-account lures

STATUS AND LIMIT

Campaign warnings; reported totals use their own time periods

FIRST RESPONSE

Separate recipient actions and route account, device and payment responses

The retained public accounts acknowledge eight individually scoped incidents in this chapter. This is the report's case set, not a national total. Broader broker-component reporting has unknown cardinality; precautionary restrictions, campaign notices and possible supplier impact are outside this eight-event count.

Reporting period	Generic role	Acknowledged boundary	Limit
April notice; February incident	Technology-services group	Part of an IT environment; possible document access	No confirmed misuse at notice date
June–July	Consumer payment-service platform	Cyberattack-related interruption and restoration	Shared service reach is not a separate-incident count
July–August reporting	Telecommunications provider	Isolated unauthorised customer-information disclosure	No broader customer incident established
September	Container-terminal operator	Cybersecurity interruption and phased restart	Actor, theft volume and industrial-control access unconfirmed
September	Credit-reporting provider	One consumer-business environment and reporting services	No conclusion about every dataset or customer institution
October	Financial institution	Operational incident and phased service recovery	No verified actor or entry route

Reporting period	Generic role	Acknowledged boundary	Limit
29 October	Municipal public-display system	Unauthorised content and display shutdown	Access route, operator and wider network boundary unestablished
November	Health-sector support platform	Limited support-file access	Clinical availability does not resolve every file question

The eight-event boundary follows the respective public accounts, with their limitations retained. [S16][S22][S23][S5][S6][S24][S7][S25][S26]

5.2 Technology suppliers: distinguish possible access from confirmed misuse

A technology-services group disclosed a 10 February incident in an April notice. It said documents containing limited personal information might have been accessed or removed. The notice described identity, contact and employment information and said it had identified no confirmed misuse at that time. [S16]

This supports a specific supplier question: which documents and business relationships were present in the affected environment? It does not support a conclusion that every customer system was reached. Nor does the absence of confirmed misuse at the notice date establish that the information could never be used.

Customers should ask for the affected document categories, relevant dates and evidence supporting the provider's boundary. They should validate unexpected changes to payment instructions through an established channel. That control is appropriate to the disclosed contact and business context without assuming an unreported payment loss.

5.3 Financial services: trading availability and data impact are separate

March reporting carried an exchange statement about incidents in specific components used by several brokers. The statement said the incidents were contained and broader market integrity remained intact. A later broker episode should be assessed on its own dates and service scope. [S27]

In late October, an online broker confirmed restrictions following a detected cybersecurity attempt. Its written response described the affected domestic-equity order channel while other functions remained available. It said there was no evidence of data loss in its assessment at that date. [S28]

The operational lesson is to prepare a channel-specific fallback. A broker needs to know which orders can still be accepted, how a manual instruction is authenticated and how queued instructions are reconciled. The report does not treat a precautionary restriction as proof that theft succeeded.

A separate October account concerned a financial institution that detected suspicious activity on 7 October. Reporting of its statement said core services resumed on 12 October. Some reset, registration and new-account functions remained unavailable at that date. The institution said customer funds were safe. [S24]

This supports a differentiated recovery test. Transaction processing, account recovery and onboarding need their own validation before the organisation describes full restoration. The source does not establish a group or entry route, and the report adds no such attribution.

The September credit-reporting case creates a different dependency. A lender can retain its own systems while losing access to an external report needed for decisions. Credit, fraud and operations teams should agree how to handle pending applications, delayed checks and subsequent reconciliation. Case G develops that boundary.

5.4 Consumer payment services: reconcile the return to normal

July reporting quoted service announcements that a consumer payment platform was back online after a cyberattack. The report says disruption notices began on 30 June and restoration was announced on 2 July. It also records user reports of balance issues. Those reports are not a measured total of lost funds. [S22]

A shared platform can support many service authorities without creating the same number of separate intrusions. The report therefore retains the interruption as one individually scoped event. It does not publish a claimed user volume or infer access to every connected authority.

For an operator, recovery should include a transaction and balance reconciliation process. Customer support needs a way to distinguish a delayed display, a disputed balance and a confirmed accounting discrepancy. Security should validate the service boundary while the business owner resolves the operational exceptions.

The completion evidence should identify which records were compared, how exceptions were handled and who approved normal operation. A running app alone does not close a customer's balance query. These are proposed controls, not a claim that the operator omitted them.

5.5 Telecommunications: isolated disclosure does not establish network entry

Reporting published in late July and early August quoted a telecommunications provider describing an isolated unauthorised disclosure of customer account information. The company said it identified an individual and had no indication of a broader incident involving other customers. That is its dated account, not proof about every later allegation. [S23]

The case concerns information access and disclosure. It does not establish a corporate-network intrusion. The report omits the person, account, bill and amount details because none is needed for the defensive decision.

The relevant owner should validate which roles can view or disclose customer information, how access is logged and how exceptional requests are approved. A review should distinguish legitimate support access from disclosure outside the authorised process. It should retain the evidence for the specific case without generalising an allegation to other staff.

An account-information disclosure can require a privacy and customer-response decision even when no wider system access is established. The service owner and privacy lead should use the same facts, including the scope of the information and the basis for any broader exclusion.

5.6 Logistics: recovery must include connected workflows

CASE F

F

A terminal interruption and phased restart

Transport and logistics

Service interruption reported

REPORTED EVENT	A container-terminal operator reported a cybersecurity incident in September. Industry reporting described operational interruption, restored systems and a progressive resumption of operations. [S5]
CHRONOLOGY	Industry reporting on 11 September described an incident shortly before midnight on 9 September and a progressive restart. These are service-status dates, not a confirmed intrusion timeline.
WHAT WE CAN ESTABLISH	The source material supports interruption, phased recovery and the reported restoration of systems. It does not establish compromise of cranes, industrial controllers or every connected logistics partner.
ALTERNATIVES	A data-theft claim and an operational outage can have different causes or scopes. A claimant's publication alone cannot settle their relationship.
LIMITS	The report has no target-side forensic record. A ransomware attribution and an advertised theft volume remain separate claims unless the operator or authority confirms them.
RESPONSE	Operations and security teams should rehearse manual gate, cargo and temperature-sensitive shipment processes. Define who validates interfaces and reconciles transactions before normal service resumes.

Bottom line

Test the fallback and reconciliation process; restoration does not establish an actor or theft volume.

A logistics exercise should follow a transaction across the interfaces that matter. The test can begin with an unavailable terminal system and end with reconciled cargo records. It should include communications to hauliers and customers, the handling of exceptions and the return to normal processing.

A successful restore is only one completion criterion. The business owner should also confirm that delayed or manually processed records are complete. Security should document what was validated before reconnection. This avoids equating a running application with a fully reconciled service.

5.7 Credit reporting: one environment is not the entire data estate

CASE G

Consumer information in a credit-reporting environment

Financial information services

Provider acknowledged access

REPORTED EVENT	A credit-reporting provider disclosed unauthorised access to one consumer-business environment on 23 September. Its filing said files containing a limited subset of consumer information were accessed. Some reporting services were temporarily unavailable. [S6]
CHRONOLOGY	The 23 September disclosure described the initial access and interruption boundary. It does not, on its own, establish a later restoration state. Each subsequent service-status statement requires its own dated support.
WHAT WE CAN ESTABLISH	The source material supports access to the described environment and a service interruption. It does not establish that every bureau dataset or every customer financial institution was affected.
ALTERNATIVES	A partner can experience delayed reporting without its own network being accessed. Data scope and service scope must therefore be checked separately.
LIMITS	The report does not convert a later conditional financial estimate into a measured incident loss. It has no independent total of affected consumers.
RESPONSE	Credit and fraud owners should identify decisions made with delayed or alternate reports. Recheck exceptions after restoration and document the evidence used for each decision.

Bottom line

Validate the affected report and data boundary, then reconcile decisions made during interruption.

A provider's narrow description should guide the first questions. Which files were involved? Which reports were unavailable? Which clients received a changed service? The answers can differ. Defenders should retain that distinction in customer notices and internal decision logs.

The same discipline helps with data-subject communications. An account in an unaffected environment should not be described as exposed merely because it belongs to the same corporate group. Conversely, an interrupted service can require operational action before the full data scope is known.

5.8 Healthcare: support files require their own access boundary

CASE H

H

Limited support-file access disclosed in November

Healthcare

Official limited-access account

OFFICIAL ACCOUNT	A health-sector statement quoted in reporting said an incident was detected on 12 November. The account described limited unauthorised access to a support-file storage and sharing platform at one facility. [S7]
CHRONOLOGY	The statement was reported on 14 November. It described access restrictions, password resets, audits and stronger authentication. Those are the institution's stated measures, not actions performed by this report's authors.
WHAT WE CAN ESTABLISH	The statement said major operational systems and patient services were unaffected. Its preliminary finding said main databases were not encrypted. These are distinct statements about service and encryption scope.
ALTERNATIVES	No main-database encryption does not establish that no files were viewed or removed. A support platform can require investigation even when care continues.
LIMITS	No official actor link or affected-data volume was established in the cited account. The report does not join this episode to a separate website incident or an actor's extortion claim.
RESPONSE	The platform owner should identify files, external links and account permissions within the affected boundary. Clinical operations should independently confirm service status and continuity arrangements.

Bottom line

Separate patient-service availability from support-file and privacy questions.

This case illustrates why a health organisation needs more than a list of clinical systems. File-sharing services can hold operational or personal information even when they do not deliver care. Their owners should know how external sharing is approved, how access is reviewed and how to suspend a link without losing required records.

The communication decision should follow the evidence. A statement about uninterrupted care answers an availability question. It does not answer every privacy question. Security, privacy and clinical operations should agree which question each sentence addresses.

5.9 Public-service transactions: integrity can require investigation without an outage

An August report carried the responsible agency director's account of unauthorised approvals on a public-service transaction platform. It described a joint enforcement operation in July. The report is an authority's investigation account, not a court finding or independent validation of every alleged technical detail. [S30]

The case supports a different question from availability monitoring: were transactions approved as intended? A platform can continue responding while its approval integrity requires investigation. The report does not infer that this occurred at any other public service or join it to a separately reported technical outage.

For the service owner, the first checks concern transaction histories, privileged access and the approval workflow. Investigators' statements about alleged involvement should remain attributed to them. A defensive review can test segregation of duties and supplier access without assigning blame or making a broader claim about employees.

The completion evidence should connect each relevant approval to its authorised record and the person or service permitted to perform it. An unresolved exception should remain visible to the business and incident owners. A normal public front page does not answer this integrity question.

5.10 Public-facing services: a website event does not identify an entry route elsewhere

The late-June extension alert and the November corporate-website account both concern internet-facing content, but they do not establish a common campaign. The June alert names a technical vulnerability. The November reporting quotes a third-party technical explanation. The report keeps those source accounts separate. [S18][S8]

Organisations should maintain an inventory of content-management extensions, the owner responsible for updates and a route to a trusted restore. A front page returning to normal is not enough to establish that unauthorised accounts or files are absent. Case E in Chapter 7 sets out the verified version guidance.

For a finance or public-service organisation, status communications should name the affected function. "Corporate website unavailable" is more precise than a statement about all digital operations. The supporting service matrix should remain available to the incident lead as facts change.

The public-website episode also illustrates how an observation and a cause statement can differ. Reporting described an outward website change; the institution gave a third-party technical explanation. This report records both without inferring a wider intrusion. [S31][S8]

Point	Public observation	Institution account	What remains unresolved
Website	A publication reported altered public-site content [S31]	The institution described a corporate-site issue [S8]	The observation alone does not establish internal access
Service scope	The outward site condition did not measure transaction or data access	The institution said banking services, deposits and customer information were unaffected [S8]	The report has no independent forensic record of the event
Cause	A visible change does not determine its cause	The institution referred to a third-party technical issue [S8]	An actor's broader assertion would need separate corroboration

5.11 Airline supplier notice: possible customer impact is not confirmed carrier-system access

A 1 November report quoted an airline's 31 October website statement about its reservation supplier. The statement said some customer data processed between August 2023 and September 2026 might be affected. It distinguished the supplier incident from its own IT systems and reported no evidence of financial-information access at that date. [S32]

The dates describe a processing period, not a confirmed intrusion duration. Possible customer impact is not a verified affected-person total. The report does not transfer another airline's booking count to Malaysian customers or assume that the supplier's entire customer base was affected.

The account remains attributed to the reporting of the company statement. It is treated as a supplier-dependency disclosure outside the eight individually scoped incident count. The report preserves the possible-impact and no-evidence qualifications.

Travel and customer-service owners should identify which bookings and fields the supplier's notice covers. They should ask for a dated impact statement and retain the distinction between reservation data, payment information and the carrier's own systems. Customer warnings should match that boundary rather than repeating an actor's larger claim.

5.12 Public displays need a vendor-access and isolation plan

On 29 October, a municipal public-display system showed unauthorised content. Reporting quoted the authority saying it shut down displays and was investigating with its vendor. Police subsequently confirmed an investigation. The access route, operator and wider network boundary were not established in the reporting reviewed. [S25] [S26]

This is one reported system incident, not a separate incident for each display. It does not establish ransomware or access to operational-control systems. Include externally managed displays in the asset inventory, restrict vendor administration and test a safe isolation and restoration procedure.

5.13 Protective action does not establish a completed incident finding

On 10 November, reporting quoted a public-body chairman describing protective cooperation concerning suspected website activity. The chairman said a full report was outstanding. This report retains a suspected-activity mention, without treating it as confirmed system access, data theft or a service outage. [S33]

The incident lead should distinguish protective action from a completed investigation. Record the available service and access evidence, the questions still unresolved and the person responsible for the next update. A later normal page does not itself settle the earlier allegation.

KEY TAKEAWAYS

01

Keep each provider, platform and service boundary distinct, including during recovery.

02

Confirmation of an incident does not confirm an actor, advertised volume or cause.

03

Give every affected process an owner, a fallback and evidence for return to normal service.

CHAPTER 06

Hacktivism and DDoS

06

THIS CHAPTER ANSWERS

What can a persona statement, an availability claim and an official website alert each establish?

27–28

relevant retained posts carrying hacktivism or DDoS themes

6.1 Availability, alteration and access are different propositions 47

6.2 A Malay-language denial is a persona statement 47

6.3 The official website alert has a separate evidence boundary 48

6.4 A claim should trigger a bounded validation task 49

6.5 Keep rhetoric separate from evidence 49

CHAPTER 06

Hacktivism and DDoS

IN SHORT

The relevant retained set contains 27–28 posts with hacktivism or DDoS themes. These are content observations, not confirmed disruptions. A Malay-language persona statement denies hacking and warns of impersonation. Separately, official technical reporting describes attacks involving a website extension. No relationship between those propositions is established here. Validate service impact, access and authorship separately, using monitoring, logs and the organisation's incident account.

DDoS means distributed denial of service: an attack from multiple sources intended to disrupt access to a system or service. [S58]

6.1 Availability, alteration and access are different propositions

The source records 27–28 relevant retained posts carrying hacktivism or DDoS themes. This narrow range does not measure the country's total DDoS activity, confirmed website alterations or successful intrusions. A country mention, a channel label or an actor slogan does not establish an affected Malaysian service. [S3]

An availability screenshot can show one observation at one time. It does not establish the duration, cause or customer effect of an outage. A claimant's description of an attack also does not establish whether access extended beyond the public website.

A changed page is a different proposition from a traffic flood. Either can have business impact, but each needs supporting evidence. The defender should preserve service records, relevant access logs and the restoration boundary before assigning a cause or accepting an actor's account.

6.2 A Malay-language denial is a persona statement

A retained post dated 9 March appears under the MalaysiaHacktivist label. The statement denies hacking government websites or other individuals and warns of impersonation. It is evidence of what that persona published. It does not establish the author, the truth of the denial or responsibility for another event. [S3]

Evidence card B08 9 Mar 2026

MalaysiaHacktivist Retained channel post Telegram Malay

ORIGINAL

Pihak Kami tidak melalukan perbuatan menggodam website kerajaan atau individu lain.

TRANSLATION

We do not carry out hacking of government websites or other individuals.

Note. Persona statement only; no connection to other website events established.

Held
The statement itself and the publishing persona label.

Not established
The author identity, truth of the denial, who performed any other activity, and any relationship with separate website events.

[GROUP malaysia-persona]

The statement matters because a name can circulate independently of its author. A claimed identity should not automatically inherit responsibility for separate posts or website events. Conversely, a denial is not independent evidence that an event did not happen. The investigation must retain the difference between a published statement and a verified attribution.

6.3 The official website alert has a separate evidence boundary

NC4's late-June alert described attacks involving the JCE extension for Joomla. The vendor and CVE Program sources address the vulnerability and fixed-version boundary. They support technical remediation without identifying who caused every website event in that period. Chapter 7 develops the technical case and its limits. [S18][S19][S34]

The retained March statement does not establish a connection to the June alert. Their dates, subjects and evidence types differ. Neither shared website terminology nor a national reference supplies the missing relationship.

9 Mar 2026	**Persona statement** A retained Malay post denies hacking and warns of impersonation; identity and truth remain unverified. [S3]
26 Jun 2026	**Technical alert** NC4 describes attacks involving a website extension; the alert does not attribute every contemporaneous website event. [S18]

This timeline places two observations in order. It is not a campaign chain, an attribution finding or evidence of coordination. A later official advisory cannot retroactively confirm an earlier persona's statement.

6.4 A claim should trigger a bounded validation task

Proposition received	First owner	Evidence that answers it	Escalation condition
Service unavailable	Service operations	Availability history and upstream traffic records	Sustained or material service impact supported by monitoring
Public content altered	Web and security teams	Trusted content comparison and administrative activity	Unauthorised changes or access evidence
Internal access asserted	Incident response	Relevant account, session and system records	Corroborated access to the claimed boundary
Files allegedly obtained	Security and privacy teams	Authorised field and provenance comparison	Relevant records or disclosure supported by evidence
Persona identity asserted	Incident lead	Independently supported authorship and relationships	Evidence connects the persona to the specific event

An organisation can confirm a service problem while the actor, cause and alleged data volume remain unresolved. Recovery should therefore record what is restored, what access was removed and which questions remain open. A normal front page alone does not establish the state of the internal service.

Operational communication should state the known boundary and next decision. An availability incident may require an alternative customer channel. A supported disclosure finding may require privacy assessment. A claim without corroboration still deserves a documented disposition, with a trigger for reopening it.

6.5 Keep rhetoric separate from evidence

The report takes no political position from claimant material. Actor slogans and labels are source statements. Language does not establish nationality, and a political theme does not establish state direction or coordination between personas.

The useful defensive question is which service or data proposition can be tested. That keeps attention on continuity, account control and privacy evidence. It also avoids treating repeated claims, relay posts or a denial as an independent count of attacks.

KEY TAKEAWAYS

01

The 27–28 relevant posts do not measure confirmed DDoS incidents.

02

A persona statement and an official website alert support different propositions, with no established link.

03

Validate impact, access and authorship separately, then tie recovery communication to the supported boundary.

CHAPTER 07

Threat actors

07

THIS CHAPTER ANSWERS

Which actor propositions are supported, and how should defenders use them without overstating attribution?

87

Malaysian ransomware leak-site listings in the reporting window

7.1 How to read relationships 52

7.2 Technical evidence without an actor attribution 53

7.3 Hacktivist claims require availability and access evidence 54

7.4 Ransomware and extortion 54

7.5 Criminal personas and data propositions 56

CHAPTER 07

Threat actors

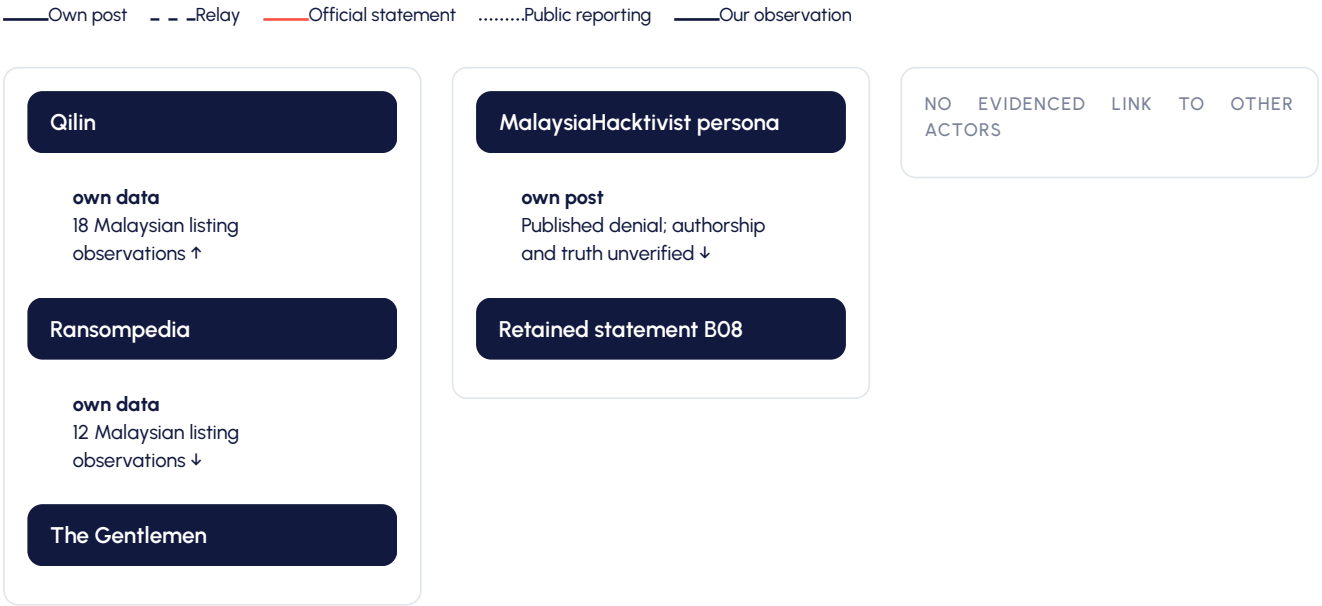
IN SHORT

Ransompedia records 87 Malaysian listings dated 1 January–22 November 2026. Qilin and The Gentlemen account for 30 of them. Those are extortion publications, not confirmed intrusions or a count of unique affected people. Technical alerts and official incident statements answer different questions. Use actor information to guide validation and recovery planning, while keeping identity, cause and impact tied to their own evidence.

7.1 How to read relationships

The relationship map shows Ransompedia listing-source associations with Qilin and The Gentlemen, and the persona's published statement B08. These relationships establish listing labels and publication, without confirming an intrusion, authorship or the statement's truth.

The same discipline applies to ransomware. Ransompedia is Brandefense's own data source for listing observations. Its connection to an actor in the map means that the source holds publications under that name. It does not establish an organisation's confirmation of the claim or an actor's exclusive control of an incident. [S4]



Any wider grouping without a concrete supporting relationship is an analytical model. This report does not infer a common operator from a shared country reference, a similar political theme or two advertisements with the same fields. A defender should not join separate investigation queues solely because the actor labels resemble each other.

7.2 Technical evidence without an actor attribution

CASE E

E

A content-management extension alert requires patch and eradication evidence

Official technical alert

Public-facing websites

OFFICIAL ACCOUNT	NC4's late-June alert described attacks involving the JCE extension for Joomla. The CVE record describes CVE-2026-48907 as allowing unauthenticated editor-profile creation that can lead to PHP upload and code execution. [S18][S34]
VERSION SCOPE	The CVE record lists JCE 1.0.0–2.9.99[.]4 as affected. The first patched release is 2.9.99[.]5. Install the latest compatible vendor release, 2.9.99[.]9 or later; the advisory provides an interim patch for older installations. Updating does not clean an already affected site. [S34][S19]
WHAT WE CAN ESTABLISH	The sources support a vulnerability and reported attacks involving it. They do not establish which actor was responsible for every website incident reported in the period.
ALTERNATIVES	A website can be altered through another vulnerable component, a stolen administrator account or a hosting problem. An outwardly similar page does not settle the entry route.
LIMITS	This report has no forensic record for an individual affected installation. It does not publish a victim domain or claim that every June defacement used this flaw.
RESPONSE	The web owner should prove the installed extension is fixed and separately investigate unauthorised profiles and files. Where necessary, restore a trusted state and validate the administrator accounts before reopening the service.

Bottom line

Prove the fixed extension state and separately establish whether unauthorised access remains.

The important distinction is between preventing a new entry and removing access already established. An update can answer the first question while leaving the second unresolved. The completion evidence should therefore include the installed version, the investigation result and the business owner's approval to return the service to normal operation.

The incident lead should also preserve the time boundary. A later clean scan or normal front page is an observation at that later time. It does not establish that the site contained no unauthorised files during the earlier period. The report recommends retaining relevant logs and documenting that uncertainty.

No state or criminal actor identity follows from the vulnerability alone. The source's technical explanation is useful without adding an unsupported geopolitical account. The same rule applies to remote-management tools in the June messaging-script warning: a tool's presence does not establish who used it. [S11]

7.3 Hacktivist claims require availability and access evidence

A claimant can name a public website, show a screenshot or point to an availability check. Those materials should be recorded as the evidence they are. They do not, on their own, establish how long a service was unavailable, whether customers were affected or whether internal access existed.

For an organisation named in a claim, the first validation should match the proposition. An availability claim calls for service monitoring and upstream traffic records. A claim about internal files calls for a scoped access review. A claim about a privileged account requires account and session checks. The response should escalate when corroborating evidence supports it.

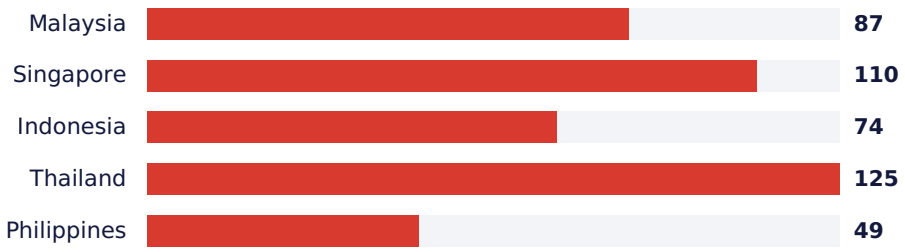
The health-sector support-platform account and the separate bank website account illustrate why broad actor narratives can mislead. Their official explanations describe different boundaries. This report does not substitute an actor's broader description for either account. [S7][S8]

Attribution should remain attached to its source. Language, country references and actor slogans are not evidence of nationality or state direction. This report does not repeat loaded framing or draw conclusions about public policy from claimant statements.

7.4 Ransomware and extortion

Ransompedia records 87 Malaysian listings in the reporting window. The largest counts are Qilin with 18 and The Gentlemen with 12. Together they account for 30 of 87 listings, or 34.5%. The remaining 57 listings appear under other group names. [S4]

Malaysia has 87 listings in the same window as four regional peers



Source: Brandefense Ransompedia, 1 January–22 November 2026; November partial [S4]. Country-labelled publications, not confirmed intrusions or a national security ranking.

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

The regional comparison describes the source's visibility. It does not adjust for population, organisation numbers, disclosure practices or national reporting coverage.

Country	Window listings	Largest listed group	Reading limit
Malaysia	87	Qilin, 18	Publications naming Malaysian organisations
Singapore	110	Qilin, 12	Different economy and disclosure coverage
Indonesia	74	Nova, 9	Country scale differs
Thailand	125	The Gentlemen, 43	Same publication window
Philippines	49	Qilin, 17	Different sector and source composition

The peers were chosen for regional business and supplier relevance. Singapore supplies a neighbouring finance and digital-services comparison. Indonesia adds a larger neighbouring digital economy. Thailand adds manufacturing and tourism context. The Philippines adds services and outsourced-operations context. These are operational comparisons, not a ranking of national security.

The Malaysian monthly counts range from three in September to 18 in October. October accounts for 20.7% of the 87 window listings. November contributes eight through the cut-off and is incomplete. These publication dates do not establish when intrusions began. [S4]

Six retained Malaysian listing records are dated 8–22 November. These are recent publications, not six confirmed new intrusions. [S4]

The source's sector labels place nine listings each in hospitality and logistics, and eight each in consulting and manufacturing. Those labels describe listings and differ from the report's selected-organisation sectors. They should not be joined as though the populations were identical. A broad or uncertain feed label is not reassigned to a more specific sector without evidence.

Qilin

Ransomware and extortion listing brand | Group name attached to Ransompedia listing observations

IN MALAYSIA, 2026

2026
18 Malaysian listings dated 1 January–22 November

CLAIMED TARGETS

Organisations named in leak-site publications; individual identities withheld

SEEN IN PUBLIC REPORTING

[S4] 18 of the 87 Malaysian listings in the reporting window

OUR ASSESSMENT

The listing count is observed; an underlying intrusion, affected-data volume and actor responsibility need their own corroboration. Recovery planning should not depend on a single group name.

CONFIDENCE

High for retained listing count; underlying claims unverified

The Gentlemen

Ransomware and extortion listing brand | Group name attached to Ransompedia listing observations

IN MALAYSIA, 2026

2026

12 Malaysian listings dated 1 January–22 November

CLAIMED TARGETS

Organisations named in leak-site publications; individual identities withheld

SEEN IN PUBLIC REPORTING

[S4] 12 of the 87 Malaysian listings in the reporting window

OUR ASSESSMENT

The listing count is observed; an underlying intrusion, affected-data volume and actor responsibility need their own corroboration. Recovery planning should not depend on a single group name.

CONFIDENCE

High for retained listing count; underlying claims unverified

For recovery planning, the useful proposition is that several extortion brands appear, with no single name covering the entire observed set. Tested backups, containment decisions, supplier dependencies and communication channels should work regardless of which group publishes a claim. A group's absence from the list is not a reason to defer a credible incident investigation.

7.5 Criminal personas and data propositions

A persona, a seller brand, an advertisement and a claimed dataset are distinct entities. One persona can advertise several unrelated products. Several personas can repeat a similar advertisement. Neither observation identifies the original data source, establishes possession or establishes a completed transaction.

The report records the strongest proposition supported by each retained card. The offer may establish an asking price and a field list. A repeated title may establish circulation. A current credential listing can justify a validation queue. None should silently become a verified intrusion in the summary or action plan.

This discipline also prevents misleading actor profiles. Confidence belongs to a proposition, such as a post date or a matched field list. It should not be attached to an entire persona as though every future assertion inherits the same credibility.

KEY TAKEAWAYS

01

Qilin and The Gentlemen account for 30 of 87 observed Malaysian listings, each still a claim.

02

A technical alert can support remediation without establishing an actor.

03

Validate relationships and impact separately, then use recovery plans that do not depend on a group name.

CHAPTER 08

The fraud economy

08

THIS CHAPTER ANSWERS

How do the reported lures turn identity, messaging and payment information into a defender's response queue?

3

response routes: payment, account and endpoint

8.1 Account and payment-control decisions 59
8.2 Payment-card observations: a narrow view 59
8.3 An assistance lure sought payment and identity information 60
8.4 A free-laptop lure sought control of a messaging account 61
8.5 A document lure required an endpoint response 62
8.6 Prices and offers do not measure market revenue 62
8.7 What the campaign evidence supports 62
8.8 Campaign warnings retain their individual limits 63

CHAPTER 08

The fraud economy

IN SHORT

The strongest public campaign evidence concerns messaging lures that ask users to submit data or run a file. The relevant response depends on what was disclosed or launched. Identity and payment details, messaging login codes and a Windows script create different investigation paths. Establish a short intake record, route it to the right owner and validate the affected account, card or device.

8.1 Account and payment-control decisions

A fraud report should begin with the requested action and the action actually taken. An offer to perform paid tasks differs from a request for an account login code. A payment made to a new recipient differs from a card number entered into a form. Grouping them as a single category can hide the control that needs attention.

A report of a task or job offer should identify the point at which the recipient was asked to send money. An initial small payment or completed task should not replace verification of a later request. The report recommends recording the payment instruction and the user's actual response.

For a bank or employer, the useful intervention point is the transition from a small task to a payment request. The report recommends a clear escalation route for staff or customers who are asked to fund a task. The case should preserve the payment destination and timing through normal incident channels without republishing personal details.

An organisation should also distinguish a fraudster's claimed access from the use of information obtained elsewhere. A message containing a real name or an account detail can be convincing. It does not establish that the sender can access the organisation's system. Customer-service staff need a procedure that avoids confirming further sensitive details to the caller.

8.2 Payment-card observations: a narrow view

SCOPE OF THE CARD FIGURES

Payment-card figures have limited coverage. They do not estimate national card theft, card usability or fraud loss in Malaysia.

The payment-card aggregates contain 1,244 distinct Malaysian-attributed cards across 1,534 occurrences. They span 1,256 source records, 190 distinct issuer-identification ranges and 13 named issuers. The issuer-bank subset in Chapter 9 contains 945 of those cards. These are different denominators, never additional national totals. [S13]

Card material is one narrow view of a wider fraud problem. An observed card record does not establish that a transaction succeeded, that the card remains usable or that the issuing bank was the source. The issuer response should be based on validation and its own transaction evidence.

The relevant operational question is what a cardholder entered and whether related activity appears in the issuer's records. A report about a suspicious page should not be turned into a bulk card-reissue instruction without that assessment. The response must preserve the distinction between exposure, attempted use and confirmed loss.

8.3 An assistance lure sought payment and identity information

CASE I

An aid-themed phishing portal

Public-service impersonation

MyCERT campaign advisory

OFFICIAL ACCOUNT	MyCERT's 11 November advisory described an assistance-themed lure distributed through SMS and WhatsApp. The advisory said the portal collected identity, payment-card and one-time-password information. MyCERT recorded verification on 26 October. [S9]
WHAT WE CAN ESTABLISH	The source supports the lure and its collection fields. It does not provide a total of actual victims, confirmed payments or fraud loss.
ALTERNATIVES	A recipient can encounter the page without submitting anything. A person who entered identity details needs a different response from someone who also supplied card information or an authentication code.
LIMITS	Impersonation of a public programme does not establish access to that programme's systems. The report does not repeat an entitlement claim as a fact about a real benefit.
RESPONSE	Ask the user what was entered. Route card details to the issuer, account credentials or codes to the relevant account owner, and suspected device activity to endpoint investigation.

Bottom line

Identify the information submitted and route payment, account and device decisions separately.

The intake process should be short enough for a help desk or call centre to use. It should identify the communication channel, the time, the page visited, the information submitted and any subsequent transaction or sign-in. This is a proposed response record, not a claim about how the campaign's victims behaved.

Where an authentication code was submitted, the account owner should examine active sessions and recent changes. Where payment information was submitted, the issuer should assess attempted transactions through its established process. These actions can proceed in parallel if the user supplied both.

8.4 A free-laptop lure sought control of a messaging account

CASE J

J

A fake eligibility check requested login codes

Messaging accounts

MyCERT campaign advisory

OFFICIAL ACCOUNT	MyCERT's 20 November advisory described a free-laptop poster leading to a false eligibility check. It said the page sought personal information, a messaging-account login code and a two-step password. MyCERT recorded renewed verification on 13 November. [S10]
WHAT WE CAN ESTABLISH	The advisory supports an active phishing mechanism at the stated dates. It does not establish that every recipient lost an account or that an employer's systems were accessed.
ALTERNATIVES	A user might have submitted personal information without a login code, or a code without completing a later step. The response should establish the actual sequence.
LIMITS	Similar lures do not establish a common operator. Any source assessment about earlier waves should retain its own confidence rather than becoming an identity claim.
RESPONSE	Review and terminate unauthorised sessions, restore a unique two-step password and check messages sent onward. If a workplace device was involved, investigate it according to the evidence of execution or access.

Bottom line

Review sessions and onward messages without inferring an employer-system incident.

The important difference from Case I is the asset the page sought. A messaging account can carry conversations and trusted relationships, even when no payment-card field is present. The report recommends checking onward messages because the account owner needs to know what actions occurred after the suspected access.

Organisations should give staff a way to report this quickly. A person concerned about a personal messaging account may not recognise the relevance to a work device or business conversation. The help desk should ask factual questions without assuming that the organisation itself suffered a data incident.

8.5 A document lure required an endpoint response

MyCERT's 22 June advisory described Windows VBScript delivered through WhatsApp Desktop or Web. The advisory said execution installed an attacker-controlled remote-management agent. That sequence differs from the November browser-form lures. The first technical question is whether a script or installer ran. [S11]

Endpoint teams should preserve the relevant process and installation evidence. They should examine unexpected scripting activity and remote-management software in the context of the user's report. The report does not recommend treating every legitimate remote-management installation as malicious.

If execution is not established, the incident record should say so. If it is established, the investigation should determine account use and subsequent actions before the case is closed. This is a conditional response to the advisory's mechanism, not a finding that a particular employee device was infected.

8.6 Prices and offers do not measure market revenue

An asking price describes what a poster requested. It does not establish the price paid, the number of buyers, the quality of the advertised material or the seller's revenue. A repeated offer is therefore evidence of advertising activity rather than a completed sale.

The same limit applies to a bundle that includes several countries or institutions. A Malaysian reference can be one part of a broader product. The report does not treat that reference as exclusive targeting or assign the entire advertised bundle to Malaysia.

For a fraud team, the field list can be more useful than the asking price. It suggests which verification questions could be answered by someone holding the claimed information. The proportionate action is to test the relevant process with synthetic data and remove unnecessary reliance on static personal facts.

8.7 What the campaign evidence supports

The public advisories support three response routes. Payment data goes to issuer assessment. Account credentials and codes go to account and session validation. File execution goes to endpoint investigation. Some reports will require more than one route.

User action	Lead owner	First validation	Completion evidence
Received a lure only	Help desk or customer support	Establish whether any page, file or form was used	Intake record and appropriate warning
Submitted identity details	Privacy and fraud teams	Identify fields and affected verification processes	Documented risk and communication decision
Submitted card information	Card issuer	Review card status and related transaction attempts	Issuer disposition under its response process
Submitted an account code or password	Identity or account owner	Review sessions, sign-ins and account changes	Sessions resolved and access restored securely
Ran a file or installer	Endpoint response	Confirm process and installation activity	Scoped investigation and containment decision

These routes make the evidence actionable without claiming that every reported lure caused harm. They also provide a common language for security, fraud and customer-support teams. The case remains open until the owner has recorded what was validated and what action followed.

8.8 Campaign warnings retain their individual limits

Official campaign notices describe different routes from a persuasive message to a payment or account action. They do not support one combined national loss figure. The table preserves each warning's mechanism and reading limit.

Published	Authority	Mechanism described	Defender decision
February	PDRM	Shopping, delivery and donation-themed lures	Examine the requested payment or information rather than the emotional story
August	BNM	A resurfaced deepfake investment endorsement	Verify the claim through the authority's own published channels
October	BNM and the Securities Commission	False investment endorsements	Check the relevant authorisation rather than trusting a video
November	MyCERT	False traffic-summons pages seeking card and authentication information	Route submitted payment and code details to the relevant owners

The notices are attributed to their issuers. They describe warnings and mechanisms, not a measured population of actual victims. The August and October endorsement warnings do not establish one common operation. [S35] [S36][S37][S38]

MyCERT's traffic-summons advisory was published on 6 November and described observations on 28–30 October. It supports a phishing page and requested information. It does not establish actual transactions, victim losses or continued activity at the report's cut-off. The response should establish what the person entered before assigning an account or payment action. [S38]

A further MyCERT advisory published on 22 November described a false cash-assistance registration page seeking messaging login codes and a two-step password. The claimed payment amount was part of the lure. The advisory did not establish a victim or loss total. Similarity to the laptop lure is not evidence of a common operator. [S39]

For organisations, the common action is to verify the requested transaction or access change through a trusted route. That principle can be tested with synthetic investment, job, shopping and assistance scenarios. The test should record whether the person or process stopped when money, credentials or a code was requested.

KEY TAKEAWAYS

01

Assistance, laptop and document lures create different asset risks.

02

Card observations and asking prices do not measure successful fraud or criminal revenue.

03

Record the user's actual actions, then close the payment, account and endpoint routes with evidence.

CHAPTER 09

Banking and finance deep dive

THIS CHAPTER ANSWERS

Which identity, customer and supplier decisions can financial organisations make from the evidence in this report?

35

banking and finance entries in the selected portfolio

9.1 Define the financial population before interpreting it 66
9.2 A corporate website and a banking service can have different states 67
9.3 Trading restrictions require an authenticated alternative 67
9.4 Credit reporting creates an external decision dependency 68
9.5 Separate the fraud response by information submitted 68
9.6 Android lures require device and account investigation together 69
9.7 Regulatory readiness needs the right activity boundary 69

CHAPTER 09

Banking and finance deep dive

IN SHORT

The financial portfolio contains 35 selected entries, including institutions and services beyond licensed banks and card issuers. Public cases describe separate website, trading and credit-reporting boundaries. Fraud advisories describe information and authentication requests, without establishing bank-system access. Keep those populations distinct, validate current identity evidence first and test the customer and supplier processes that depend on the affected service.

9.1 Define the financial population before interpreting it

The 35 entries are a selected financial-services portfolio. They include banking, investment, development, fund and market-infrastructure activities. They are not 35 independent licensed banks or 35 card issuers. The report does not infer an issuer denominator from this wider set. [S2]

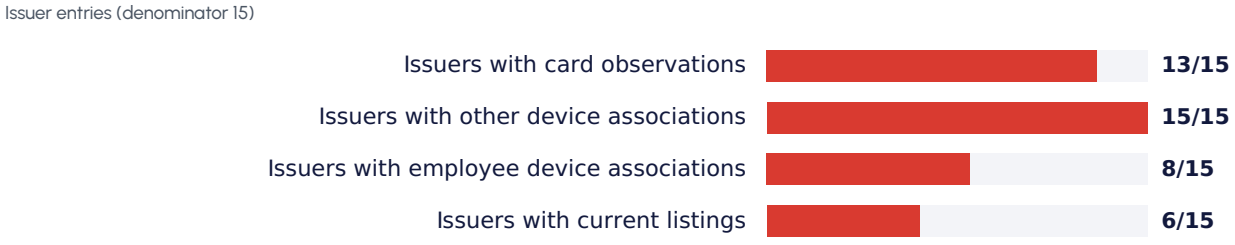
That distinction matters whenever a card figure is presented. A card attributed to an issuer describes a payment-card observation within the narrow scope in §8.2. It does not show that the issuer's systems were the source. A current account listing is another population again.

All 35 selected financial entries have usable exposure results. Nine had a credential listed for sale when checked. Thirty have device associations and historical credential records, while 23 have employee-classified device associations. These observations describe the financial portfolio, without a sector rating. [S1]

The portfolio has 55,933 recorded device associations, including 782 employee-classified associations, and 472,196 historical credential-record associations. Device ownership and current account validity remain unverified. The 1,250 document associations are not established as confidential files.

The issuer subset covers 15 card-issuing bank entries within that wider financial portfolio. Thirteen have card observations, totalling 945 distinct cards within the narrow scope in §8.2. Six had a current credential listing. An issuer association does not establish access to the bank's infrastructure. [S13][S1]

Issuer observations retain distinct card and device populations



Separate observation populations



The top three issuer card counts account for 67.4% of 945 cards; not fraud loss. Source: issuer observations [S13][S1]. 15 issuers within 35 financial entries. Card, credential and device populations are separate; issuer association does not establish access to bank infrastructure.

Those 15 issuer entries have 308 employee-classified device associations and a further 14,291 device associations not classified as employee devices. The latter are not established as customer-owned. The three largest issuer card counts represent 67.4% of the 945 cards. Concentration describes observations, not fraud loss or bank security.

Passive observations cover 33 of the 35 selected financial entries. Published DMARC policies include 12 rejection, 11 quarantine and four monitoring results; no policy was observed for six. Two entries remain without completed observations. TLS was valid for 32 observed entries and invalid for one. [S12]

Of the 33 observed entries, 23 homepages answered; HSTS was observed on all 23 answering pages. This is a configuration observation, not evidence that every financial application is protected. Keep the homepage denominator separate from the 35-entry portfolio.

9.2 A corporate website and a banking service can have different states

November reporting quoted a financial institution's statement that its corporate-website issue did not affect banking services, deposits or customer information. The report retains that stated boundary and date. It does not use the visible website change as evidence of access to core systems. [S8]

For a financial organisation, the response should maintain separate records for the public site, customer authentication, transaction processing and data. Each record needs a responsible owner and a current evidence source. A change in one row should trigger the relevant investigation without silently changing every other row.

The communication process should follow the same structure. A statement that transactions remain available does not answer every question about website integrity. A statement that a public site was restored does not establish the outcome of a separate data investigation. Precise boundaries make later updates easier to understand.

9.3 Trading restrictions require an authenticated alternative

The October broker account described restrictions following a detected attempt, with some channels remaining available. Its response did not establish data loss at the time of reporting. This supports a continuity exercise focused on the actual affected order route. [S28]

The business owner should define which instructions can be handled manually, how the customer is authenticated and how the instruction is reconciled after normal service returns. Security should validate the restored channel before the owner accepts it. The exercise should preserve the distinction between a precautionary restriction and a confirmed unauthorised transaction.

March reporting of incidents in specific broker components supplies a second boundary example. The market operator said broader market integrity remained intact. A component-level incident should therefore not be rewritten as an exchange-wide incident. [S27]

The report does not assume that the March and October events share a supplier, entry route or actor. Their similarity is operational: each requires a clear description of the channel involved. Any stronger relationship would need additional evidence.

9.4 Credit reporting creates an external decision dependency

The credit-provider case in Chapter 5 concerns one environment and some interrupted reporting services. A financial customer may need a fallback while the provider determines the full data scope. That does not establish access to the financial customer's own systems. [S6]

Credit and fraud teams should agree how to record decisions made with an alternate source or delayed report. They should identify applications requiring later review and how customers will be informed where appropriate. The completion evidence should include reconciliation after the provider restores service.

Supplier-risk teams should also retain the distinction between interruption and data access. The contact responsible for service status may differ from the person responsible for the privacy assessment. Both should reach the organisation's incident lead through an established route.

9.5 Separate the fraud response by information submitted

The MyCERT assistance and laptop advisories describe payment and messaging-account information as different objectives. A customer's report should establish which fields and codes were submitted. It should not be reduced to the fact that the customer saw a suspicious message. [S9][S10]

For payment-card information, the issuer should use its established validation and transaction-review process. For a messaging login code or password, the account owner should review sessions and changes. If a file ran on a device, endpoint response should assess that activity. The routes can overlap without becoming one undifferentiated incident.

Financial organisations should test account recovery and payment-change procedures with synthetic personal data. The purpose is to discover whether knowledge of a real name, phone number or other static detail can replace the intended verification. A convincing message should not be allowed to determine the verification route.

9.6 Android lures require device and account investigation together

MyCERT's June and October advisories described Android lures involving sideloaded applications. The reported behaviours included Accessibility abuse, bank-login overlays, code capture and device control. The October advisory related its variants to the June campaign. That source relationship should not become a count of separate national incidents. [S40][S41]

The relevant intake question is whether an application was installed and which permissions were granted. Receiving a parcel, job or utility-themed message differs from installing its application. An account action can also require investigation even before a financial loss is established.

The report recommends joint handling by the account owner, fraud team and endpoint response. Account teams should examine relevant sign-ins and payment changes. Device teams should assess the installation and permissions. The case should retain the link between those decisions without assuming that every reported lure produced device control.

A reset alone should not close a device question. Conversely, a device investigation should not leave a relevant account session unexamined. Completion evidence should state which app and account propositions were validated, what action followed and which uncertainty remains.

9.7 Regulatory readiness needs the right activity boundary

Chapter 10 distinguishes the personal-data framework, NCII obligations and the March 2027 payment-services policy. The same financial group can contain different activities with different applicability. The report does not assign one deadline to all 35 portfolio entries. [S42][S43][S44]

Legal and compliance should identify the relevant entity and processing activity in advance. Technology and business owners should provide the facts needed for a timely notification assessment. Supplier terms should support the required information flow.

The April enforcement example concerns a 2024 incident. Its 2026 announcement belongs in governance context, not the year's intrusion tally. It should prompt a question about sustained control evidence without being joined to an unrelated later claim. [S45]

KEY TAKEAWAYS

01

The financial sample is broader than licensed banks or card issuers.

02

Validate website, trading, credit-reporting and account propositions within their own boundaries.

03

Run identity checks, customer-fraud controls and supplier-continuity work with distinct owners and completion evidence.

CHAPTER 10

Regulatory and national response

10

THIS CHAPTER ANSWERS

Which obligations apply to which organisation, and which clock should the incident lead record first?

3

applicability questions before a notification decision

10.1 Decide applicability before borrowing a deadline 71
10.2 NCII duties begin with designation and knowledge 72
10.3 Personal-data duties require an event and harm assessment 72
10.4 Data-protection officer readiness is a management task 73
10.5 A 2026 policy can require 2027 preparation 73
10.6 Enforcement dates are not intrusion dates 74
10.7 What CISOs should do now 74

CHAPTER 10

Regulatory and national response

IN SHORT

Malaysia's cyber and personal-data duties have different scopes. Designated critical-information-infrastructure entities have specific incident obligations. Personal-data notification depends on the applicable activity, event and harm assessment. A March payment-services technology policy takes effect in March 2027. Map your entity and processing activities to the relevant rules, record the first known facts and run the notification decision alongside technical investigation.

10.1 Decide applicability before borrowing a deadline

The Cyber Security Act 2024 assigns specified duties to designated NCII entities. NCII means computer systems within the Act's essential-function and detrimental-impact definition. A company's industry alone does not establish designation. The incident duty concerns relevant NCII the entity owns or operates. [S43]

The Personal Data Protection Act has a different scope. The official applicability guidance covers processing connected with commercial transactions, subject to the Act's territorial provisions. It excludes Federal and State Governments. Credit-reporting business conducted under the Credit Reporting Agencies Act 2010 is also outside its application. [S42]

These boundaries matter in this report. The selected-organisation population includes public bodies, companies and financial services with different activities. It is not a list of entities to which one notification deadline can be assigned. An incident lead should record the entity, activity and data involved before applying a clock.

The table identifies duties and dates from the cited official texts. It is an operational guide to the relevant questions, not legal advice.

Rule	Applicability	Trigger and timing	Required preparation
Cyber Security Act 2024	Designated NCII entity and its owned or operated NCII	Notify the Chief Executive and relevant sector lead when the statutory incident duty applies	Retain designation, sector and contact records
NCII incident regulations	Incident that has or might have occurred, when known within the regulated scope	Immediate notification; particulars within 6 hours; additional information within 14 days, as specified	Maintain the required channel and a documented fallback
Personal-data breach duties	Processing and entities within the Act's application	Statutory notification as soon as practicable; Commissioner guidance supplies the assessment and reporting framework	Record awareness, facts, harm assessment and notification decision

Rule	Applicability	Trigger and timing	Required preparation
Data-protection officer duties	Controllers and processors meeting appointment conditions	Appointment and registration obligations under the applicable guidance	Record the appointment, contact details and accountable management
Payment-services technology policy	Defined non-bank payment-services regulatees, with specified treatment and exceptions	Issued 12 March 2026; effective 12 March 2027	Complete an applicability and readiness assessment before the effective date

The table draws on the Act, its notification regulations, the amendment and Commissioner guidelines, and BNM's policy. Their scopes should not be combined into a universal rule. [S43][S46][S47][S48][S49][S44]

10.2 NCII duties begin with designation and knowledge

The notification regulations require immediate electronic notification when a qualifying incident is known. They require specified particulars within six hours of knowledge, and further information, to the extent practicable, within 14 days after notification. Updates can also be required. The stated channel is the NC4 System, with specified fallback communications during disruption. [S46]

A qualifying report is therefore not something to postpone until every forensic question is resolved. The response team should distinguish an initial notification from the later supporting information. It should preserve the facts available at each stage and the time at which the responsible people knew them.

For an organisation unsure of its designation or service boundary, the first action is to resolve that status with its legal and sector contacts. The report does not assign NCII status to any sampled organisation. It also does not treat every unverified advertisement as an incident within the statute's scope.

The governance record should connect the regulated infrastructure to the incident plan. It needs the service owner, incident lead, relevant sector contact, reporting channel and fallback. A generic list of regulators is not enough if the team cannot determine who must receive the initial report.

10.3 Personal-data duties require an event and harm assessment

The 2024 amendment introduced data-protection officer and breach-notification provisions. Those provisions took effect on 1 June 2025. The amendment also extends Security Principle obligations to processors. Appointing an officer does not remove the controller's or processor's accountability. [S47][S50]

The Commissioner guideline states 72 hours from occurrence in §6.1. Its §6.2 examples explain the clock through knowledge or confirmation in different circumstances. Its Commissioner-notification assessment includes harm criteria and a scale condition exceeding 1,000 affected people. The examples do not justify waiting for complete forensic certainty. Affected-person notification follows its own significant-harm test and timing. [S48]

The guideline specifies notification to affected people without unnecessary delay and no later than seven days after the initial Commissioner notice, where the duty applies. Scale alone is not the test for that communication. The incident team should keep the Commissioner decision and the affected-person decision as separate entries. [S48]

The response record should therefore begin with the first report and known facts. It should identify the processing activity, categories of information, possible harm and assessment owner. Later evidence can update the record. A decision to notify, not notify or seek further facts needs a documented basis and review time.

Supplier terms should support this process. The customer needs information quickly enough to assess its own duties. A provider's statement that an investigation continues does not remove the need for an initial assessment. Equally, a customer's contract does not establish that every reported provider incident falls within the same personal-data rule.

10.4 Data-protection officer readiness is a management task

The DPO guideline includes processing information about more than 20,000 people, or sensitive information, including financial information, about more than 10,000 people. Regular systematic monitoring is another condition. The controller registers the appointment and contact details within 21 days of appointment. [S49]

Management should assess the actual processing activities against that guidance. The completion evidence is an applicability decision and, where required, a recorded appointment with clear access to the incident process. A name in an organisation chart does not show that the officer receives the facts needed during an incident.

The officer's role should be exercised before a live notification decision. A tabletop can test whether technical staff can describe what data was involved, whether a supplier can provide timely facts and whether management can approve an initial notice. The purpose is to expose missing information and unclear ownership.

10.5 A 2026 policy can require 2027 preparation

BNM issued its payment-services technology requirements on 12 March 2026, with an effective date of 12 March 2027. The policy applies to defined non-bank payment-services regulatees, with tiered treatment and exceptions. It should not be described as replacing the separate banking technology framework. [S44]

Affected organisations should use the period before the effective date to identify applicable provisions, assign owners and retain completion evidence. The action plan should distinguish work required under an existing duty from readiness for a future effective date. This avoids reporting a planned control as though it were already required by the new policy.

The distinction is particularly relevant to payments and outsourced technology. A provider and a regulated customer can have different obligations. Their incident and service agreements should specify the information each needs without assuming that one organisation's regulatory status transfers to the other.

10.6 Enforcement dates are not intrusion dates

A financial institution's April statement addressed a regulatory penalty and explicitly dated the underlying incident to 2024. This report treats the statement as 2026 regulatory context, not a 2026 intrusion. [S45]

The useful management question is what evidence demonstrates a sustained control improvement. Penalty payment alone is not a technical closure criterion. A board should expect the accountable team to identify the control, the validation performed and the remaining exception, where one exists.

The report does not use this older incident to substantiate a later actor claim or website event. Similar institutional context is not evidence of a shared entry route or continuing access. Each proposition needs its own dated support.

10.7 What CISOs should do now

First, maintain a short applicability record. It should separate NCII designation, personal-data activities and sector-specific requirements. Legal should own the interpretation; the relevant business and system owners should provide the operating facts.

Second, maintain a notification log alongside the technical timeline. Record when information arrived, what it established, who assessed it and which deadline or exception was considered. Distinguish preliminary facts from later confirmation without erasing either.

Third, exercise a supplier incident with incomplete information. Ask the provider for a narrow service and data boundary, then test whether the organisation can make and update its own decision. The exercise should end with a completed record and an identified route for unresolved questions.

KEY TAKEAWAYS

01

NCII, personal-data and payment-services rules have different applicability tests.

02

Record knowledge and assessment promptly; an initial notice and later updates are separate obligations.

03

Treat the March 2027 effective date as readiness work and verify each organisation's duties against the official texts.

CHAPTER 11

Outlook

11

THIS CHAPTER ANSWERS

Which conditional scenarios deserve preparation, and what evidence should change the plan?

5

judgments with an explicit basis and change signal

11.1 Key judgments 76

11.2 What would change the assessment 77

11.3 Conditional scenarios 77

CHAPTER 11

Outlook

IN SHORT

The evidence supports preparation for identity abuse, data claims, supplier disruption, public-website incidents and extortion. It does not establish a national attack probability or a common operator across these populations. The scenarios below are planning assumptions tied to observed mechanisms. Assign an owner to each change signal and revise the response when corroborating evidence arrives.

11.1 Key judgments

Confidence applies to the proposition in each row. It does not predict the chance of an organisation being attacked. A well-supported observation can still leave the underlying actor assertion unverified.

Judgment	Confidence and basis	Boundary	Change signal
Identity and account validation remain a useful first investment	High for observed campaign mechanisms and the need to validate current access	An advertised or historical record need not remain usable	A validated active account or session linked to the organisation
Supplier incidents need joint operational and privacy decisions	High for the reported interruption and access boundaries in the retained cases	No common provider or campaign is inferred	A provider confirms the organisation's service or data within its affected scope
Website claims require independent impact checks	High for the distinction between public content and operational services	An outward change does not establish internal access	Traffic, application or account records corroborate the claimed effect
Extortion readiness should not depend on one actor name	High for 87 listings distributed across several brands	Listings remain claims and do not measure national prevalence	An actor claim matches retained files, system evidence or an official confirmation
Messaging lures require separate payment, account and endpoint routes	High for the MyCERT mechanisms	Advisory activity does not establish actual victim or loss totals	A user report establishes submitted information or file execution

The bases are the retained own-data observations and public cases in Chapters 3–9. The judgments preserve the source boundaries. They do not convert publication volume into the probability of an incident. [S4][S9][S10][S11]

The account-validation judgment is conditional on the organisation receiving relevant evidence. A security lead should first ensure the evidence reaches an accountable team. That team can then determine freshness, ownership and current validity before deciding whether a reset or containment step is justified.

The supplier judgment is about decision coverage rather than a claim of increasing incidents. The terminal, credit-reporting and technology-services cases show different ways an external environment can matter. They justify testing the relevant dependency without supporting a national trend estimate.

11.2 What would change the assessment

The report recommends a small set of signals that can change the response. Each one should arrive through an established incident channel with an owner and timestamp. A new claim alone should be recorded, but the action depends on what it establishes.

New evidence	What changes	Responsible owner
A listed credential matches an active account and relevant recent activity	Move from exposure validation to a scoped identity investigation	Identity lead and incident response
A supplier confirms access to files or service components used by the organisation	Review the affected dependency, customer impact and notification duty	Supplier owner, privacy lead and operations
Availability monitoring corroborates a disruption claim	Activate the tested service and mitigation plan	Service owner and network operations
Internal records corroborate an advertised file or access route	Preserve evidence and contain the supported boundary	Incident response and data owner
A user confirms a code submission or file execution	Follow the relevant account or endpoint route	Help desk, identity and endpoint response
An official text changes the entity's applicable duty or effective date	Update the plan, contact route and completion target	Legal and compliance

Some findings can also narrow the response. A historical account that was disabled before the advertisement does not justify the same action as a current privileged account. A provider's supported exclusion of the organisation's environment can reduce the relevant scope. The record should preserve why the decision changed.

The absence of corroboration is not proof that a claim is false. It can mean the available evidence does not settle it. The incident lead should set a review date and identify what additional evidence would be material, rather than leaving an unowned investigation open indefinitely.

11.3 Conditional scenarios

Scenario 1: an identity offer becomes a current-access incident. A post or exposure alert names an organisational domain. The identity team validates an active account and finds activity requiring investigation. The planning assumption is that the team can obtain the relevant logs and contact the account owner promptly. The exercise should test that dependency.

The first decision is whether the evidence supports session revocation, account restriction or device containment. The completion evidence should record the account's status, related activity and action taken. A bulk reset without this reasoning can leave the underlying device or session question unresolved.

Scenario 2: a supplier service stops while data scope is uncertain. Operations needs a fallback before the provider completes its investigation. Privacy and legal need enough facts to assess duties. The planning assumption is that the contract and contact route support an early, narrow statement followed by updates.

The exercise should test a real business process, such as a credit decision or a logistics transaction. It should end with a reconciled queue and a documented return-to-service decision. No scenario assumption should be presented as evidence that a supplier actually failed to provide timely information.

Scenario 3: a public website changes and an actor claims wider access. The service owner sees a visible issue while social media carries a larger claim. The planning assumption is that status monitoring can distinguish the website from authentication, transactions and core systems.

Communications should publish only the supported boundary and update it as evidence changes. Security should test the technical claim separately. A restored front page should not close an internal-access question that has not been investigated.

Scenario 4: an assistance lure reaches staff and customers together. Some users submit personal information; others provide authentication codes or run a file. The planning assumption is that the help desk can route these reports without forcing them into one incident type.

The exercise should test payment, account and endpoint handoffs. It should also test whether staff understand that a personal messaging-account problem can be relevant to a work device or business conversation. The outcome should be a completed disposition for each route.

These scenarios are not forecasts of timing or loss. They are exercises derived from the evidence types in this report. The board should ask whether the organisation can detect the change signal, make the decision and demonstrate closure.

KEY TAKEAWAYS

01

Plan around validated access, service dependencies and user actions rather than raw claim volume.

02

Give each change signal an owner and a documented response threshold in the organisation's own plan.

03

Reassess when new evidence changes the boundary, and retain the reason for each decision.

CHAPTER 12

Action plan

12

THIS CHAPTER ANSWERS

Who should do what in the next 90 days, and which evidence should the board receive?

20

actions with an owner and completion evidence

12.1 30/60/90 days 80
12.2 Evidence the board can use 83
12.3 By role 83
12.4 How Brandefense can help 84

CHAPTER 12

Action plan

IN SHORT

Begin by making relevant exposure and incident evidence available to named owners. Validate current identity signals, define supplier and service boundaries, and map applicable notification duties. Then improve the controls and fallback processes tied to the observed mechanisms. Finish with timed exercises and a board record that covers every action. Use the evidence column to distinguish completed work from a planned change.

12.1 30/60/90 days

The lanes are relative to adoption of this plan, not a claim about an organisation's existing maturity. An action applies when its stated condition is present. The owner should record a justified alternative where a control or service is outside scope.

1Days 1–30

Establish a route for current credential, device and relevant external-incident alerts for the organisation's domains

ACCOUNTABLE OWNER

CISO and threat-intelligence lead

COMPLETION EVIDENCE

Named recipients, tested delivery and an owned triage queue

Validate every current credential listing received; prioritise active privileged, remote and staff accounts

ACCOUNTABLE OWNER

Identity lead

COMPLETION EVIDENCE

Account status, activity review and a disposition for every item

Investigate employee-associated device evidence where it relates to current accounts or sessions

ACCOUNTABLE OWNER

Endpoint and identity leads

COMPLETION EVIDENCE

Ownership, relevant dates and account/device action recorded

Identify critical suppliers that process relevant data or support essential transactions

ACCOUNTABLE OWNER

Supplier-risk and business owners

COMPLETION EVIDENCE

Service/data map with contact, notice terms and fallback

Verify applicability of NCII, personal-data and sector rules

ACCOUNTABLE OWNER

Legal and compliance

COMPLETION EVIDENCE

Approved applicability matrix and tested notification contacts

Check Joomla installations for the JCE version scope in Case E; investigate affected systems separately from patching

ACCOUNTABLE OWNER

Web and infrastructure owners

COMPLETION EVIDENCE

Fixed-version evidence plus a scoped eradication assessment

Establish a fraud-report intake covering page visits, submitted fields, codes and file execution

ACCOUNTABLE OWNER

Fraud and customer-support leads

COMPLETION EVIDENCE

Tested routing to payment, account and endpoint owners

Prepare a service-status matrix separating public websites, authentication, transactions and core systems

ACCOUNTABLE OWNER

Incident lead and communications

COMPLETION EVIDENCE

Owners, monitoring sources and approved statement templates

2Days 31–60

Introduce or expand phishing-resistant authentication for privileged and remote access where supported

ACCOUNTABLE OWNER

Identity and platform owners

COMPLETION EVIDENCE

Adoption report, tested recovery and dated exceptions

Review published mail-domain policies and move suitable domains toward validated rejection or quarantine

ACCOUNTABLE OWNER

Messaging owner

COMPLETION EVIDENCE

Policy validation, legitimate-sender checks and exception plan

Review external file sharing on support and collaboration platforms

ACCOUNTABLE OWNER

Data and platform owners

COMPLETION EVIDENCE

Access review, expired-link handling and approved exceptions

Test payment-change and customer-recovery processes using synthetic personal information

ACCOUNTABLE OWNER

Fraud, finance and service owners

COMPLETION EVIDENCE

Recorded tests and remediation of weak verification steps

Test manual processing for a critical trading, credit or logistics dependency

ACCOUNTABLE OWNER
Business-continuity and operations leads

COMPLETION EVIDENCE
Timed fallback, authenticated instructions and reconciliation record

Exercise a supplier incident with incomplete service and data information

ACCOUNTABLE OWNER
Supplier owner, privacy and legal

COMPLETION EVIDENCE
Initial decision, update requests and notification assessment

Assess the March 2027 payment-services policy where applicable

ACCOUNTABLE OWNER
Compliance and technology leadership

COMPLETION EVIDENCE
Provision-by-provision readiness plan with accountable owners

3Days 61–90

Run a timed restore of a critical system from a trusted recovery source

ACCOUNTABLE OWNER
Infrastructure and business owner

COMPLETION EVIDENCE
Restore time, integrity validation and business acceptance

Rehearse a website disruption combined with a wider data-access claim

ACCOUNTABLE OWNER
Incident response, network and communications

COMPLETION EVIDENCE
Separate impact checks, statement decisions and escalation log

Rehearse assistance and messaging-account lures across staff and customer channels

ACCOUNTABLE OWNER
Fraud, help desk and endpoint response

COMPLETION EVIDENCE
Completed payment/account/device dispositions

Resolve or formally accept outstanding DNS, TLS and homepage findings

ACCOUNTABLE OWNER
Infrastructure and service owners

COMPLETION EVIDENCE
Validated remediation or signed, dated exception

Present the full action register and unresolved evidence gaps to the board

ACCOUNTABLE OWNER
CISO and executive risk owner

COMPLETION EVIDENCE
Status and evidence link for all 20 actions

The first lane addresses prerequisites and urgent validation. The second changes controls and tests business boundaries. The third demonstrates recovery and coordination. A later lane should not delay an urgent containment step where current evidence already justifies it.

Each team should retain the difference between a configuration change and its validation. Publishing a mail policy does not establish that every legitimate sender still works. Restoring an application does not establish that manual transactions were reconciled. Closing a listing without checking the account does not answer the current-access question.

12.2 Evidence the board can use

A useful board record reports completion, exceptions and unresolved evidence. It should avoid combining unrelated populations into one risk total. The same incident can generate several work items without becoming several incidents.

Board question	Evidence to request	Reading limit
Are current identity alerts being assessed?	Queue age, active-account dispositions and unresolved ownership	Alert volume is not a breach count
Can critical services continue during a supplier interruption?	Timed fallback and reconciliation tests	A successful tabletop is not a production guarantee
Can the organisation state its impact boundary?	Tested service matrix and communication decisions	A narrow clean service does not clear every platform
Are legal decisions timely and supported?	Applicability, awareness and assessment records	A deadline without scope can be misleading
Have critical controls been validated?	Authentication, mail, sharing and patch evidence	Configuration presence is not universal effectiveness
Can the organisation recover and reconcile?	Restore and transaction-validation results	A running system is not the whole recovery outcome

The record should show all 20 actions, including those judged inapplicable. It should identify who accepted the exception and when it will be revisited. An aggregate completion percentage without that detail can conceal the most consequential unresolved dependency.

Where an action remains open, the board should receive the missing evidence and its consequence. For example, an unknown account owner prevents a final identity disposition. An untested manual order process leaves a service-continuity assumption unresolved. These are concrete decision gaps rather than general warnings.

12.3 By role

CISO and security leadership. Establish the evidence route and make the triage queue accountable. Connect identity, endpoint, supplier and privacy decisions rather than treating them as separate reporting exercises. Escalate a current validated exposure according to the organisation's incident plan.

SOC and threat intelligence. Preserve the proposition supported by each post or alert. Distinguish an original assertion, a relay and corroborating service evidence. Do not turn a country tag, shared alias or file advertisement into a verified intrusion.

Identity and endpoint teams. Validate current account status and relevant device activity together. A password change can leave a device or session question open. Record which asset was assessed and what evidence supports closure.

Fraud and customer protection. Ask what the person submitted or launched. Route payment data, account codes and file execution to the appropriate owner. Use synthetic cases to test whether static personal details can override a secure verification process.

Business and supplier owners. Identify which transactions and datasets depend on each critical provider. Test the fallback and the return to normal processing. Preserve the reconciliation record so a service restart does not hide unresolved exceptions.

Legal, privacy and communications. Use the same dated facts as the technical team. Apply the relevant entity and activity scope, retain the notification decision and state only the supported service or data boundary. Update the record when new evidence changes it.

12.4 How Brandefense can help

This report uses Brandefense observations to support underground-claim assessment and ransomware-listing context. Relevant exposure evidence should inform an organisation's decisions alongside its own logs and service records. The useful next step is a workflow that connects external evidence to an accountable internal owner.

For an organisation using external monitoring, the first practical step is to define its domains, recipients and validation owners. The useful output is an actionable queue with a documented disposition. A monitoring result does not replace the organisation's account checks, forensic investigation or legal assessment.

Discuss the evidence and decision workflow with Brandefense: https://brandefense.io/request-a-demo/

KEY TAKEAWAYS

01

Establish monitoring ownership and validate current signals before treating them as completed incidents.

02

Test service, supplier and fraud controls with the business owners who must use them.

03

Give the board evidence and exceptions for all 20 actions by day 90.

APPENDICES

Appendices

A–D

THIS CHAPTER ANSWERS

Which populations and limits should remain beside every conclusion?

5

distinct evidence populations, never added into a national incident total

Appendix A. Scope and evidence 86
Appendix B. Evidence register 89
Appendix C. Sources 90
Appendix D. Glossary 93

Appendix A. Scope and evidence

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

A.1 Window and source categories

The reporting window is 1 January–22 November 2026. Post observations are dated by publication, rather than the date they entered a retained source. The recent-activity section covers 8–22 November. Public incident accounts can contain different dates for access, detection, disclosure and restoration; the report keeps those meanings separate.

Own observations come from Brandefense Blackhole, Ransompedia, Atlas and public domain checks for the selected portfolio. Public sources include official advisories and legal texts, organisational statements, news reporting and vendor security guidance. These categories answer different questions. Their counts are not combined into a national incident total.

The five principal populations are posts, leak-site listings, selected-domain entries, public campaign notices and reported incidents. A post can describe several countries. Several notices can concern one incident. A listing can remain unconfirmed. A selected domain is not a random sample of national organisations.

A.2 Underground posts

The source count is 782,224 Malaysian-tagged posts. The retained tagged view contains 25,355 distinct posts, with 8,748–9,196 relevant observations. The difference reflects coverage and relevance boundaries, not an estimate of undisclosed attacks. [S3]

The recent window contains 922 Malaysian-tagged posts, including eight tagged forum posts. A separate forum view contains 14 posts, and the Malay-labelled tagged population contains 15. These populations overlap. They are not added together or described as unique incidents.

A recent advertisement does not establish recent acquisition. Matching titles or field lists do not establish the same file, possession, a sale or a common operator. The report distinguishes the retained post from the underlying assertion.

Post counts describe visibility in the retained source. They do not measure attack frequency, criminal revenue, affected people or successful access. A low count or absent claim does not establish an absence of incidents.

A.3 Selected organisation-domain portfolio

The portfolio contains 250 selected entries across 11 sector cells. It was chosen for descriptive business and public-service relevance. It is not an official top-250 ranking, a census or a random sample. Related groups, brands and local service relationships can overlap. [S2]

One selected primary domain represents each entry. A DNS or homepage response is not conclusive evidence of independent legal ownership. Unknown results remain unknown, with the assessed denominator stated beside each public control result.

A.4 Exposure ratings and associations

Exposure observations checked on 22 November cover 249 of the 250 selected entries; one is unavailable. Of the assessed entries, 55 had a credential listed for sale when checked. The national Atlas headline is 48/100. No sector or group rating is published. [S1]

Device, credential, document and listing counters are cumulative records held at the check, not 2026-only incidents. Lookalike candidates cover 19 October–18 November 2026. Mention observations cover the preceding 365 days ending 22 November 2026. The populations can overlap and cannot be added into a people or incident total.

Where a reader receives relevant exposure evidence for its own organisation, a current listing, a historical credential and a device association require separate validation. They are not unique people or confirmed current access. The recommended response depends on ownership, dates, validity and corroborating activity.

A.5 Public domain observations

The public results concern mail policies, DNS records, TLS and responding homepages at the stated observation date. A published reject or quarantine policy is not a claim of universal enforcement. Non-observation of a signing record does not establish no signing. A delegation record does not establish a fully validated DNSSEC chain. [S12]

Valid, invalid and unresolved TLS outcomes are separate. Homepage-header findings use responding pages as the denominator. The report does not interpret an unanswered request as a confirmed failed control.

A.6 Payment-card observations

Payment-card observations have limited coverage. The figures do not estimate national card theft, card usability, actual use or fraud loss.

Issuer-level observations do not establish that the issuer's systems were the source. They should support the issuer's validation process alongside its own transaction evidence. Payment-card observations are not added to device, account or incident populations.

A.7 Ransomware listings

Ransompedia supplies 87 Malaysian listings dated within the reporting window. The same-window regional comparison covers Singapore, Indonesia, Thailand and the Philippines. Publication dates do not establish intrusion dates, and a listing does not establish the claimant's role or the organisation's confirmation. [S4]

The sector labels in the listing source differ from the report's selected-domain sectors. The populations are not joined as though they were identical. Different national counts can reflect coverage and disclosure differences as well as the underlying activity.

A.8 Public incidents and campaigns

The report uses official incident accounts, campaign advisories, organisational notices and supporting reporting. An acknowledged incident, its alleged volume, its entry route, the actor's identity and its business impact are separate propositions. The report retains each source's attribution and date.

Coverage remains partial. Private incidents and sales can leave no public account. Early-removed posts can be absent. Public statements can leave scope unresolved. An incident's absence from this report is not evidence that it did not occur.

A technical outage is not automatically counted as malicious activity. An enforcement announcement is dated separately from the incident that produced it. A warning about a plausible mechanism is not automatically a confirmed campaign. These boundaries apply equally to summaries, tables and cards.

A.9 Confidence and naming

High confidence describes a supported observation or a clearly sourced proposition. It does not transfer credibility to every statement made by a persona. An interpretation retains its basis and alternative. "Unverified" means not independently established, rather than false or confirmed.

Targets of unverified assertions use labels that can fit several organisations. An organisation is named only when the incident is officially confirmed, widely reported and recorded in the public naming register. Source descriptions and links preserve the same protection. Actor contact details, victim indicators and personal information are not published.

Source attribution does not make an actor's rhetoric the authors' view. The report retains the security-relevant proposition and omits loaded wording. Recommendations describe proposed defender actions; they do not claim that any named or unnamed organisation failed to perform them.

Appendix B. Evidence register

The register links the public post cards to the sections where they appear. A card's "held" statement describes the observation. Its limitation describes what the observation does not establish.

Card	Posted	Venue	Alias	Language	Shown in
B01	2026-01-09	Retained forum advertisement	Seller persona	English	§4.3
B02	2026-05-08	Retained forum advertisement	Seller persona	English	§4.3
B03	2026-08-23	Retained forum advertisement	Seller persona	English	§4.3
B04	2026-09-06	Retained forum advertisement	Seller persona	English	§4.3
B05	2026-11-19	Retained forum advertisement	Seller persona	English	§4.3
B06	2026-02-01	Retained forum advertisement	Seller persona	Russian	§4.3
B07	2026-02-10	Retained forum discussion	Forum participant	English	§4.4
B08	2026-03-09	Retained channel post	MalaysiaHacktiv-ist	Malay	§6.2
B09	2026-03-08	Retained channel post	Seller persona	Chinese	§4.4

A public card ID is a reference within this report, not a link to a criminal channel or a victim asset.

Appendix C. Sources

Brandefense's own observations have no public source address. Each external entry records the date its supporting material was checked. Where an article identifies a withheld target, a press or official issuer citation uses the publisher's root and notes that the article URL is withheld. Other such citations have no public URL.

S1: Brandefense Atlas, Malaysian selected-domain exposure snapshot, 22 November 2026; lookalike observations 19 October–18 November 2026. Verified on 22 November 2026.

S2: Odin by Brandefense, Selected Malaysian organisation population and scope register, 22 November 2026. Verified on 22 November 2026.

S3: Brandefense Blackhole, Malaysian post observations dated 1 January–22 November 2026. Verified on 22 November 2026.

S4: Brandefense Ransompedia, Ransomware leak-site listings for Malaysia, Singapore, Indonesia, Thailand and the Philippines, 1 January–22 November 2026. Verified on 22 November 2026.

S5: The Loadstar, Container-terminal incident and phased restoration, September 2026. https://theloadstar.com/ (article URL withheld). Verified on 23 November 2026.

S6: Bernama, Credit-reporting provider disclosure, September 2026. https://www.bernama.com/ (article URL withheld). Verified on 22 November 2026.

S7: Bernama, quoting the official statement, Health-sector support-platform incident account, 14 November 2026. https://www.bernama.com/ (article URL withheld). Verified on 22 November 2026.

S8: Malay Mail, quoting the institution, Corporate-website disruption and stated service boundary, 7 November 2026. https://www.malaymail.com/ (article URL withheld). Verified on 22 November 2026.

S9: MyCERT, MA-1501.112026: assistance-themed phishing, 11 November 2026. https://www.mycert.org.my/portal/advisory?id=MA-1501.112026. Verified on 22 November 2026.

S10: MyCERT, MA-1511.112026: free-laptop messaging-account phishing, 20 November 2026. https://mycert.org.my/portal/details?id=8b8bb3b1-ff5c-42b2-b34c-4d3c2c1574d2&menu=431fab9c-d24c-4a27-ba93-e92edafdefa5. Verified on 22 November 2026.

S11: MyCERT, MA-1464.062026: malicious Windows scripts delivered through messaging, 22 June 2026. https://mycert.org.my/portal/advisory?id=MA-1464.062026. Verified on 22 November 2026.

S12: Odin by Brandefense, Public DNS, TLS and homepage observations for selected Malaysian domains. Verified on 22 November 2026.

S13: Brandefense Blackhole, Malaysian-attributed payment-card observations, 1 January–22 November 2026. Verified on 22 November 2026.

S14: OpenDOSM, ICT survey population and use-period metadata. https://open.dosm.gov.my/data-catalogue/icths_internet_device. Verified on 22 November 2026.

S15: Department of Statistics Malaysia, ICT use and access by individuals and households, reference year 2025; released 23 April 2026. https://www.dosm.gov.my/site/downloadrelease?id=ict-use-and-access-by-individuals-and-households-survey-report-2025&lang=English. Verified on 23 November 2026.

S16: Company public notice, Technology-services incident notice, April 2026. (article URL withheld). Verified on 22 November 2026.

S17: Bernama, reporting MKN and NACSA, Official assessment of circulating personal-data claims, 21 June 2026. https://www.bernama.com/en/general/news.php?id=2571178. Verified on 23 November 2026.

S18: NACSA, Official alert index: late-June JCE extension warning. https://www.nacsa.gov.my/alert.php. Verified on 23 November 2026.

S19: JCE, Security update and free patch for older sites. https://www.joomlacontenteditor.net/news/jce-security-update-and-a-free-patch-for-older-sites. Verified on 23 November 2026.

S20: NACSA, Assessment of a cloud-productivity disruption. https://www.nacsa.gov.my/ (article URL withheld). Verified on 22 November 2026.

S21: Bernama, Ministerial assessment of circulating leak claims, 18 November 2026. https://web26.bernama.com/en/news.php?id=2636239. Verified on 22 November 2026.

S22: Malay Mail, quoting service announcements, Consumer payment-platform interruption and restoration, July 2026. https://www.malaymail.com/ (article URL withheld). Verified on 22 November 2026.

S23: The Edge, quoting the provider, Isolated telecommunications customer-information disclosure, July–August 2026. https://theedgemalaysia.com/ (article URL withheld). Verified on 22 November 2026.

S24: Lowyat, quoting the institution, Financial-institution service restoration, October 2026. https://www.lowyat.net/ (article URL withheld). Verified on 22 November 2026.

S25: Malay Mail, Council account of a municipal public-display incident, 30 October 2026. https://www.malaymail.com/ (article URL withheld). Verified on 22 November 2026.

S26: The Star, Police account of a municipal public-display investigation, 30 October 2026. https://www.thestar.com.my/ (article URL withheld). Verified on 22 November 2026.

S27: Bernama, reporting the market operator statement, Broker-component incident statement, 12 March 2026. https://www.bernama.com/ (article URL withheld). Verified on 22 November 2026.

S28: The Edge, quoting a written response, Online broker restrictions following a detected attempt, 30 October 2026. https://theedgemalaysia.com/ (article URL withheld). Verified on 22 November 2026.

S30: Bernama, quoting the responsible authority, Public-service transaction-approval investigation, August 2026. https://www.bernama.com/ (article URL withheld). Verified on 22 November 2026.

S31: Lowyat, Public-website observation, November 2026. https://www.lowyat.net/ (article URL withheld). Verified on 22 November 2026.

S32: Bernama, quoting a company statement, Airline reservation-supplier disclosure, November 2026. https://www.bernama.com/ (article URL withheld). Verified on 22 November 2026.

S33: Bernama, Authority account of suspected public-website activity, 10 November 2026. https://www.bernama.com/ (article URL withheld). Verified on 22 November 2026.

S34: CVE Program, CVE-2026-48907: Joomla CNA record. https://cveawg.mitre.org/api/cve/CVE-2026-48907. Verified on 23 November 2026.

S35: PDRM, emotional shopping/delivery/donation lures, 2026-02-19. https://www.rmp.gov.my/arkib-berita/keratan-akhbar/page/25. Verified on 22 November 2026.

S36: BNM, official impersonation deepfake investment lure, 2026-08-25. https://www.bnm.gov.my/-/amaran-20260825. Verified on 22 November 2026.

S37: BNM, deepfake investment endorsements, 2026-10-13. https://amlcft.bnm.gov.my/web/guest/-/scamalert. Verified on 22 November 2026.

S38: MyCERT, MA-1499.112026: false traffic-summons phishing, 6 November 2026. https://www.mycert.org.my/portal/advisory?id=MA-1499.112026. Verified on 22 November 2026.

S39: MyCERT, MA-1513.112026: false cash-assistance registration and messaging-account phishing, 22 November 2026. https://www.mycert.org.my/portal/advisory?id=MA-1513.112026. Verified on 22 November 2026.

S40: MyCERT, MA-1451.062026: Android banking-malware lure advisory, 6 June 2026. https://www.mycert.org.my/portal/advisory?id=MA-1451.062026. Verified on 22 November 2026.

S41: MyCERT, MA-1482.102026: related Android malware variants, 18 October 2026. https://www.mycert.org.my/portal/advisory?id=MA-1482.102026. Verified on 22 November 2026.

S42: Personal Data Protection Department, Application and non-application of the Act. https://www.pdp.gov.my/en/akta/application-and-non-application-of-the-act/. Verified on 22 November 2026.

S43: Attorney General's Chambers, Cyber Security Act 2024, Act 854. https://lom.agc.gov.my/ilims/upload/portal/akta/outputaktap/2177706_BI/Act%20854.pdf. Verified on 22 November 2026.

S44: Bank Negara Malaysia, Technology requirements for payment-services regulatees, March 2026. https://www.bnm.gov.my/documents/20124/943361/pd-tecreq-psr-mar2026.pdf. Verified on 23 November 2026.

S45: Institution public statement, Response to the administrative penalty, 1 April 2026. https://dmedia.penerangan.gov.my/ (article URL withheld). Verified on 22 November 2026.

S46: Attorney General's Chambers, Cyber Security (Notification of Cyber Security Incident) Regulations 2024. https://lom.agc.gov.my/ilims/upload/portal/akta/outputp/2303986/PUA220_2024.pdf. Verified on 22 November 2026.

S47: Personal Data Protection Department, Personal Data Protection (Amendment) Act 2024, Act A1727. https://www.pdp.gov.my/wp-content/uploads/2024/11/Act-A1727.pdf. Verified on 22 November 2026.

S48: Personal Data Protection Commissioner, Data Breach Notification Guideline. https://www.pdp.gov.my/wp-content/uploads/2025/08/GP_DBN_ENG.pdf. Verified on 22 November 2026.

S49: Personal Data Protection Commissioner, Appointment of Data Protection Officer Guideline. https://www.pdp.gov.my/wp-content/uploads/2025/08/GP_DPO_ENG.pdf. Verified on 22 November 2026.

S50: Federal Gazette, Commencement notification P.U.(B)522. https://www.pdp.gov.my/wp-content/uploads/2024/12/PENETAPAN-TARIKH-PERMULAAN-KUAT-KUASA.pdf. Verified on 22 November 2026.

S51: RFC Editor, RFC 7489: DMARC. https://www.rfc-editor.org/rfc/rfc7489. Verified on 23 November 2026.

S52: RFC Editor, RFC 7208: SPF. https://www.rfc-editor.org/rfc/rfc7208. Verified on 23 November 2026.

S53: RFC Editor, RFC 6376: DKIM. https://www.rfc-editor.org/rfc/rfc6376. Verified on 23 November 2026.

S54: RFC Editor, RFC 4033: DNSSEC. https://www.rfc-editor.org/rfc/rfc4033. Verified on 23 November 2026.

S55: RFC Editor, RFC 8446: TLS. https://www.rfc-editor.org/rfc/rfc8446. Verified on 23 November 2026.

S56: RFC Editor, RFC 6797: HSTS. https://www.rfc-editor.org/rfc/rfc6797. Verified on 23 November 2026.

S57: Flare Systems, Combolists & the Dark Web: The Different Types of Leaked Credentials. https://flare.io/learn/resources/blog/combo-lists-the-dark-web-understanding-leaked-credentials. Verified on 23 November 2026.

S58: MS-ISAC, MS-ISAC Guide to DDoS Attacks. https://www.cisecurity.org/insights/white-papers/ms-isac-guide-to-ddos-attacks. Verified on 23 November 2026.

Appendix D. Glossary

These terms explain the evidence and decisions in the report. They do not add a technical or legal conclusion beyond the cited chapters.

Term	Plain meaning
MKN	National Security Council of Malaysia [S17]
NACSA / NC4	National Cyber Security Agency and its National Cyber Co-ordination and Command Centre, which issues national alerts [S18][S46]
PDRM	Royal Malaysia Police [S35]
BNM	Bank Negara Malaysia, the central bank [S44]
Atlas headline	Brandefense's national exposure rating for the assessed portfolio on a 0–100 scale; a higher value indicates more observed exposure. It is not a sector rating or a prevalence estimate [S1]
DMARC	Domain-based Message Authentication, Reporting, and Conformance: a domain policy for handling and reporting email authentication results [S51]
SPF	Sender Policy Framework: lets a domain authorise which servers may send email using it [S52]
DKIM	DomainKeys Identified Mail: a digital signature associates a signing domain with a message and supports checking signed content for changes [S53]
DNSSEC	Domain Name System Security Extensions: authenticates the origin and integrity of DNS data [S54]
TLS	Transport Layer Security: protects network communications against eavesdropping, tampering and message forgery [S55]
HSTS	HTTP Strict Transport Security: a website policy directing browsers to use secure connections [S56]
Stealer log	A record produced by information-stealing malware [S57]
Combolist	Compiled username/password combinations [S57]
DDoS	Distributed denial of service: an attack from multiple sources intended to disrupt access to a system or service [S58]
Advertisement	A post offering or requesting a product; it does not establish a completed transaction
Current credential listing	An observed offer associated with an account or domain at the time of observation; current account validity still needs checking

Term	Plain meaning
Device association	Evidence relating a device to an account or domain; ownership and current status need validation
NCII	Computer systems within the Cyber Security Act's essential-function and detrimental-impact definition [S43]
Data-protection officer	An appointed person supporting applicable personal-data responsibilities; accountability remains with the organisation [S49]
Data-breach notification	A notice required under the applicable event, scope and assessment rules [S48]
One-time password	A temporary authentication code that a phishing page can request [S9]
JCE	A Joomla editor extension covered by the vendor's security-update guidance [S19]
Remote-management agent	Software that can support remote device administration; the June advisory describes attacker-controlled installation after script execution [S11]
Listing	An extortion publication observed in the source; not an independently confirmed incident [S4]
Planning assumption	A condition used in an exercise or scenario, rather than a prediction
Unknown result	A proposition that the retained observation does not settle

About this report

Prepared by Odin by Brandefense for the Brandefense Country Report series. The research window is 1 January–22 November 2026. The report prioritises retained Brandefense observations and uses public sources for incident accounts, technical guidance and legal context.

This is a descriptive threat-landscape report, not a census of Malaysian cyber incidents. It separates observations, claims, official accounts and analytical judgments. The English edition is the master text. The Malay edition carries an AI-translation notice and preserves the same figures, source IDs, card IDs and directives.

© 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