BRANDEFENSE COUNTRY REPORT · SAUDI ARABIA 2026

Brandefense Saudi Arabia Cyber Threat Landscape Report 2026

Customer-data claims, identity demand and repeated disruption narratives across a connected service economy

Odin by Brandefense
Research window: 1 January–22 November 2026
Version 1.0 · Public Research Edition · TLP:CLEAR · 22 November 2026

4
leadership decisions tied to owned actions

96 of 249
assessed domains had a credential listed for sale when checked

220
country-tagged forum posts in the window

30
Saudi-labelled ransomware listings in the reporting window

CONTENTS

Contents

01	Executive summary	05
	Report map	09
02	Saudi Arabia's digital and threat context	10
03	National exposure: a selected 250-domain portfolio	13
04	Dark-web observations and case evidence	20
05	Targeting examples by sector	41
06	Hacktivism, disruption claims and service status	45
07	Threat actors, claims and ransomware listings	52
08	The fraud economy visible in the evidence	60
09	Banking and financial services deep dive	65
10	Regulatory and national response	69
11	Outlook	73
12	Action plan	77
A	Appendix A. Scope, sources and confidence	84
B	Appendix B. Public evidence-card register	88
C	Appendix C. Sources	89
D	Appendix D. Glossary	91
E	Appendix E. Additional reviewed claim themes	93
	About this report	96

Executive leadership	1 → 3 → 11 → 12
SOC and identity	4 → 6 → 7 → 12
Fraud and support	8 → 9 → 12
Data and supplier owners	4 → 5 → 10 → 12
Legal and compliance	1 → 10 → 12

About this edition

AI-assisted research, analysis and drafting by Odin by Brandefense. The English master and Arabic edition share the same evidence boundaries. Source verification date: 22–23 November 2026. Method summary in Appendix A.

Contents and reading routes

Chapter	Question
1. Executive summary	Which decisions matter first?
2. Digital context	Where do identity and service trust intersect?
3. National exposure	What does the selected portfolio establish?
4. Dark-web evidence	What was offered, requested or claimed?
5. Sector examples	Which owner should act first?
6. Hacktivism and disruption	How do claims compare with service evidence?
7. Actors and ransomware	What do posting identities and listings establish?
8. Fraud economy	Where could account and data offers meet payment risk?
9. Financial services	How should identity, support and fraud work together?
10. Regulatory response	Which reporting conditions and owners apply?
11. Outlook	Which new evidence would change the response?
12. Action plan	What must be tested over 30/60/90 days?
Appendices A–E	Scope, evidence cards, sources and glossary

The executive route is Chapters 1, 3, 10, 11 and 12. The SOC route is Chapters 4, 6, 7 and 12. The data, application and supplier route is Chapters 4, 5, 8, 9 and 10.

Three evidence labels govern the report. **Observed** means a retained post, listing or public observation exists. **Claimed** means a poster asserts an outcome. **Reported or confirmed** names the source and the exact proposition it supports. None of these labels validates every statement in a source.

CHAPTER 01

Executive summary

01

THIS CHAPTER ANSWERS

What should Saudi organisations prioritise, and how strong is the evidence?

4

leadership decisions tied to owned actions

Four decisions for leaders 07

The study in numbers 07

CHAPTER 01

Executive summary

IN SHORT

A disclosed mobile-app incident, customer-data advertisements and repeated disruption claims require different response paths. Ransompedia records 30 Saudi-labelled listings. Credentials tied to 96 of 249 assessed domains were listed for sale; the national Atlas headline is 52/100. These observations do not establish current access or national prevalence. Validate identities and data relationships, test recovery, and establish one route for incident reporting and customer protection.

The report covers posts and publications from 1 January to 22 November 2026. The recent-activity view covers 8–22 November. The cut-off day was still in progress during research. Own observations and public reporting are separate evidence populations. A post date is not automatically an intrusion date. [S1][S2]

1. A disclosed app incident separates confidentiality from continuity. Budget Saudi's 9 June issuer statement confirmed limited unauthorised access to some mobile-app customer data. The company said financial and banking data were unaffected and operations continued. Those impact limits remain the issuer's account. The disclosure supplied no affected-customer count or root cause (§4.5, Case A). [S17][S18][S28]

2. Advertisements describe sensitive services and suppliers, with outcomes unverified. Ten forum dossiers cover public-body code, health data, account demand, investment records, contractor archives, wellness CRM, driver data and parcels. They document advertisements or demand, rather than confirmed intrusions. The response begins with an authorised internal or supplier match (§4.6). [S1]

3. Disruption narratives recur from March through October. The retained 313 Team material contains 17 posts across nine claim sequences from March through October. Financial, public, education, employee-facing and telecommunications services appear. Claimed attack durations are not measured downtime (§6.3). [S1]

4. Ransomware listings justify readiness without establishing incident prevalence. The retained feed has 30 Saudi-labelled listings, compared with 84 for the UAE, 9 for Qatar, 7 for Kuwait and 9 for Oman. Three Saudi entries fall in the recent period. Their dates and labels remain feed observations, without official target confirmation established here (§7). [S2]

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

5. Current listings give identity validation a defined scope. Credentials tied to 96 of 249 assessed domains were listed for sale. The national Atlas headline for the assessed portfolio is 52/100. One of the 250 selected domains remains unknown. Ownership and group overlap limit entity inference; email, DNS and web control prevalence remains unassessed (§3). [S3][S4]

Four decisions for leaders

1. **Establish identity triage now.** The identity leader should own a route for listing, account-demand and device-association signals. Investigate received alerts promptly; contain immediately when usable stolen authentication material or unauthorised activity is evidenced. Retain a disposition and recovery decision (A01–A03, §12.1).
2. **Validate customer and supplier data relationships.** Application and supplier-risk owners should map sensitive data access and shared document stores. Test mobile-app access separation and confirm critical supplier escalation routes. Escalate a claim when credible matching material or supplier confirmation appears (A04, A09, §12.1).
3. **Prove recovery and independent service-status assessment.** Continuity and operations leaders should restore a critical service and rehearse disruption-claim handling. The completion evidence is a restore result and a telemetry-backed account of affected functions (A05, A10, §12.1).
4. **Connect fraud, privacy and reporting owners.** Test one safe customer-recovery and payment-change journey. Document who assesses notification conditions, who approves communications and who protects the transaction. Incident-driven action takes priority over the programme schedule (A08, A11, A12, §12.1).

The study in numbers

748,946

Saudi-associated country-tagged posts in the window

WHAT IT IS NOT

Not attacks, affected people or verified Saudi targeting

220

Retained country-tagged forum posts across the window

WHAT IT IS NOT

Not unique incidents or all Saudi forum content

17 / 9

Posts / claim sequences from the 313 Team posting identity

WHAT IT IS NOT

Not measured outages or independent operators

30

Saudi-labelled Ransompedia listings

WHAT IT IS NOT

Not confirmed intrusions, encryption events or loss estimates

3

Saudi-labelled listings dated 8–22 November

WHAT IT IS NOT

Not three newly confirmed incidents

250

Candidate organisation domains in ten merged cells

WHAT IT IS NOT

Not a representative sample or a validated entity ranking

52/100

National Atlas headline for 249 assessed domains

WHAT IT IS NOT

Not a breach percentage or a national prevalence estimate

16

Detailed case dossiers, including source-reported campaigns

WHAT IT IS NOT

Not a national incident total

19

Public post cards tied to private source records

WHAT IT IS NOT

Not all observed posts or independently confirmed claims

Report map

Follow a decision from the executive finding to its evidence, owner and closure test. Chapter references identify where the proposition is assessed.

Executive leadership	What should receive attention and funding first?	1 → 3 → 11 → 12
SOC and identity	Does the signal concern usable access or service impact?	4 → 6 → 7 → 12
Fraud and support	Can a customer event be linked to an account or payment change?	8 → 9 → 12
Data and supplier owners	Which shared records or permissions could be relevant?	4 → 5 → 10 → 12
Legal and compliance	Which conditions and clocks require a decision?	1 → 10 → 12

Evidence question	Read	Completion question
Is the record a demand, advertisement or confirmed disclosure?	4 and Appendix B	What proposition has actually been established?
Are two observations connected?	7	Is there a concrete link or only an analytical model?
Is a service affected?	6	What do independent operational records show?
Does a rule apply to this entity?	10	Who documented applicability and the reporting decision?

KEY TAKEAWAYS

01

Start with identity, customer data, continuity and owned reporting decisions.

02

Separate observed claims from verified access and service impact.

03

Use the action plan's completion evidence to judge progress.

CHAPTER 02

Saudi Arabia's digital and threat context

02

THIS CHAPTER ANSWERS

Which features of the digital economy shape the defensive priorities?

99.6%

internet use among people aged 15–74 in the official 2026 survey

2.1 Connectivity makes service identity a security boundary 11

2.2 Energy, transport and suppliers require different response plans 11

2.3 Regional campaigns are context, with bounded Saudi evidence 12

2.4 Read official warnings as operational tasks 12

CHAPTER 02

Saudi Arabia's digital and threat context

IN SHORT

Saudi services operate in a highly connected environment. The official household survey reports widespread internet and digital-government use, while security researchers describe enterprise phishing and password spraying against Saudi targets. These sources describe different populations. They support attention to identity, mobile applications and trusted service brands, without establishing a national attack rate. Map the accounts and suppliers that can change a payment or expose customer information, then test their controls.

2.1 Connectivity makes service identity a security boundary

The official statistics release of 1 November reports internet use of 99.6% among people aged 15–74. It reports digital-government use of 98.4% in that age group. These are survey results, not measures of security or the whole population. [S16]

For defenders, the practical question is where people place trust. A customer may move from a message to an app, a support call and a payment approval within one transaction. A strong control at one stage cannot establish the identity of every other participant. The control owner needs a view of the entire transaction.

This report therefore connects enterprise identity with consumer-facing fraud. The connection is an analytical model of possible abuse. It does not establish a shared operator between an enterprise-phishing campaign and a separate account seller.

2.2 Energy, transport and suppliers require different response plans

The organisation portfolio includes public services, energy, finance, logistics, industry, education, healthcare and commercial services. Its purpose is to support decisions across dependencies. It is not an economic ranking or a representative survey of Saudi organisations. [S3]

An industrial operator needs to protect engineering access and safe recovery. A transport provider needs to protect booking, customer data and operational interfaces. A university needs to distinguish staff accounts from student and alumni accounts. Applying one response to every domain association would obscure these differences.

Suppliers can hold copies of operationally important data even when a principal's own system is unaffected. A claim naming a contractor therefore calls for a data-sharing review. It does not establish access to every project partner.

2.3 Regional campaigns are context, with bounded Saudi evidence

Unit 42 reported enterprise credential phishing and financial fraud directed at Saudi organisations in its regional brief (version updated 17 April). Check Point reported limited Saudi targeting within a wider Microsoft 365 password-spray campaign. Neither source supplies a national Saudi incident total. [S11][S12]

The defensive implications differ. A convincing enterprise login lure calls for origin-aware authentication and user reporting. Password spraying calls for tenant-wide authentication analysis. Neither observation establishes which Saudi account, if any, was used successfully.

Political labels appear only where a source's attribution is necessary to understand its research. The report assesses the reported cyber activity. It offers no assessment of governments, the royal family, regional relationships, religion or public policy choices.

2.4 Read official warnings as operational tasks

NCA's existing Essential Cybersecurity Controls provide a baseline for entities within their scope. Saudi CERT publishes product-security warnings. The warnings establish advice to investigate affected products, rather than evidence that Saudi networks were attacked through those products. [S6][S13]

The relevant operating discipline is a closed loop. Identify the service owner, determine applicability, act, and retain evidence of the result. A warning ticket closed because a patch was downloaded does not establish that every affected instance was updated.

KEY TAKEAWAYS

01

Keep survey connectivity separate from attack measurements.

02

Protect the whole identity and payment journey, including suppliers.

03

Turn each applicable warning into a named task with closure evidence.

CHAPTER 03

National exposure: a selected 250-domain portfolio

03

THIS CHAPTER ANSWERS

Which observed signals need an accountable validation owner?

96 of 249

assessed domains had a credential listed for sale when checked

3.1 Universe card 14
3.2 National Atlas headline and sector signals 15
3.3 Devices and credential records require different owners 16
3.4 Mentions and similar names are context 18
3.5 External domain-control observations 19
3.6 Keep the response proportional 19

CHAPTER 03

National exposure: a selected 250-domain portfolio

IN SHORT

Credentials tied to 96 of 249 assessed domains were listed for sale when checked. The selected portfolio contains 250 candidate organisation domains; one has no complete exposure result. The national Atlas headline for the assessed portfolio is 52/100. Its device and credential associations describe external observations, not confirmed intrusions or national prevalence. Ownership and related-group overlap remain limitations. Validate current accounts, employee-device associations and relevant service relationships with their responsible owners.

3.1 Universe card

Item	Definition
Selection	250 candidate organisation domains in ten sector cells of 25, chosen for public-service roles or significant Saudi operations
Unit	One selected primary domain per candidate; related legal entities and shared groups may overlap
Identity status	Ownership, operating status and independent entity status have not been established for every domain
Exposure snapshot	22 November 2026; 249 complete domain assessments, with one unknown result in digital services and communications
Record dates	Device, credential, document and listing observations held at the snapshot; they are not restricted to material first captured during 2026
Mention context	19 November 2025–18 November 2026; separate from the report's post-publication window
Similar names	A separate 30-day observation window; candidate relationships require validation
Generalisation	Descriptive results for selected domains only; no national prevalence estimate or independent-entity census

The portfolio is an investigation aid. It is not a list of victims. Inclusion does not establish an incident or identify every associated record as an employee's. The missing domain remains unknown and is excluded from exposure denominators. [S3]

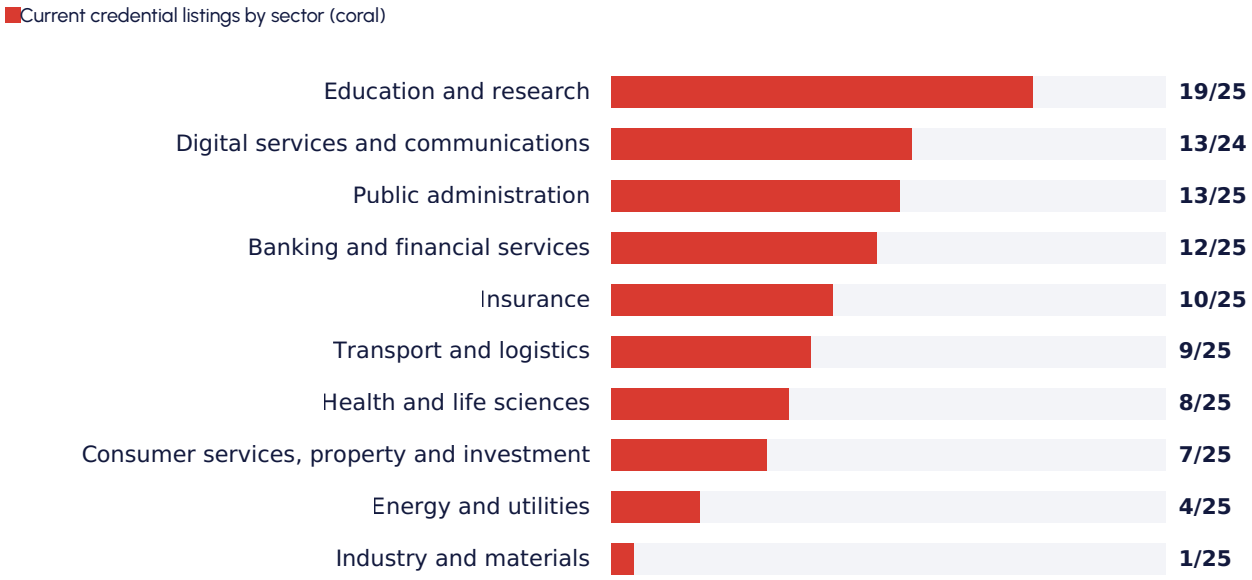
3.2 National Atlas headline and sector signals

Credentials tied to 96 of 249 assessed domains were listed for sale. A listing establishes an advertisement at the check, without establishing credential validity, an active account, a completed sale or an intrusion. Validate the relevant service and identity before taking disruptive action. [S3]

The national Atlas headline for the assessed 249-domain portfolio is 52/100. Higher values indicate greater observed exposure on the 0–100 scale. This figure is not a breach percentage, incident probability or assessment of every Saudi organisation. It excludes the domain without a complete result.

Only the national rating is published. Sector rows show measured signals and their denominators. In the chart and table below, "Currently listed" counts assessed domains with credentials listed for sale at the check, not organisations offered for sale. Equal selected-domain counts do not imply equal economic size, ownership independence or security risk.

Current credential listings across the assessed sector populations



Listed domains / assessed domains; the one unknown result is excluded. A listing does not establish usable access. Source: Brandefense Atlas and Blackhole domain associations, 22 November 2026 [S3]. 250 selected domains, 249 assessed; records can overlap and include older observations.

Sector	Selected	Assessed	Currently listed	Documents
Public administration	25	25	13	220
Banking and financial services	25	25	12	70
Insurance	25	25	10	10
Energy and utilities	25	25	4	133
Industry and materials	25	25	1	44

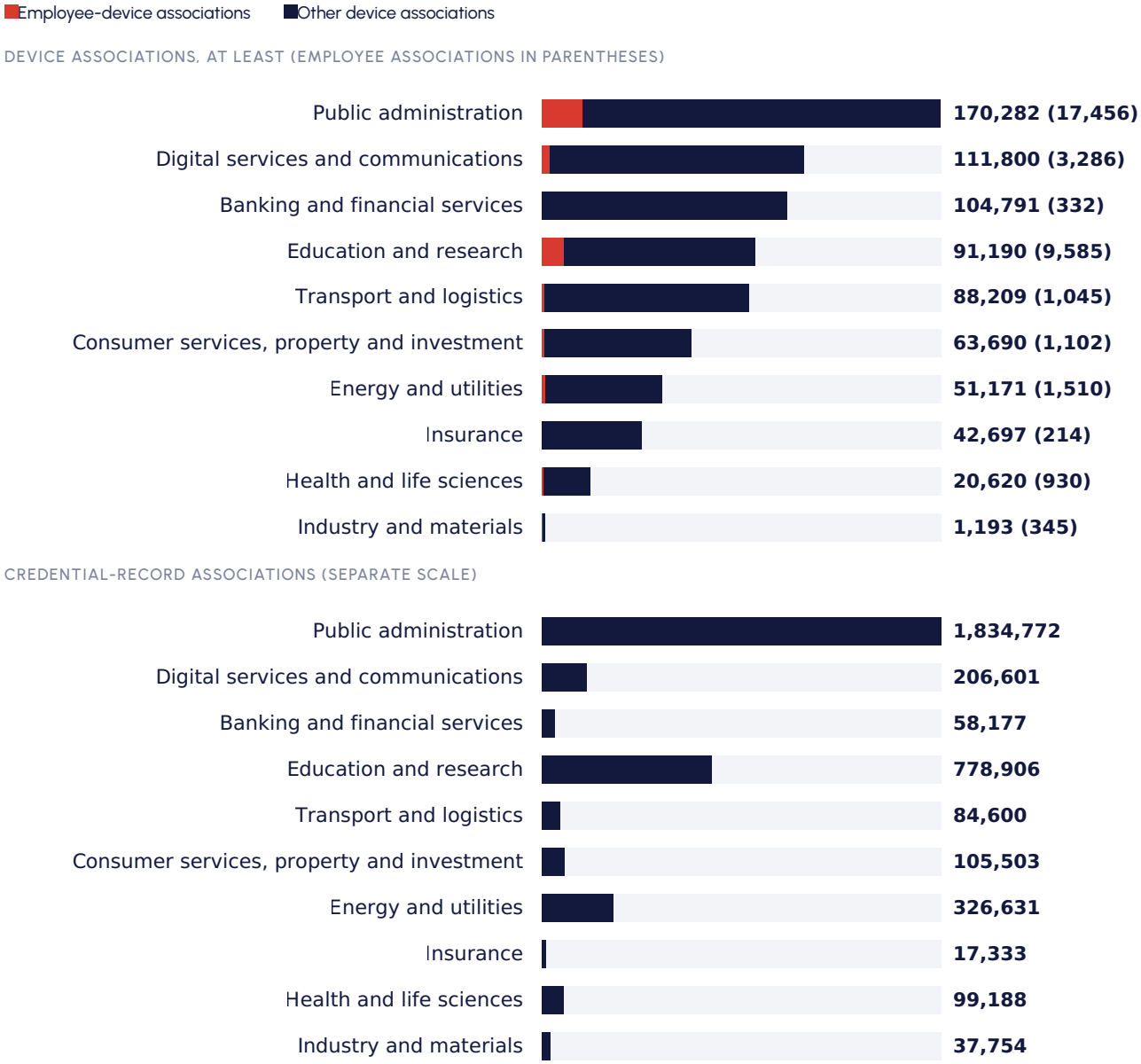
Sector	Selected	Assessed	Currently listed	Documents
Transport and logistics	25	25	9	86
Digital services and communications	25	24	13	110
Health and life sciences	25	25	8	88
Education and research	25	25	19	269
Consumer services, property and investment	25	25	7	98
Total	250	249	96	1,128

The document column counts 1,128 document associations across 156 assessed domains. These observations do not establish confidentiality, unlawful acquisition or adversary access. Public documents and repeated material can explain an association.

3.3 Devices and credential records require different owners

The assessed portfolio contains at least 745,643 device associations, including 35,805 employee-device associations. It also contains 3,549,465 credential-record associations. These populations can overlap across domains; they are not unique people or a national endpoint count. [S3]

Device associations and credential records have different populations



Source: Brandefense Atlas and Blackhole domain associations, 22 November 2026 [S3]. 250 selected domains, 249 assessed; records can overlap and include older observations.

Sector	Assessed	Devices, at least	Employee devices	Credential records
Public administration	25	170,282	17,456	1,834,772
Banking and financial services	25	104,791	332	58,177
Insurance	25	42,697	214	17,333
Energy and utilities	25	51,171	1,510	326,631
Industry and materials	25	1,193	345	37,754

Sector	Assessed	Devices, at least	Employee devices	Credential records
Transport and logistics	25	88,209	1,045	84,600
Digital services and communications	24	111,800	3,286	206,601
Health and life sciences	25	20,620	930	99,188
Education and research	25	91,190	9,585	778,906
Consumer services, property and investment	25	63,690	1,102	105,503
Total	249	745,643	35,805	3,549,465

Employee-device associations are presented within the device view and must not be added to it. Other device associations can concern customers or other service users. A banking-domain association does not by itself establish access to bank infrastructure.

Public administration contributes 1,834,772 credential-record associations, while education and research contributes 778,906. These totals support focused validation with identity and service owners. They do not rank current compromise rates or establish when an account was exposed.

Historical records can remain visible after remediation. Establish whether the identity exists, whether relevant authentication material has changed and whether suspicious activity followed. When employee access is corroborated, review sessions, recovery methods and delegated authority alongside passwords.

3.4 Mentions and similar names are context

The annual mention view contains chat references for 56 selected domains and web references for 27. These overlapping populations can include news, legitimate links, customer discussions and advertising. A mention alone does not establish hostile activity. [S3]

Similar-name candidates appear for 182 of the 249 assessed domains. Similarity alone does not establish impersonation or phishing. Validate ownership, authorisation and service behaviour before escalating suspected brand misuse.

A current listing, historical credential record, document association and similar-name candidate are separate signals. Do not add them into an affected-person total. Route each credible proposition to the relevant identity, endpoint, fraud, data or brand owner.

3.5 External domain-control observations

Complete external domain-control results are unavailable. The report therefore publishes no DMARC, SPF, DKIM, DNSSEC, TLS or web-header prevalence, and no sector hygiene index. The selected-domain count is not an assessed-control denominator. [S4]

Public DNS and website observations describe services at their check date. They do not measure the effectiveness of an organisation's entire security programme. A valid certificate does not establish application access control, and a missing observation is not a failed control.

Email authentication should be evaluated across the actual sending estate. A selected-domain policy may not describe every subsidiary, subdomain or outsourced sender. Identify legitimate mail flows and test the business effect before changing enforcement.

3.6 Keep the response proportional

Observation	First validation	Proportionate decision
Credential advertisement	Identity, usability, freshness and prior remediation	Investigate; contain when usable stolen access or abuse is evidenced
Device association	Ownership, context and relevant accounts	Route to the appropriate endpoint or customer-security process
Historical credential record	Whether relevant access changed	Close with evidence or investigate unresolved exposure
Similar-name candidate	Brand use, service behaviour and authorisation	Review and use the appropriate brand-response route
Email or web policy issue	Actual sending or service configuration	Correct with the responsible service owner

KEY TAKEAWAYS

01

The national Atlas headline covers 249 assessed domains within the selected portfolio.

02

Device, credential, listing and document populations overlap and cannot be summed as victims.

03

Validate the identity, owner and service before choosing a disruptive response.

CHAPTER 04

Dark-web observations and case evidence

THIS CHAPTER ANSWERS

What does the retained material establish about data, account and access claims?

220

country-tagged forum posts in the window

4.1 Universe card 21
4.2 Monthly volume and its limits 21
4.3 Recurring evidence categories 23
4.4 Timing, repetition and recency 24
4.5 Cases from public reporting 24
4.6 Forum case dossiers 27
4.7 Recent activity: 8–22 November 37
4.8 What the cases do and do not support 39

CHAPTER 04

Dark-web observations and case evidence

IN SHORT

The retained forum material contains advertisements for customer and document data, account demand and remote-access offers. The wider country tag is dominated by the first two months, while the content view has explicit limits. Ten forum dossiers preserve the differences between a post, a dataset claim and verified access. Public reporting adds a confirmed app disclosure and reported campaigns. Validate relevance through internal records and established supplier channels before describing impact.

4.1 Universe card

Item	Scope
Window	1 January–22 November 2026 by post time
Country-tagged volume	748,946 posts associated with Saudi Arabia; a tag does not establish targeting
Country-tagged forum material	220 retained posts in the window
Arabic-associated material	5,043 retained posts carrying the Arabic association
Retained combined material	33,458 distinct posts across the content views
Interpretation	Posts, accounts, advertisements, claimed datasets and incidents remain different units
Outcome evidence	Claims are not target-side validation; no advertised access was tested

The universe describes the observed material. Many posts can repeat a product, name several countries or discuss an older event. A country association therefore cannot be converted into a victim count. [S1]

4.2 Monthly volume and its limits

The monthly figure shows country-tagged post volume. January and February account for 97.4% of that volume. The report does not interpret this distribution as a change in attack frequency. [S1]

The first two months dominate country-tagged volume



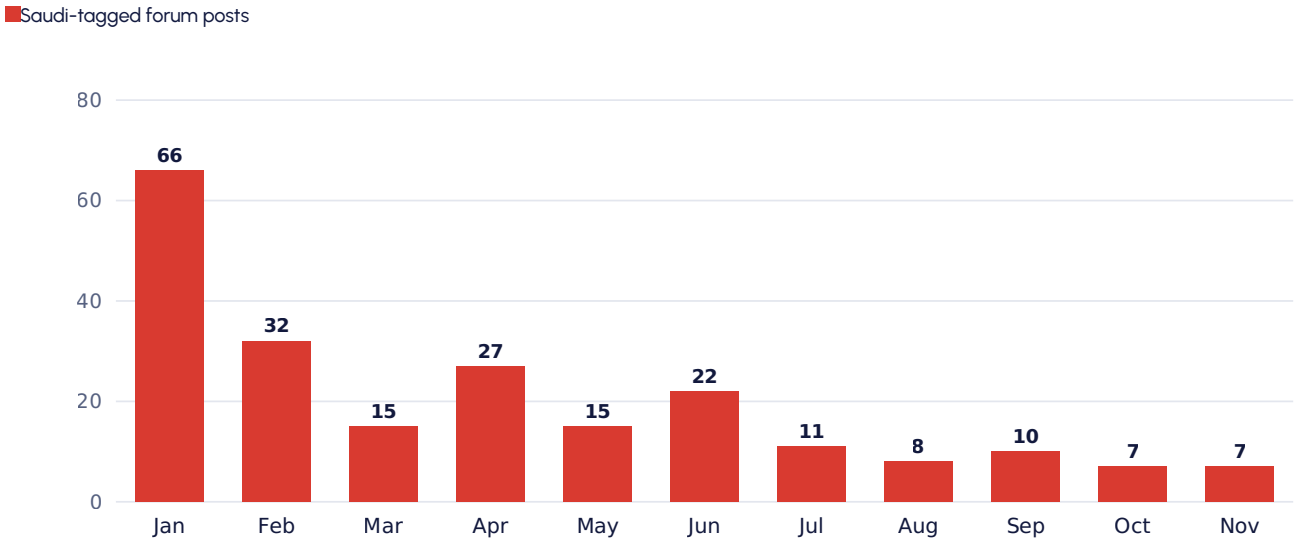
Source: Brandefense Blackhole, Saudi-tagged posts, 1 January–22 November 2026; November partial [S1]. Tagged volume does not measure attacks.

Month	Country-tagged posts
2026-01	412,060
2026-02	317,126
2026-03	4,257
2026-04	3,296
2026-05	1,993
2026-06	1,984
2026-07	2,474
2026-08	2,067
2026-09	1,564
2026-10	1,319
2026-11	806
Total	748,946

Service-menu advertisements predominate in the January and February material, often mentioning Saudi Arabia as one item in a multi-country offer. This limits its value as country-specific threat evidence. Coverage varies by month and source. These observations do not establish national prevalence or changes in attack frequency.

The forum view is useful for a different question: which offers and discussions were visible in that source population? It contains 66 January posts; every later month has fewer than January. This is coverage of forum observations, not a national incident curve.

The country-tagged forum view has its largest volume in January



Source: Brandefense Blackhole, Saudi-tagged posts, 1 January–22 November 2026; November partial [S1]. Tagged volume does not measure attacks.

4.3 Recurring evidence categories

Category	Examples held	What can be established	What cannot be inferred
Data advertisements	Investment, health, wellness, driver and parcel descriptions	An offer and its stated fields or quantities	Authenticity, current access or affected people
Document and code bundles	Public-body and contractor archives	A description and circulation chronology	Classification, production access or partner-wide impact
Account demand	Requests for Saudi-related accounts	Expressed buyer interest	Supply, a transaction or usable access
Remote-access advertising	Medical-facility access offer	A seller's capability claim	Successful authentication or operational control
Disruption claims	Repeated service-target posts and updates	A posting narrative	Measured downtime, cause or data access
Fraud-service advertising	Account-holder provisioning and receiving-account demand	A service offer or solicitation	Completed laundering, fraud success or bank-system access

These categories overlap in their subject matter. They are not mutually exclusive incident verdicts and are not summed into a national total. The case dossiers preserve the specific proposition supported by each source.

4.4 Timing, repetition and recency

A repost can renew attention without establishing a new intrusion. In Case E, the poster explicitly describes republication. In Case H, a follow-up adds sample material on the same day. In Case L, several forum records describe one archive theme. [S1]

A separate workforce-data offer in March illustrates unresolved freshness. A reply asked whether the material came from 2021, while the poster asserted it was fresh. The exchange does not resolve the age of the underlying records. It supports checking prior incidents and remediation before choosing a new disruptive response. [S1]

The same distinction applies to technical entry narratives. A seller can claim employee deception or persistence without providing evidence that the described path worked. The report preserves those assertions as claims rather than adopting them as established attack chains.

A 10 September relay also described public-sector documents. Its relationship to the June archive is unestablished. Similar descriptions do not prove file identity or a new acquisition date. [S1]

4.5 Cases from public reporting

The cases below separate a controller disclosure, a relayed criminal claim and vendor-observed campaigns. Their dates refer to publication unless a source explicitly supplies an event date. They are not four additional confirmed intrusions.

CASE A

A

A mobile-app customer-data disclosure

Transport and logistics

Issuer disclosure

CLAIM AND SOURCE	On 9 June, Budget Saudi disclosed unauthorised access to a limited portion of some customers' data through its mobile application. The official issuer statement was also published by financial-news outlets. [S17][S18][S28]
CHRONOLOGY	The company said it activated containment procedures after detection and continued technical assessment with relevant authorities. Its public disclosure did not give an intrusion date or affected-customer count.
ESTABLISHED PROPOSITION	The issuer publicly confirmed a customer-data access incident. It said financial and banking information was unaffected and services continued without disruption. Those scope and impact limits remain the company's statements.
ALTERNATIVES AND LIMITS	The disclosure does not identify an actor, a vulnerability, the affected fields or a ransomware connection. Continued service availability does not settle confidentiality impact.

RESPONSE	Application owners should map customer-data access, test separation between customer accounts and preserve the decision chronology. Privacy teams should assess the notification conditions against verified data scope.

Bottom line

Confirm scope through the incident process; continuity and confidentiality are separate.

The case shows why operational continuity and data confidentiality need separate assessment. It does not support a conclusion about the security of other applications or the entire transport sector.

CASE B

B

An unverified construction-sector data claim

Construction

Relayed claim, unverified

CLAIM AND SOURCE	The National reported a monitor's account of a WallStreet claim involving a construction business. The allegation concerned a large file collection and employee information. Its stated quantities remain unverified. [S19]
CHRONOLOGY	The article was published on 6 October and associated the allegation with 3 October. The claimed event date is not a verified intrusion timestamp. A 21 October relay repeated a similar allegation, without independent confirmation or an established new event. [S1]
ESTABLISHED PROPOSITION	The newspaper reported the claim and sought comment. It did not provide an official confirmation of data theft. The reviewed account did not contain a substantive company response or authority confirmation.
ALTERNATIVES AND LIMITS	The material could include supplier-held records, repeated data or an over-stated scope. Neither an advertisement nor project references establish entry into a principal's network. The report does not establish which alternative is correct.
RESPONSE	Relevant data owners should review contractual data sharing and ask affected suppliers for a scoped statement through established channels. Escalate when credible records or supplier confirmation connect the claim to protected data.

Bottom line

Validate the data relationship before describing partner impact.

A supplier allegation is a reason to establish the data relationship. It is not a reason to announce that every partner experienced an intrusion. The public citation withholds the article URL to protect the unnamed business.

CASE C

C

A reported cloud password-spray campaign

Cross-sector identity

Vendor-observed campaign

CLAIM AND SOURCE	Check Point reported three campaign waves on 3, 13 and 23 March. Its research described limited Saudi targeting within a campaign concentrated in other countries. [S12]
CHRONOLOGY	The report was published on 31 March. It describes attempts across many accounts rather than one Saudi disclosure. It does not provide a Saudi-specific count of successful sessions.
ESTABLISHED PROPOSITION	The source observed campaign activity against some Saudi targets. Check Point assessed the actor's origin as Iran with moderate confidence. This report repeats that attribution only as the source's assessment.
ALTERNATIVES AND LIMITS	Campaign-wide descriptions of mailbox access must not become proof of access at every Saudi target. A shared technique does not establish that any named actor in another report operated this campaign.
RESPONSE	Identity teams should investigate authentication failures across accounts and correlate them with successful sessions and subsequent activity. Preserve alternative explanations such as legitimate identity-service changes.

Bottom line

Investigate accounts and sessions without extending campaign-wide outcomes.

The practical unit is the account and session. Country attribution does not change the need to validate the observed authentication sequence before choosing containment.

CASE D

D

Reported enterprise-login and payment impersonation

Cross-sector fraud

Vendor-observed campaign

CLAIM AND SOURCE	Unit 42 described Saudi-directed enterprise credential phishing using ERP-brand impersonation, alongside utility-billing, investment and banking lures. The brief is a campaign account, not a national victim census. [S11]
CHRONOLOGY	The cited version was updated on 17 April 2026. Its wider regional observations involve different countries and should not all be assigned to Saudi Arabia.

ESTABLISHED PROPOSITION	The source reported Saudi-directed phishing and financial fraud. It did not publish a Saudi loss total, a complete victim list or a count of successful account access for these observations.
ALTERNATIVES AND LIMITS	An impersonated brand can be a lure without its own systems being accessed. Reused page designs or hosting services do not establish one operator. No state attribution is added to this Saudi fraud description.
RESPONSE	Test enterprise sign-in reporting and trusted verification of payment instructions. Link customer-support and fraud cases when the same transaction or recovery process is involved.

Bottom line

Protect trusted sign-in and payment verification paths.

Brand trust crosses organisational boundaries. A response therefore needs both technical evidence and a safe route for customers to verify an instruction. A brand-monitoring alert alone cannot establish who lost money.

4.6 Forum case dossiers

The following dossiers describe observed advertisements and one buyer request. None establishes an officially confirmed intrusion. Reposts and replies remain part of their original dossier. The card register records post dates, not theft dates. [S1]

E

CASE E

A public-body source-code and credential claim

Evidence card B01 | 17 Jan 2026 | Forum | Public administration

Claim unverified

CLAIM	A poster advertised source code and database credentials attributed to a public body. The poster presented an alleged copyright complaint as confirmation of the material.
CHRONOLOGY	The retained thread begins on 17 January, with related records on 18 and 24 January. The poster explicitly said it was a repost. These dates establish circulation, not initial acquisition.
ESTABLISHED PROPOSITION	The forum advertisement and repost narrative are held. The report does not validate the displayed code or any credential.
ALTERNATIVES AND LIMITS	A complaint does not establish authenticity. The material could be historical, copied or a test configuration. Repetition does not make the alleged access current.

RESPONSE	Repository and identity owners should compare the claim with authorised internal records. If a real exposed secret matches current use, contain that exposure through the incident process. Do not test advertised access.

Bottom line

Check source-control provenance and current secrets through authorised internal records.

Evidence card B01 17 Jan 2026

zer0sintt Forum Forum English

ORIGINAL

so I am reposting it

Note. Advertisement or demand only; the date is the post date. [S1]

Held

Source-code and credential advertisement with an explicit repost narrative. [S1]

Not established

Copyright action, a code fragment and repeated posts do not establish an intrusion or valid current access. The fragment could be old, copied, a test configuration or otherwise unusable.

F

CASE F

A health-data service offer

Evidence card B02 | 30 Jan 2026 | Forum | Healthcare

Claim unverified

CLAIM	A 30 January post offered data attributed to a health-data service and described it as fresh. Its field descriptions combined identity, contact and health-related information.
CHRONOLOGY	The post date is the only established timing for the offer. It does not establish when the records originated or when any alleged access occurred.
ESTABLISHED PROPOSITION	The poster advertised a dataset with sensitive field categories. The statement of freshness belongs to the poster.
ALTERNATIVES AND LIMITS	A field list cannot establish production-system origin or completeness. Public, synthetic, supplier-held or historical material can resemble an internal schema. The report does not determine which explanation applies.
RESPONSE	Data owners should validate field relationships against authorised data stores and assess sensitivity. Where corroboration exists, privacy and incident teams should scope access and reporting. A sample description alone does not settle that decision.

Bottom line

Match fields to controlled data flows before scoping privacy response.

Evidence card B02 — 30 Jan 2026

alwayslearning | Forum | Forum | English

ORIGINAL

Data is fresh. Data is highly valuable.

Note. Advertisement or demand only; the date is the post date. [S1]

Held

Health-data offer describing identity, contact and health fields. [S1]

Not established

Country association and schema descriptions do not validate origin, completeness, recency or access to production. A supplied sample is unverified.

CASE G

G

Demand for digital-identity and infrastructure accounts

Evidence card B03 | 2 Feb 2026 | Forum | Cross-sector identity

Demand observed

CLAIM	On 2 February, a buyer sought Saudi-related accounts described as ready and checked. The request included identity and infrastructure services, which are described broadly here.
CHRONOLOGY	One demand post is held for this dossier. No seller response, transaction or later successful authentication is established.
ESTABLISHED PROPOSITION	The post shows an expressed purchasing interest. It does not show an available account or a vulnerable service.
ALTERNATIVES AND LIMITS	A buyer can advertise demand without acquiring anything. The request cannot establish price, supply, account validity or the owner's relationship to the requested service.
RESPONSE	Identity teams should review high-risk recovery and contractor-access paths. The demand informs a control review; disruptive account actions require a stronger connection to an actual identity or abusive activity.

Bottom line

Review recovery controls; a buyer request does not identify an exposed account.

Evidence card B03 — 2 Feb 2026

l0rd0f | Forum | Forum | English

ORIGINAL

Looking to buy any saudi-arabia related accounts

Note. Advertisement or demand only; the date is the post date. [S1]

Held

One request for Saudi-related identity and infrastructure accounts. [S1]

Not established

Demand establishes interest only. It does not show a seller, a transaction, account validity, successful authentication or victim compromise.

CASE H

H

An investment-platform customer-data offer

Evidence card B04 | 13 Feb 2026 | Forum | Financial services

Claim unverified

CLAIM	A seller advertised around 7,000 investor records attributed to an investment platform. The description included identity and registration fields, alongside financial-account references.
CHRONOLOGY	The seller posted on 13 February and added further sample material later that day. These are two records in one dossier.
ESTABLISHED PROPOSITION	The advertisement and follow-up are held. Their matching context supports a continuing offer, not two incidents.
ALTERNATIVES AND LIMITS	The claimed record count, balances and data origin are unverified. References to wallet or account fields do not establish funds were accessed or lost.
RESPONSE	Data and fraud owners should assess whether the described fields match authorised interfaces. Investigate linked account activity when corroborated. Keep the disclosure assessment separate from the payment-loss assessment.

Bottom line

Separate customer-data disclosure from wallet integrity and financial loss.

Evidence card B04 — 13 Feb 2026

agent7001 | Forum | Forum | English

ORIGINAL

around 7k of investors data.

Note. Advertisement or demand only; the date is the post date. [S1]

Held

Investment-record offer and a same-day follow-up. [S1]

Not established

The two posts are one dossier, not two incidents. Record counts and account/wallet fields are seller claims; no balance accuracy, loss or live access is established.

CASE I

A contractor bundle with project documents

Evidence card B05 | 23 Feb 2026 | Forum | Construction and engineering

Claim unverified

CLAIM	A seller advertised a contractor bundle for 40,000 USD. The description included personnel material, project maps and contracts, and alleged an agreement affecting one company's inclusion.
CHRONOLOGY	Two substantially matching records carry the same 23 February time. They document repeated advertising rather than independent confirmation.
ESTABLISHED PROPOSITION	The offer, quoted size and asking price are held as seller statements. No completed sale or agreement is established.
ALTERNATIVES AND LIMITS	Supplier-held documents can concern a principal without establishing access to the principal's systems. The contents, technical sensitivity and operational relevance remain unverified.
RESPONSE	Procurement and engineering-security teams should identify shared document dependencies. Validate relevance through authorised owners, then review supplier permissions and reporting obligations where a match exists.

Bottom line

Validate contractor data sharing without assigning impact to principals.

Evidence card B05 — 23 Feb 2026

ryhem | Forum | Forum | English

ORIGINAL

Data volume: [quantity removed] Price: $40,000

Note. Advertisement or demand only; the date is the post date. [S1]

Held

Two substantially matching contractor-bundle advertisements. [S1]

Not established

Substantially matching copies support repetition, not independent confirmation. The claimed agreement, data contents, industrial-system information and extent of access remain unverified.

CASE J

J

A wellness-service CRM claim

Evidence card B06 | 27 Feb 2026 | Forum | Healthcare and consumer services

Claim unverified

CLAIM	A 27 February advertisement claimed customer records attributed to a wellness service, with an asking price of 150 USD. The poster alleged that an employee had been deceived into enabling CRM access.
CHRONOLOGY	The retained post establishes when the offer appeared. It does not establish when the alleged employee interaction or data extraction occurred.
ESTABLISHED PROPOSITION	The seller described a dataset, a price and a proposed entry narrative. These are claims within one advertisement.
ALTERNATIVES AND LIMITS	A pasted schema does not validate the social-engineering account or continuing CRM access. Record count and identity-document claims remain unverified.
RESPONSE	Where the description matches internal data, review CRM permissions, support-assisted access and unusual exports. Preserve relevant session and administrative-change evidence before deciding the scope of containment.

Bottom line

Review CRM permissions and exports if an internal match exists.

Evidence card B06 — 27 Feb 2026

sexyskin | Forum | Forum | English

ORIGINAL

tricked employee to get me inside the CRM panel

Note. Advertisement or demand only; the date is the post date. [S1]

Held

Wellness CRM offer, asking price and claimed employee-deception narrative. [S1]

Not established

The entry method, record count and identity-document claims are not independently established. A pasted schema and sample cannot show continuing access or nationwide impact.

CASE K

K

A driver and permit-related data offer

Evidence card B07 | 19 Apr 2026 | Forum | Transport and public services

Claim unverified

CLAIM	An April offer described records with driver, identity, contact, licence and vehicle-related fields. The public role label covers a transport-data service rather than identifying a particular system.
CHRONOLOGY	Related records appear on 19 and 20 April. Copies and replies repeat the same advertised data theme.
ESTABLISHED PROPOSITION	The field descriptions and the advertised count are held as a claim. The displayed card provides no supporting quotation for those fields. Multiple posts do not establish multiple source incidents.
ALTERNATIVES AND LIMITS	The data could reflect an older collection, a supplier export or mixed sources. The forum title does not establish fresh access or unique people.
RESPONSE	Transport and data owners should compare the described relationships with authorised records. Inspect relevant bulk lookup or export activity if a match exists. Avoid attributing a source solely from familiar field names.

Bottom line

Validate driver-data relationships before attributing a system or counting people.

Evidence card B07 — 19 Apr 2026

Unnamed poster | Forum | Forum | English

ORIGINAL

No public excerpt displayed; field categories are summarised in Case K.

Note. Advertisement or demand only; the date is the post date. [S1]

Held

An offer and replies describing driver, licence and vehicle-related fields. No quotation substantiating those fields is displayed. [S1]

Not established

Repeated wording is one advertised dataset. The forum label does not establish a fresh incident, record uniqueness, target-system access or data provenance.

CASE L

L

Circulation of a public-sector document bundle

Evidence card B08 | 8 Jun 2026 | Forum | Public administration

Claim unverified

CLAIM	A June thread described an archive containing documents, notices, photographs and messaging material attributed to the public sector. The original description also asserted sensitivity.
CHRONOLOGY	Related posts appeared across 8 and 9 June. Different timestamp formats refer to the same circulation period and do not establish separate thefts.
ESTABLISHED PROPOSITION	The archive description circulated across forum records. The claimed classification and authenticity are not established by that description.
ALTERNATIVES AND LIMITS	Copies can repeat historical or mixed material. Archive size and the appearance of a document do not establish access to a production system or a new intrusion.
RESPONSE	Records and security owners should assess authenticity and current sensitivity through authorised channels. Review relevant document-sharing controls if corroborated. Do not download a circulated archive merely to reproduce the claim.

Bottom line

Assess authenticity and sensitivity; repeated archives are not new intrusions.

Evidence card B08 — 8 Jun 2026

Unnamed poster | Forum | Forum | English

ORIGINAL

Photos of docs + whatsapp chats

Note. Advertisement or demand only; the date is the post date. [S1]

Held

A document-archive description circulating across forum records. [S1]

Not established

An archive description does not prove authenticity, classification, production-system access or a new intrusion. The mirrors and replies are not independent incidents.

M

CASE M

A parcel-data release claim

Evidence card B09 | 15 Sep 2026 | Forum | Transport and logistics

Claim unverified

CLAIM	A September poster alleged a large parcel dataset described in lines and advertised a smaller portion. The description named sender and recipient field categories.
CHRONOLOGY	The retained post is dated 15 September. Its assertion of a 2026 event is not an independently established incident date.
ESTABLISHED PROPOSITION	The advertisement and its quantities are held. The quantities describe what the poster claimed, not a measured population of affected people.
ALTERNATIVES AND LIMITS	Lines, records, shipments and people are different units. Two parties per line cannot be multiplied into a unique-person total. Extraction, recency and any completed sale remain unverified.
RESPONSE	Delivery-service owners should validate origin against authorised transaction records. Assess customer-service impersonation risk and unusual data access if supported. Do not publish shipment identifiers or contact data during validation.

Bottom line

Treat shipment lines, records and people as different units.

Evidence card B09 — 15 Sep 2026

Unnamed poster | Forum | Forum | English

ORIGINAL

affecting both domestic and international shipments.

Note. Advertisement or demand only; the date is the post date. [S1]

Held

A parcel-data advertisement asserting line counts and sender/recipient fields. [S1]

Not established

Lines, records and people are different units. Two fields/parties per line do not establish twice as many unique people. No verified extraction, root cause, official response or completed sale is held.

CASE N

N

A contractor source-code and document archive claim

Evidence card B10 | 28 Sep 2026 | Forum | Construction and engineering

Claim unverified

CLAIM	A 28 September post described a contractor archive containing source code, project material, contracts and identity-document images. It described compressed and unpacked archive sizes, which are omitted here.
CHRONOLOGY	The post advertised circulation and included a separate assertion of persistence. It supplied no target-side evidence establishing when access began or ended.
ESTABLISHED PROPOSITION	The description, sizes and persistence assertion are held as the poster's statements. They do not validate archive contents.
ALTERNATIVES AND LIMITS	Source code can be copied without proving production access. A document bundle can come from shared storage or an older incident. Industrial-system impact is not established.
RESPONSE	Contractor security teams should validate ownership and review repository and document permissions. Investigate persistence through internal telemetry where supported. A public assertion does not justify testing any advertised access path.

Bottom line

Validate repository and document scope before investigating claimed persistence.

Evidence card B10 28 Sep 2026

Unnamed poster Forum Forum English

ORIGINAL

Free full leak includes:

Note. Advertisement or demand only; the date is the post date. [S1]

Held

A contractor code and document archive description with an unverified persistence claim. [S1]

Not established

The poster also claims persistence, which is unverified. Archive size and a content list do not establish successful intrusion, current access or industrial-system impact.

Each dossier ends at its evidence boundary. A credible internal match can change the response, but it does not retrospectively validate every detail in a seller's narrative.

4.7 Recent activity: 8–22 November

Recent activity combines different evidence types. The table does not add them into an incident total. A November publication may describe a warning, an advertisement or older material rather than a new intrusion.

The five-post count below and the monthly forum chart describe country-tagged material. Case P describes four posts in the wider retained material. Their overlap with the tagged population is not established here; do not add these counts. [S1]

Date	Evidence	Assessment	Immediate decision
8–22 November	5 country-tagged forum posts	Includes an ambiguous country-labelled collection and unrelated service/software posts; no new confirmed Saudi incident established	Check the stated topic and age before opening a new incident [S1]
9–10 November	Contractor session-access offer across four forum posts	One unverified access-advertisement dossier, distinct from the October archive claim	Validate relevant identities and supplier data responsibilities [S1]
9 November	N0n listing, education-labelled target	Criminal claim in Ransompedia	Validate any relevant service or supplier relationship [S2]
11 November	Thegentlemen listing, health-labelled target	Criminal claim in Ransompedia	Assess sensitive-data and continuity relevance without assuming confirmation [S2]
16 November	Aoqin listing	Criminal claim; the industry label differs from a public relay	Validate the business and country relationship [S2]

Date	Evidence	Assessment	Immediate decision
11–12 November	Microsoft and Google CERT alerts	Official patch advice, not Saudi exploitation evidence	Assign applicable asset owners and retain update evidence [S26][S27]
20 November	Veeam and GitLab critical alerts	Official warning entries	Verify vendor details and product applicability [S13]
21 November	Palo Alto Networks and Cisco critical alerts	Official warning entries	Review applicable edge and network assets [S13]

CASE P

P A November contractor session-access offer

Evidence card B19 | 9 Nov 2026 | Forum | Construction and engineering

Access offer, unverified

CLAIM

A seller advertised an active session associated with a construction contractor and described tender, financial and engineering material. The assertion that the material was current belongs to the seller. [S1]

CHRONOLOGY

Four retained forum posts appeared on 9 and 10 November. They form one offer dossier, rather than four established incidents.

ESTABLISHED PROPOSITION

The advertisements and their repeated scope descriptions are held. The seller asserted an access capability, beyond an ordinary static-data offer.

ALTERNATIVES AND LIMITS

No session, credential or advertised payload was tested. Usability, data authenticity, recency and target impact remain unverified. The construction theme does not establish a link to the separate October archive allegation.

RESPONSE

Relevant identity and supplier owners should assess account scope, authorised sessions and data-sharing responsibilities through internal records. If usable stolen material or unauthorised activity is evidenced, contain it immediately and preserve the reporting decision.

Bottom line

Validate the relevant identity and supplier relationship without testing advertised sessions.

Evidence card B19 9 Nov 2026

Unnamed seller Forum Forum English

ORIGINAL

including closed technical and financial tender proposals

Note. The claimed active session was not tested. This is separate from the October construction archive claim.

Held
Four posts advertise one contractor session-access offer and describe tender, financial and engineering material. [S1]

Not established
Usable session access, data validity, freshness, unique records, completed delivery or target impact.

The versioned example below comes from the vendor's 11 November PAN-OS advisory. It is not assigned to a Saudi incident. The NVD record was checked, and the affected and fixed releases were read in the vendor table. [S14][S15]

Vulnerability	Affected branch	Fixed release	Interpretation
CVE-2026-0326	PAN-OS 12.2 before 12.2.4-h2	12.2.4-h2 or later	Conditional service-processing issue
Same CVE	PAN-OS 12.1 before 12.1.10-h4	12.1.10-h4 or later	Check the vendor's configuration conditions
Same CVE	PAN-OS 11.2 before 11.2.16-h2	11.2.16-h2 or later	Confirm the installed branch
Same CVE	PAN-OS 11.1 before 11.1.16-h5	11.1.16-h5 or later	Older unsupported versions require a supported fixed release

The vendor describes service disruption or memory corruption under specified configurations. Its reviewed advisory says it is unaware of malicious exploitation. Panorama and Prisma Access are stated to be unaffected. Cloud NGFW customers should follow the vendor's maintenance instructions. [S14]

A patch advisory can justify action without establishing a Saudi attack. Close the task using actual asset, configuration and installed-version evidence. The report does not supply an exploit or a detection rule.

4.8 What the cases do and do not support

Together, the cases support practical investigation paths for sensitive data, accounts, suppliers and services. They do not establish a complete national victim list, unique criminal operators or an aggregate financial-loss figure.

A case can remain an unverified claim while still justifying a proportionate control review. The decision should record both its evidence and its limit. Where an internal match changes confidence, preserve the new evidence as a separate proposition.

KEY TAKEAWAYS

01

A post establishes circulation before it establishes target impact.

02

Recent listings, advisories and disclosures are separate populations.

03

Validate the account, data relationship or service before deciding containment and reporting.

CHAPTER 05

Targeting examples by sector

THIS CHAPTER ANSWERS

Which evidence matters to each service owner, and what should they do first?

10

sector cells in the portfolio; examples describe evidence, not sector risk ratings

5.1 Route the evidence to the service owner 42

5.2 Medical remote access is a distinct proposition 43

5.3 Data can cross sector boundaries without proving a shared incident 43

5.4 Use a closure criterion that fits the claim 44

CHAPTER 05

Targeting examples by sector

IN SHORT

Sector labels help route a finding to an owner. They do not establish prevalence or justify a rating. The strongest examples concern public-body code and document claims, health-related offers, investor data, contractor archives and transport records. Only the named mobile-app case has an official disclosure in these dossiers. Match a relevant observation to the actual data or service, then take the first action supported by that match.

5.1 Route the evidence to the service owner

The table shows examples and first responses. A blank incident finding for a sector must not be read as evidence that the sector was unaffected. [S1][S2][S17]

Sector	Observed example	Evidence status	First response
Public administration	Source-code, credential and document descriptions; service-disruption claims	Advertisements and claims, without target-side validation	Validate relevant code or document provenance and service status
Banking and financial services	Investor-data offer, account demand and credential campaigns	Seller statements and vendor reporting	Join identity, recovery and payment investigation paths
Insurance	Health-data service offer may concern connected workflows	Claimed data categories; no insurer-wide impact established	Check data-sharing relationships before assigning ownership
Energy and utilities	Contractor-document offers and an energy-data relay	Supplier claims and relayed quantity	Scope principal and supplier data separately
Industry and materials	Project and contractor archive descriptions	Authenticity and operational impact unverified	Review authorised engineering-document and repository permissions
Transport and logistics	Confirmed app disclosure; parcel and driver-data offers	One issuer disclosure; separate unverified offers	Assess customer-data access, supplier copies and impersonation
Digital services and communications	Account demand and telecommunications disruption claim	Demand or claim, not confirmed service access	Validate account pathways and independently measure availability
Health and life sciences	Health-data and wellness CRM offers; medical remote-access advertisement	Claims of data or access; no completed sale established	Validate sensitive-data scope and review privileged access

Sector	Observed example	Evidence status	First response
Education and research	Education-service disruption claims and feed listings	Claim sequences and listing observations	Separate public-site availability from student and staff data access
Consumer services, property and investment	Service impersonation and customer-data offers	Official scam notices and seller claims	Link support reports with trusted payment and recovery verification

5.2 Medical remote access is a distinct proposition

A 3 May forum advertisement offered remote access associated with a Saudi medical facility. The seller's description of scale and access was not validated. It is separate from the health-data offer in Case F. [S1]

Evidence card B15 — 3 May 2026

Unnamed poster | Forum | Forum | English

ORIGINAL

Huge medical facility

Note. Advertisement, demand or relay only.

Held

A seller advertised medical-facility remote access; no current access or transaction is validated. [S1]

Not established

Capability, delivery, completed transactions, current access or target-side impact.

The difference matters. A dataset claim calls for a provenance and disclosure assessment. An access advertisement also calls for an identity and remote-service investigation when a credible match exists. Neither claim, alone, establishes a patient-safety event or operational disruption.

5.3 Data can cross sector boundaries without proving a shared incident

A contractor's archive can contain documents involving energy or transport. A customer-data service can connect a healthcare provider and a financial workflow. The presence of several sector names does not establish that every organisation's own system was accessed.

The owner of the relevant contract or data flow should lead the first scope check. Security teams can then determine which systems, permissions and records need investigation. This avoids assigning a broad incident to every brand named in an advertisement.

5.4 Use a closure criterion that fits the claim

Finding	Closure evidence	What does not close it
Old data repeatedly advertised	Validated age, affected scope and prior remediation	Seller says fresh
Code or credential description	Internal provenance assessment and exposure decision	Forum reputation or a claimed com-plaint
Supplier document bundle	Confirmed data-sharing scope and supplier response	A principal's public service stays online
Remote-access offer	Identity/service assessment and relevant log review	No matching public breach statement
Disruption claim	Independently measured service status and affected functions	Actor says the attack ended

These are investigation outcomes, rather than a request to test external access or acquire advertised material. Every case can be assessed through lawful internal records and established supplier channels.

KEY TAKEAWAYS

01

Route each observation to a data, service or supplier owner.

02

A multi-sector advertisement does not establish a multi-sector intrusion.

03

Close the proposition with appropriate evidence, not with a seller's assurance.

CHAPTER 06

Hacktivism, disruption claims and service status

THIS CHAPTER ANSWERS

How should a defender respond when public claims outrun verified impact?

17

retained posts in nine claim sequences from one posting identity

6.1 A timeline with distinct evidence types 46
6.2 Relayed DDoS claims need an independent service account 47
6.3 Repeated claim sequences in the retained posts 47
6.4 Claim versus verified account 50
6.5 Operations and communications should share one fact record 50
6.6 Prepare a usable holding statement 50

CHAPTER 06

Hacktivism, disruption claims and service status

IN SHORT

Public disruption claims can create pressure before an organisation has established impact. Unit 42 relayed Saudi examples involving a financial-service website and a government service. The source account does not provide independently measured outage duration for these examples. Treat the claim as a signal to verify availability, authentication and data access separately. Prepare upstream mitigation contacts and a factual communications route, then test those routes with operations.

6.1 A timeline with distinct evidence types

The timeline distinguishes published research, official statements and own-source listing observations. It is not a sequence of confirmed intrusions. Dates are publication or listing dates, except where the entry explicitly says otherwise.

31 Mar 2026	**Check Point Research** Reports three March password-spray waves with limited Saudi targeting [S12]
16 Apr 2026	**Police notice** Reports action concerning fraudulent service advertisements, without a system-intrusion claim [S20]
9 Jun 2026	**Issuer disclosure** Confirms limited mobile-app customer-data access; impact statements remain the issuer's [S17]
6 Oct 2026	**The National** Relays an unverified construction-sector data claim [S19]
9 Nov 2026	**Ransompedia observation** A Saudi-labelled education listing appears; no official confirmation established [S2]
11 Nov 2026	**Ransompedia observation** A Saudi-labelled health listing appears; no official confirmation established [S2]
12 Nov 2026	**Saudi CERT** Publishes a Google security-update advisory [S27]
16 Nov 2026	**Ransompedia observation** A third recent Saudi-labelled listing appears; sector classification requires care [S2]
20 Nov 2026	**Saudi CERT** Lists critical Veeam and GitLab advisories [S13]
21 Nov 2026	**Saudi CERT** Lists critical Palo Alto Networks and Cisco advisories [S13]

6.2 Relayed DDoS claims need an independent service account

Unit 42's regional brief relayed a Sylhet Gang claim concerning government systems and a DieNet claim concerning a Saudi bank website. We use broad target categories because official confirmation of those alleged incidents was not established. [S11]

These are claims about targets, not proof of successful activity. The brief's separate airport example has a country inconsistency and is not used as Saudi evidence. No geographic or political conclusion is drawn from it.

A screenshot or remote availability check can help an analyst decide where to investigate. It cannot establish the user's experience, outage cause or access to protected data. A website may be reachable from one network and unavailable from another. Service operations should establish the affected functions from its own telemetry.

6.3 Repeated claim sequences in the retained posts

The retained material contains 17 posts from the 313 Team posting identity, grouped into nine claim sequences. They concern public services, financial services, education, an employee-facing application and a telecommunications service. These are claim sequences, not nine confirmed outages. [S1]

Post dates	Broad target	Observed statement type	Impact boundary
24 March	Public-facing service	Announced a disruption claim and intended duration	Duration unmeasured
25 March	Public-sector services	Two target-list posts	Target lists do not establish impact
6–8 August	Public-facing applications	Claim and follow-up posts	Internal access unverified
11–12 September	Public-facing services	Claimed disruption of internal servers	No target-side confirmation held
13 September	Financial service	Claim and follow-up	Customer impact unmeasured
14 September	Another financial service	Claim and follow-up	Customer impact unmeasured
18 September	Education service	Claim and updates	Service and data impact unverified
19 September	Employee-facing application	Announced disruption and intended duration	No verified employee-service outage
2 October	Telecommunications service	Announced disruption and intended duration	No verified network-wide effect

The follow-up language is part of the claim record. Repeated assertions about internal systems are not independent evidence of internal access. Intended attack durations must not be summed into total downtime.

Evidence card B11 — 24 Mar 2026

313 Team | Chat channel | Telegram | English

ORIGINAL

The attack will last for two hours.

Note. Claimed durations are not measured downtime.

Held
A self-published claim or update by the posting identity. [S1]

Not established
Actual outage duration, internal access or data theft.

Evidence card B12 — 6 Aug 2026

313 Team | Chat channel | Telegram | Arabic

ORIGINAL

سيستمر الهجوم لمدة 6 ساعات.

TRANSLATION

The attack will continue for 6 hours.

Note. Claimed durations are not measured downtime.

Held
A self-published claim or update by the posting identity. [S1]

Not established
Actual outage duration, internal access or data theft.

Evidence card B13 — 11 Sep 2026

313 Team | Chat channel | Telegram | English

ORIGINAL

The attack resulted in the disruption of internal servers

Note. Claimed durations are not measured downtime.

Held
A self-published claim or update by the posting identity. [S1]

Not established
Actual outage duration, internal access or data theft.

Evidence card B14 — 2 Oct 2026

313 Team | Chat channel | Telegram | Arabic

ORIGINAL

سيستمر الهجوم لمدة 24 ساعة.

TRANSLATION

The attack will continue for 24 hours.

Note. Claimed durations are not measured downtime.

Held
A self-published claim or update by the posting identity. [S1]

Not established
Actual outage duration, internal access or data theft.

CASE O

A repeated disruption campaign narrative (B11, B12, B13, B14)

Public and commercial services

Claim sequences, impact unverified

CLAIM

The 313 Team posting identity repeatedly claimed service disruption and described planned durations. One sequence asserted an effect on internal servers, without evidence from the target environment.

CHRONOLOGY

The retained sequences run from March through October. Updates within a sequence are follow-ups to the same claim context, not independent target confirmations.

ESTABLISHED PROPOSITION	The posts and the continuity of the posting identity are observed. They establish a repeated public claim narrative across several service categories.
ALTERNATIVES AND LIMITS	A public page may be unavailable without internal-system access. Maintenance, filtering or legitimate traffic can affect visibility. The report does not determine whether any of these claims caused a verified outage.
RESPONSE	Correlate edge-provider, service and authentication telemetry. Confirm the affected function and duration independently. If evidence concerns protected data or accounts, investigate that proposition separately from availability.

Bottom line

Keep stated attack durations separate from independently measured service impact.

The same separation applies to the early-March DieNet relay and a March payment-service claim attributed to Keymous Plus in retained reporting. They establish that claims circulated, rather than a common operator or verified customer impact. [S1]

Posts using the ServerKillers label on 12 September and the DARKSTORM label on 26 October also listed public-website targets. No independently measured impact is held for these examples. Several sites in one list do not establish several verified outages. [S1]

A separate Arabic relay attributed an energy-sector data claim to Handala. This is a secondary claim. It does not establish dataset authenticity, encryption, operational-technology impact or a target's confirmation. [S1]

Evidence card B18 4 Mar 2026

Unnamed poster Chat channel Telegram Arabic

ORIGINAL

[quantity removed] حوالي

TRANSLATION

About [quantity removed]

Note. Advertisement, demand or relay only.

Held
An Arabic news-style relay of a Handala energy-data claim. [S1]

Not established
Capability, delivery, completed transactions, current access or target-side impact.

6.4 Claim versus verified account

Point	Claim or report	Official account held	Independent boundary
Government-service disruption	A claim relayed by Unit 42	No incident confirmation held for this example	No measured service-impact conclusion [S11]
Financial website disruption	A DieNet claim relayed by Unit 42	No incident confirmation held for this example	No outage duration or transaction-impact conclusion [S11]
Construction data	A WallStreet allegation reported through a monitor	No substantive confirmation in the reviewed account	Claimed quantities remain unverified [S19]
Mobile-app customer data	Issuer disclosed unauthorised access	Limited customer-data incident confirmed by issuer	Financial-data and continuity limits are the issuer's statements [S17][S18]

The columns answer different questions. A lack of a held confirmation does not prove a claim false. An official statement about service continuity does not, by itself, establish that confidentiality was unaffected.

6.5 Operations and communications should share one fact record

The incident team needs a service-status record with time, affected function, supporting telemetry and known uncertainty. Communications should use that record. It should not estimate stolen-data volumes from an actor's headline or infer customer loss from traffic volume.

When an availability event is verified, engage the mitigation provider and the responsible service owner. Preserve the normal baseline so that a legitimate demand surge or maintenance issue remains a testable alternative. Do not delay recovery while deciding who wrote a public post.

When evidence points to data access, run a separate investigation. The distinction matters because a successful DDoS mitigation does not close a confidentiality incident. Similarly, a data-sale claim does not establish a need to declare an outage.

6.6 Prepare a usable holding statement

A holding statement should identify the service under assessment in terms customers understand, describe verified impact and give the next update point. It should avoid attribution until supported and approved. Sector-specific coordination requirements still apply (§10).

An exercise can test whether support, security, operations and communications produce the same account of events. The completion criterion is a consistent, telemetry-supported statement and an actionable escalation path. It is not agreement on the actor's political narrative.

KEY TAKEAWAYS

01

Treat disruption posts as claims until service evidence establishes impact.

02

Availability, data access and attribution need separate findings.

03

Rehearse mitigation contacts and factual communications with operations.

CHAPTER 07

Threat actors, claims and ransomware listings

07

THIS CHAPTER ANSWERS

Which identities appear in the evidence, and what relationships can be supported?

30

Saudi-labelled ransomware listings in the reporting window

7.1 Separate an identity from an operator 53
7.2 Source-attributed campaign research 54
7.3 Posting identities and hacktivist claims 55
7.4 Regional ransomware comparison 57
7.5 Listing identities and concentration 57
7.6 Use extortion evidence for continuity decisions 59

CHAPTER 07

Threat actors, claims and ransomware listings

IN SHORT

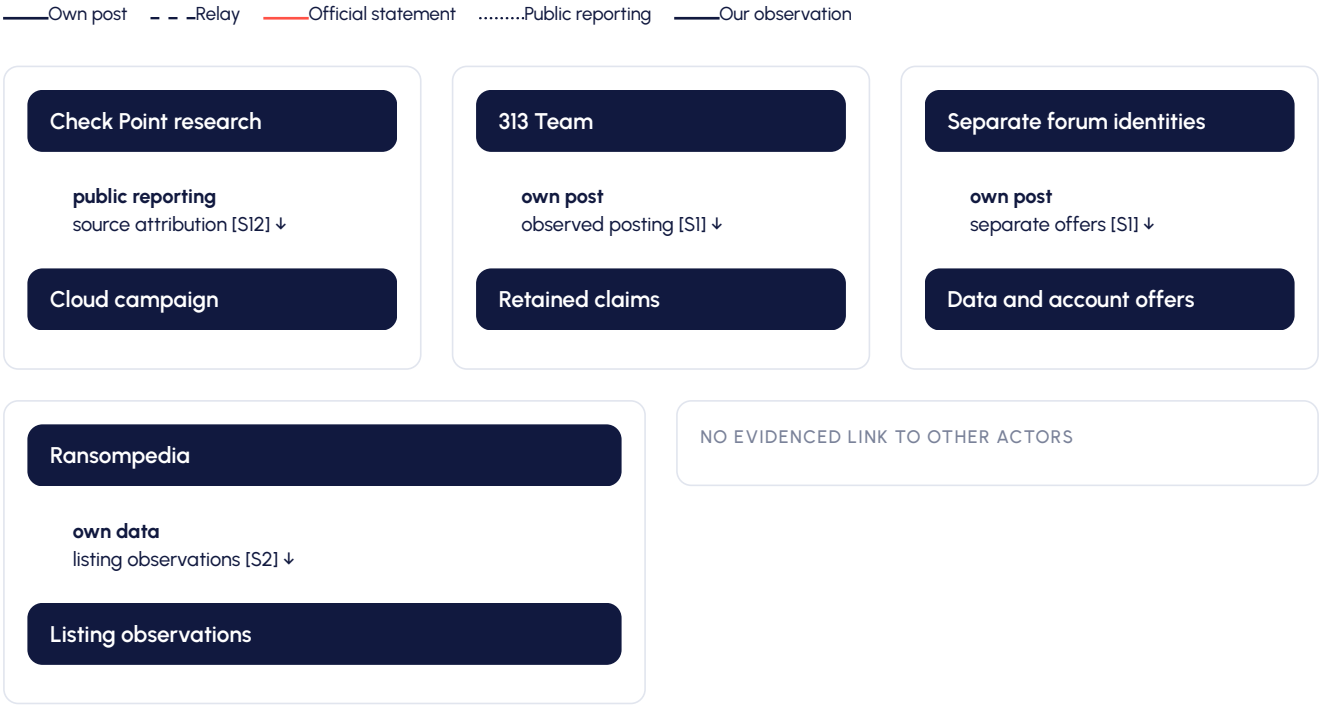
Ransompedia records 30 Saudi-labelled listings in the window. The UAE comparison has 84, Qatar 9, Kuwait 7 and Oman 9. These are feed observations of criminal claims, not confirmed incident rates. Actor names identify posting or listing identities; they do not identify operators by themselves. Keep vendor attribution attached to its source, and use each listing to test relevant continuity and identity-response plans.

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

7.1 Separate an identity from an operator

A forum account, a ransomware leak-site label and a campaign name are different kinds of entity. A repeated alias supports a posting association. It does not establish that the same person controlled every account or that a seller operated a reported intrusion campaign.

The relationship view below labels source relationships and planning links. The figure shows source relationships. Planning links discussed in the text are an analytical model, without an assertion of shared operators.



The link from Ransompedia to listing observations represents Brandefense's own data. It is not an independent public corroboration of each incident. The link from a research publisher to a campaign represents that publisher's report. [S1][S2][S11][S12]

7.2 Source-attributed campaign research

Unnamed cloud password-spray campaign

Campaign name follows the source description

Vendor-reported credential campaign | Origin assessed by Check Point as Iran, with moderate confidence

IN SAUDI ARABIA, 2026

3, 13, 23 March
Campaign waves; limited Saudi targeting

31 March
Research publication

CLAIMED TARGETS

Limited Saudi targets; no Saudi success count supplied

SEEN IN PUBLIC REPORTING

[S12] Check Point: three waves, with limited Saudi targeting and moderate-confidence origin assessment

OUR ASSESSMENT

The source establishes campaign activity against some Saudi targets. It does not establish successful access at every target.

CONFIDENCE
Vendor-observed targeting; Saudi outcomes unresolved

Check Point assessed the origin of the Microsoft 365 password-spray actor as Iran with moderate confidence. That attribution belongs to Check Point. Its account gives limited Saudi targeting, without establishing Saudi-specific successful access totals. [S12]

Microsoft's 2026 Digital Defense Report places Saudi Arabia at 2% of its Iran-related nation-state notifications between July 2025 and June 2026. The report also notes that state-linked actors combine long-term espionage and pre-positioning with potential disruption. That 2% share reflects vendor notifications to Microsoft customers rather than a national attack rate, and stays separate from the hacktivist claims in Chapter 6. [S33]

The technique mapping is an analytical model of the behaviour described by the source. It does not identify an actor or demonstrate that every step succeeded at a Saudi organisation.

TECHNIQUES NAMED IN THE VENDOR RESEARCH, BY TACTIC

Credential Access

T1110.003
Password Spraying: source-described behaviour, analytical model

Analytical model by Odin by Brandefense of the behaviour in Check Point research [S12], checked against MITRE ATT&CK [S30] on 22 November 2026; not an attribution or a confirmed full intrusion chain. [S12]

Tactic	Technique	Evidence	Defensive question
Credential Access	T1110.003, Password Spraying	Check Point describes attempts across many accounts using weak passwords; MITRE defines the technique	Which attempted accounts show suspicious successful sessions or follow-on activity?

MITRE's technique description and the source account support the behavioural mapping. The report does not add a complete intrusion chain or deployable detection rule. [S12][S30]

7.3 Posting identities and hacktivist claims

313 Team

Posting identity only

Disruption claimant | No state affiliation inferred in this report

IN SAUDI ARABIA, 2026

March
Claim sequences concerning public services

August
Application-related claims and updates

September
Public, finance, education and employee-application claims

October
Telecommunications-service claim

CLAIMED TARGETS

Broad public and commercial service categories

IN THEIR WORDS

"سيستمر الهجوم لمدة 6 ساعات." B12

SEEN IN PUBLIC REPORTING

[S1] 17 retained posts in nine claim sequences; impact unverified

OUR ASSESSMENT

Repeated claims and updates support a posting association. They do not establish measured downtime, internal access or common control with other identities.

CONFIDENCE
High for observed posting; target impact unverified

Separate forum sellers and buyers

Analytical model of evidence categories

Independent advertisements and demand | No shared organisation or operator established

IN SAUDI ARABIA, 2026

January–September
Data, document and account advertisements

February
Account demand and customer-data offers

CLAIMED TARGETS

Public administration, health, finance, transport and suppliers

IN THEIR WORDS

"Looking to buy any saudi-arabia related accounts" B03

SEEN IN PUBLIC REPORTING

[S1] Retained forum advertisements; no transaction or target-side confirmation

OUR ASSESSMENT

These are separate posting identities and product descriptions. The grouping organises defender tasks and does not describe one criminal organisation.

CONFIDENCE
High for observed offers and demand; advertised capabilities unverified

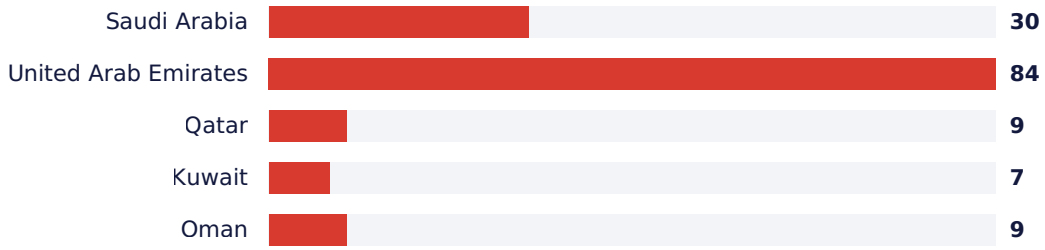
Posting identities can help analysts recognise repeated claims and follow-up offers. They should not become a reason to adopt an actor's claims about target impact or political affiliation. Chapter 6 tests disruption claims against a separate service-status question.

No concrete infrastructure or operational evidence here links the forum sellers, the password-spray campaign and the ransomware identities. The report does not present them as one organisation.

7.4 Regional ransomware comparison

The comparison uses the same source and date window across the five countries. The figure compares listing observations. It does not adjust for population, number of organisations, public disclosure practice or feed visibility. [S2]

Saudi-labelled listings sit below the UAE and above the three other Gulf comparators



Listings in the same source and date window; no adjustment for population or feed visibility and no national risk ranking. Source: Brandefense Ransompedia, 1 January–22 November 2026; November partial [S2]. Listings are source observations, not confirmed incidents.

Country	Listings	Interpretation
Saudi Arabia	30	Saudi-labelled entries
United Arab Emirates	84	Same source and window
Qatar	9	Same source and window
Kuwait	7	Same source and window
Oman	9	Same source and window

The four peers provide regional operating context. They cover energy, finance, logistics and digital services, with different organisational populations. A higher count is not proof of a higher probability of attack.

7.5 Listing identities and concentration

The retained Saudi listings use 18 distinct group labels. The largest is Thegentlemen, with 8 of 30 listings (26.7%). N0n has 3; Hyflock, APT73 and INC Ransom each have 2. The remaining labels appear once each. These are label frequencies, not counts of independent operators. [S2]

Ransompedia listing view

Separate leak-site identities

Own-data listing observations | No common operator inferred

IN SAUDI ARABIA, 2026

January–November
30 Saudi-labelled listings

8–22 November
3 recent listings

CLAIMED TARGETS

Feed-labelled sectors; country and legal-entity identity require care

SEEN IN PUBLIC REPORTING

[S2] 30 listings, including 8 under Thegentlemen; these are criminal claims

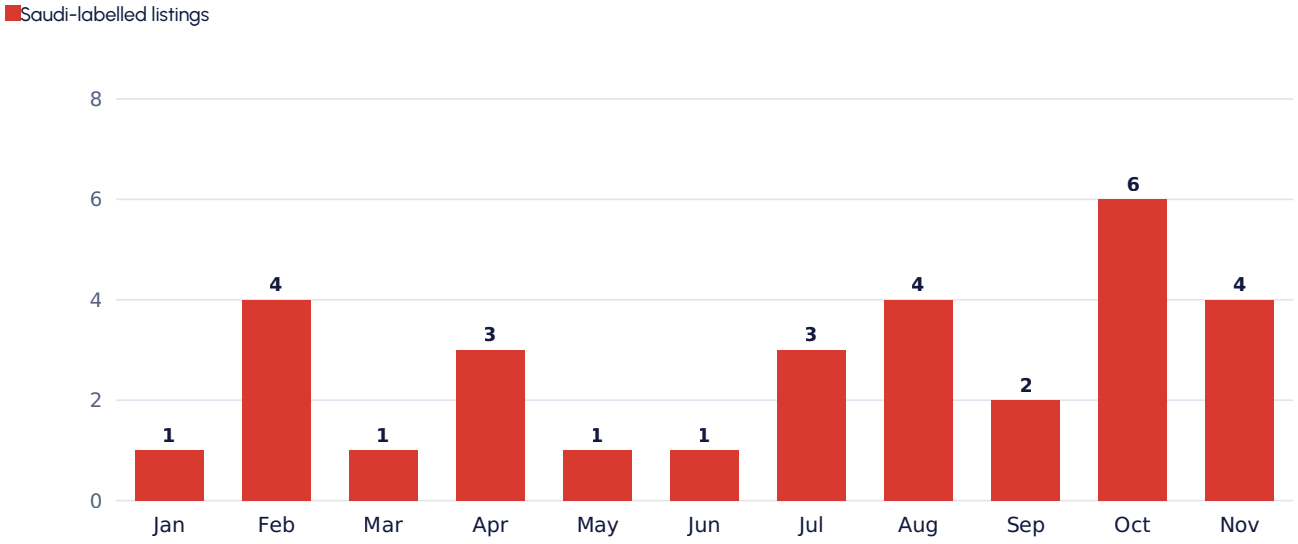
OUR ASSESSMENT

Listing frequency supports scoped continuity review. It does not establish intrusion, encryption, financial loss or independent operator counts.

CONFIDENCE
High for retained feed entries; target outcomes unverified

The date distribution contains 6 listings in October and 4 in November through the cut-off. Three November entries fall within 8–22 November. The report does not infer a growth rate from the current partial month.

Listings appear throughout the window, with six in October



Source: Brandefense Ransompedia, 1 January–22 November 2026; November partial [S2]. Listings are source observations, not confirmed incidents.

The feed's sector fields are descriptive labels supplied with the listings. Some need validation, particularly where a trading or service business is classified under another industry. A domain label also needs country validation before becoming a claim about a Saudi legal entity.

The listings carry 29 different target labels. That is not a verified count of independent Saudi organisations. Related brands, repeated victims, suppliers and country-label errors can affect the interpretation. The report therefore retains the listing count as its primary unit.

7.6 Use extortion evidence for continuity decisions

A relevant listing should prompt a scoped assessment: do the named data categories or services connect to the organisation, and is there corroborating internal or supplier evidence? Operations should verify service status. Identity teams should investigate usable authentication material where indicated. Privacy teams should assess personal-data scope.

Backups deserve a separate readiness test. An advertised dataset does not establish that systems were encrypted, and a successful restore does not establish that data was not disclosed. A useful incident record keeps those conclusions apart.

KEY TAKEAWAYS

01

Posting and listing labels do not identify independent operators.

02

The Gulf comparison measures feed listings, with distinct country populations.

03

Validate the affected relationship and test recovery without treating claims as confirmed impact.

CHAPTER 08

The fraud economy visible in the evidence

THIS CHAPTER ANSWERS

What do account demand, customer-data offers and official scam notices tell a defender?

2

asking prices retained as examples, without evidence of completed sales

8.1 Demand is visible before supply is established 61
8.2 Customer data can support a fraud hypothesis 62
8.3 Card material in posts: a narrow view 62
8.4 Asking prices do not measure a market's value 63
8.5 Official notices describe a seasonal scam route 63
8.6 Keep the fraud chain as a planning model 64

CHAPTER 08

The fraud economy visible in the evidence

IN SHORT

The evidence shows demand for Saudi-related accounts and advertisements for customer, investment, transport and supplier data. It also includes official notices about fraudulent seasonal services. These are distinct observations, with different links to financial harm. A price is an asking price; a request is demand; a dataset description is a claim. Connect support, fraud and identity teams around the customer journey, and validate any affected account or transaction.

8.1 Demand is visible before supply is established

The buyer request in Case G sought ready and checked accounts associated with Saudi services. It establishes demand for an account capability. It does not establish supply, an account owner or a completed transaction. [S1]

That distinction affects the response. A demand post can justify reviewing recovery controls and supplier access. It cannot identify an account to disable. Teams need a match to an actual identity or credible abusive activity before taking a targeted containment action.

Seller descriptions can combine several products: account access, identity information, contact lists and document archives. The report does not treat every item as a usable access product. The offer itself is the observed event.

The request in Case G is complemented by a Russian-language service advertisement offering mule account holders across Saudi Arabia and other markets. An Arabic post also sought a payment-receiving account and proposed a commission. Neither establishes a completed transaction or bank-system access. [S1]

Evidence card B16 — 18 Jul 2026

FandyUAE | Forum | Forum | Russian

ORIGINAL

Есть много дропов по ОАЭ, Сауди и другим арабским странам.

TRANSLATION

There are many drops (mule account holders) for the UAE, Saudi Arabia and other Arab countries.

Note. Advertisement, demand or relay only.

Held
A multi-country service advertisement offering mule account-holder provisioning. [S1]

Not established
Capability, delivery, completed transactions, current access or target-side impact.

Evidence card B17 — 3 Apr 2026

Unnamed poster | Chat channel | Telegram | Arabic

ORIGINAL

رجاء يكون شخص مستقبل و عنده توثيق و سمعة

TRANSLATION

Please be a receiving account holder with verification and reputation.

Note. Advertisement, demand or relay only.

Held
A demand post for a payment-receiving account; completion is not established. [S1]

Not established
Capability, delivery, completed transactions, current access or target-side impact.

8.2 Customer data can support a fraud hypothesis

The investment, wellness and parcel dossiers describe different field categories. If authentic and current, such material could help a fraudster tailor a message or impersonate a service. That is a conditional analytical model, rather than evidence that those advertisements caused a particular fraud loss. [S1]

A support team may hold the first useful evidence. A customer can describe an unexpected recovery call, payment request or change to contact details. The support record should preserve the message safely and connect to the identity or fraud case when appropriate.

Do not ask customers to send credentials or payment-card details through ordinary support messages. Provide a trusted service route and use internal transaction references. Public evidence cards deliberately omit personal data and shipment identifiers.

8.3 Card material in posts: a narrow view

SCOPE OF THE CARD FIGURES

These limited payment-card observations do not establish current validity, completed fraud, issuer-system compromise or national fraud losses.

The retained content from 1 January to 22 November 2026 contains 337 distinct Saudi-associated card records across 386 posts. A distinct card record is one unique payment-card number tied to a Saudi issuer prefix; one record may be repeated across several posts, and a single post may list multiple records. These observations do not support an issuer-security ranking, and they do not establish current validity or a fraud transaction. [S5]

8.4 Asking prices do not measure a market's value

The two examples below are seller statements. They do not show that a buyer paid, that the material was delivered or that the quantities were genuine. [S1]

Dossier	Advertised quantity	Asking price	Established boundary
Contractor bundle, Case I	Contractor document bundle	40,000 USD	Repeated advertisement; agreement and sale unverified
Wellness CRM, Case J	Claimed customer records	150 USD	Claimed count and entry narrative unverified

The prices cannot be compared as reliable unit costs. The advertised products, data categories, claimed sensitivity and credibility differ. Neither the low price nor the high price establishes authenticity.

A defensive budget should follow business criticality and validated exposure. Dividing an asking price by a claimed record count would add apparent precision without establishing the product's quality, reach or financial impact.

8.5 Official notices describe a seasonal scam route

Official police notices on 16 and 23 April, and 3 and 19 May, described false service advertisements on social media. The 10 May notice described fake services and counterfeit wristbands; it did not explicitly identify social-media advertising. [S20][S21][S22][S23][S24]

These notices describe arrests and referrals, rather than convictions or confirmed system intrusions. Their security relevance is the route from a trusted service theme to a payment or identity request. No conclusion about the underlying public-service policy is necessary.

Service owners should make the legitimate purchase and support routes easy to verify. Customer warnings should name the unsafe behaviour, such as acting on an unsolicited payment instruction, and direct users to a known channel. They should avoid reproducing an active criminal link.

8.6 Keep the fraud chain as a planning model

Possible stage	Supporting observation	What remains unestablished	Defensive owner
Acquire identity context	Advertised customer and document data	Authenticity, current scope and a buyer	Data and privacy
Obtain an account capability	Buyer demand and access narratives	A completed transaction or valid access	Identity
Impersonate a service	Vendor research and official scam notices	A link to any specific seller dossier	Digital risk and support
Request or redirect payment	Billing and investment lures in research	National loss or success rate	Fraud operations
Reuse material	Reposts and replies in the corpus	File identity or common operators	Threat intelligence

This is an analytical model of investigation tasks. It is not an observed end-to-end criminal operation. A concrete account, transaction or supplier match is needed to join cases operationally.

KEY TAKEAWAYS

01

Advertised demand, offered data and completed fraud are different findings.

02

The card view is narrow and cannot measure fraud loss.

03

Join support, identity and fraud evidence around verified customer events.

CHAPTER 09

Banking and financial services deep dive

09

THIS CHAPTER ANSWERS

How should a financial organisation connect identity signals, customer-data claims and payment controls?

25

assessed financial-service domains in the selected portfolio

9.1 Keep the financial populations separate 66
9.2 Financial-domain exposure 66
9.3 Account recovery can change a payment decision 67
9.4 SAMA's 2026 applicability matters 67
9.5 A financial-service investigation should preserve the chain 68
9.6 Questions for the financial CISO 68

CHAPTER 09

Banking and financial services deep dive

IN SHORT

The portfolio's financial cell includes banks and other financial services. Its 25 domains have complete exposure results, but they cannot supply a bank-only denominator. The useful evidence is more specific: an investor-data offer, account demand, reported credential attacks and SAMA's control requirements. Test how recovery, new access and payment instructions interact. Escalate when an actual account or transaction provides corroboration, and preserve the reporting decision.

9.1 Keep the financial populations separate

Population	Available finding	What it cannot establish
Selected finance domains	25 assessed domains; 12 associated with current credential listings	Independent bank count or national prevalence
Investment-data advertisement	Around 7,000 claimed records in one dossier	Verified investors, balances or financial loss
Buyer account request	A demand post concerning Saudi services	Supply, validity or a completed account sale
Payment-card observations	Limited observations described in §8.3	Issuer security or national card-fraud loss
Credential campaigns	Vendor reports of Saudi-directed activity	Saudi-wide account-access success rate

The investment-data claim concerns a financial-service context. It does not establish a banking-system incident. Similarly, a bank brand used in a phishing lure does not establish access to the bank's own systems. [S1][S11][S12]

No issuer ranking is published here. The observations do not establish affected-customer counts or issuer security. Fraud and support decisions require evidence concerning an actual customer or transaction.

9.2 Financial-domain exposure

The 25 assessed finance domains contain at least 104,791 device associations, including 332 employee-device associations, and 58,177 credential-record associations. Current credential listings concern 12 domains. These observations do not establish bank-system intrusions, active stolen accounts or affected-customer counts. [S3]

Payment-card observations remain subject to the limits in §8.3. They do not establish present validity, fraud, issuer-system access or responsibility for a device infection. [S5]

A finance owner should separate employee-device validation from customer account protection. The next step is to establish account relevance and freshness within authorised records. Fraud and support teams need transaction and customer evidence before deciding whether a financial event occurred.

9.3 Account recovery can change a payment decision

A useful internal review starts with a synthetic customer journey. Test a legitimate recovery request, a change to contact details, a new device and a new payment destination. Determine which team sees each event and whether evidence follows the case between teams.

The test should be authorised and avoid real customer data. Its result is evidence about that tested journey. It is not proof that every form of impersonation is prevented.

MFA is one part of the assessment. Teams should also inspect existing sessions, recovery paths and the authority behind payment instructions. Its presence alone should not close an investigation into usable stolen authentication material or suspected session abuse.

9.4 SAMA's 2026 applicability matters

SAMA's Counter-Fraud Fundamental Requirements became effective on 13 April 2026. Their scope addresses finance companies and payment-service providers according to the stated entity and service provisions. The separate banking Counter-Fraud Framework should not be described as newly created by that date. [S9]

The Fraud Prevention requirements call for risk-based authentication, including MFA for higher-risk actions such as registration, payments, credential reset and loan-disbursement instructions. They also address verification of customer identity and third-party risk. [S10]

For a member organisation, the task is to map the applicable rules to its services. Legal scope cannot be inferred merely because a domain is in this report's finance cell. The regulatory liaison should confirm SAMA's applicability notification and the relevant reporting and communications instructions (§10).

9.5 A financial-service investigation should preserve the chain

Signal	First check	Trigger for escalation	Record to retain
Investor-data offer	Relevant fields and lawful data-sharing relationships	Credible match to protected records	Scope, source assessment and privacy decision
Suspicious recovery	Customer authorisation and support actions	Unapproved change, usable stolen material or abusive session	Recovery and authentication chronology
New payment instruction	Trusted verification and related account changes	Failed verification or credible fraud evidence	Payment disposition and customer contact
Credential campaign indicator	Accounts, attempts and successful sessions	Corroborated suspicious access or follow-on activity	Identity and application evidence
Relevant extortion listing	Business and supplier relationship	Internal or supplier confirmation, or credible matching material	Continuity, confidentiality and notification assessments

The table describes proposed response logic. It does not claim that every signal occurred at a bank in the reporting window.

9.6 Questions for the financial CISO

Ask whether the organisation can link a support interaction to the following account and payment events. Ask whether a night-shift analyst can reach a decision-maker who can contain access and protect a transaction. Ask whether the reporting route can operate before a complete forensic conclusion exists.

Completion evidence should include a tested case, the responsible owners and the retained decision record. A dashboard showing more alerts cannot substitute for that evidence.

KEY TAKEAWAYS

01

Finance domains, bank customers and card observations are separate populations.

02

Test recovery and high-risk payment changes as one customer journey.

03

Confirm SAMA applicability and preserve evidence for each escalation and reporting decision.

CHAPTER 10

Regulatory and national response

10

THIS CHAPTER ANSWERS

Which obligations belong in the incident plan, and who owns each decision?

72 hours

maximum authority-notification period for qualifying personal-data incidents, measured from awareness

10.1 Applicability comes before the deadline 70
10.2 Keep the notification routes distinct 71
10.3 Evidence should follow the control owner 71
10.4 Enforcement and warning notices have different meanings 72
10.5 Turn compliance into a tested response 72

CHAPTER 10

Regulatory and national response

IN SHORT

Several reporting duties can apply to the same event. NCA controls address cybersecurity incidents. SAMA has sector-specific notification requirements. The personal-data regulation makes the authority-notification deadline conditional on potential harm or affected rights and interests. Their scope, triggers and recipients differ. A fraud warning is not itself a reportable breach. Assign legal and operational owners, document the awareness time, and exercise the applicable reporting routes before an incident.

10.1 Applicability comes before the deadline

The following table is a working allocation guide. It does not replace advice on an entity's legal position. A supplier's contractual duty may arise before its own regulatory reporting duty.

Entity	Relevant instrument	First check	Accountable owner
Government or in-scope critical-infrastructure entity	NCA Essential Cybersecurity Controls	Confirm scope, incident classification and regulator instructions	CISO and compliance
Bank subject to SAMA framework	SAMA Cyber Security Framework and relevant banking rules	Confirm current incident classification and notification route	CISO and regulatory liaison
Finance company or payment provider	Counter-Fraud Fundamental Requirements and applicable cyber rules	Confirm licence, service, SAMA applicability notification and additional-control applicability	Fraud leader and compliance
Controller of personal data	PDPL and Implementing Regulation	Assess potential harm and rights or interests affected	Privacy officer and counsel
Outsourced service provider	Applicable regulation and customer contracts	Identify affected customers, contract clocks and reporting dependencies	Service owner and legal

The ECC scope covers government entities and affiliated companies, as well as private entities owning, operating or hosting critical national infrastructure. Other entities are encouraged to use the controls. Applicability should be documented rather than inferred from a sector label. [S6]

NCA's published CSCC 2:2026 complements ECC-2:2024 for critical systems. Its scope covers national owners or operators of systems meeting the document's criteria, including public and private entities. Determine system-level applicability alongside the baseline; no new effective date is inferred here. [S31]

The table is not an exhaustive legal inventory. Sector, cloud, operational and other applicable instruments still need an entity-specific review.

10.2 Keep the notification routes distinct

The core provisions read for this report are set out below. No uniform deadline is inferred for all cyber events.

Instrument	Verified provision	Practical task	Limit
ECC-2:2024	Incident response plans, classification and reporting to NCA	Keep an NCA escalation route in the incident plan	This provision does not supply a universal 72-hour clock
SAMA Cyber Security Framework, 3.3.15	Immediately inform SAMA's IT Risk Supervision when an identified incident is medium or high; seek no-objection before related media interaction	Couple classification, regulatory liaison and communications	Confirm the applicable current instructions for the member organisation
PDPL Implementing Regulation, Article 24	Notify the competent authority within 72 hours of awareness when potential harm or affected rights/interests meet the provision	Record awareness, scope, risk, containment and notice decisions	Incomplete information must follow as soon as possible with reasons for delay
Article 24, affected individuals	Notify the data subject without undue delay where its harm condition applies	Prepare clear individual notices and safe contact channels	The authority deadline is not a substitute for this separate duty
Counter-Fraud Fundamental Requirements	Effective 13 April 2026; applies according to the defined member and service scope	Map products and licences to required controls	Do not describe it as a new framework for every bank

These provisions come from the official texts. The SAMA banking framework predates 2026. The Fundamental Requirements were issued in 2025 and became effective in 2026. Their publication and effective dates must not be interchanged. [S6][S7][S8][S9]

10.3 Evidence should follow the control owner

A reporting decision needs a defensible factual basis. Record what was known, when it became known, the data involved, likely harm and the responsible decision-maker. Update the assessment as evidence changes. A public claim may be the starting signal without yet establishing unauthorised access.

For privacy, avoid waiting for a final forensic report before assessing the notification condition. For service disruption, distinguish customer impact from the availability of a public homepage. For fraud, preserve the transaction chronology and the approval journey separately from the marketing message.

Counsel should prepare a short decision record with the CISO and fraud leader. It should show the applicable instruments, the chosen routes and the reason for any decision not to notify. This report makes no claim that a notification was sent in any case it describes.

10.4 Enforcement and warning notices have different meanings

On 16 January, the official news agency reported that SDAIA committees issued 48 decisions during the previous year. The statement concerned personal-data handling, safeguards and marketing practices. These are prior-year administrative decisions, not a tally of 2026 cyber incidents. [S25]

Official police notices in April and May concerned fraudulent services and permit-related schemes. Four mentioned social-media advertising. The 10 May notice described fake services and counterfeit wristbands. They are evidence of enforcement notices about scams. They do not establish entry into the information systems of the organisations impersonated. [S20][S21][S22][S23][S24]

The practical lesson is to join customer support with security. A customer who reports a false service advertisement should reach a team that can preserve the message, assess payment exposure and direct the customer safely. The report offers no comment on the underlying public-service policy.

10.5 Turn compliance into a tested response

Test	Owner	Evidence of completion
A claim arrives outside office hours	Incident commander	Timed acknowledgement and recorded classification decision
Customer data may have been accessed	Privacy officer	Awareness time, harm assessment and route decision
Payment changes follow a support interaction	Fraud leader	Linked case record and transaction review
A supplier reports an exposure	Third-party risk owner	Data-sharing scope and customer-notification dependencies
Public statements become necessary	Communications and regulatory liaison	Approved factual statement and required regulator coordination

KEY TAKEAWAYS

01

Scope and notification triggers differ across NCA, SAMA and privacy requirements.

02

Preserve awareness time and uncertainty without waiting for every forensic answer.

03

Exercise the reporting and communications routes with named owners.

CHAPTER 11

Outlook

11

THIS CHAPTER ANSWERS

Which judgements are supported, and which signals would change the response?

3

conditional planning scenarios, without probability estimates

11.1 Key judgements 74

11.2 Signals that would change the assessment 75

11.3 Conditional scenarios 75

11.4 What leadership should measure next 76

CHAPTER 11

Outlook

IN SHORT

Identity abuse, customer-facing fraud and extortion claims require different evidence and response paths. Current reporting supports preparing for each; it does not establish their national frequency or a forecast of loss. The strongest judgement concerns process: validate the account, service or dataset before describing impact. Treat the scenarios below as planning assumptions. Assign an owner and a signal that would start, change or stop each response.

11.1 Key judgements

Confidence refers to the stated proposition. It is not a rating of a seller, country or organisation.

Judgement	Confidence	Basis	Limit
Credential attacks deserve a standing investigation route	High for the need to investigate	Saudi phishing and password-spray activity reported by two research teams	Neither provides a national Saudi success rate
Public extortion claims justify continuity preparation	High for planning relevance	Ransompedia listings in the window	A listing does not establish intrusion, encryption or loss
Supplier data claims can require a customer-data review	Moderate as a conditional risk	Construction and other business-data claims	File authenticity, ownership and access route may remain unknown
Service impersonation requires fraud and support coordination	High for operational relevance	Vendor reporting and official fraud notices	Notices do not quantify national fraud prevalence
The selected portfolio cannot support a national exposure estimate	High	Purposive domains and 249 complete exposure assessments	No statistical inference beyond the defined observations

The first judgement does not require evidence of a completed attack at every organisation. It requires a credible route from a signal to a decision. The owner should establish whether an account exists, whether access is usable and whether suspicious activity followed. [S11][S12]

The second judgement concerns readiness, not a prediction that a listed organisation will experience downtime. A restore test can be justified by business criticality without adopting a criminal group's account of events. [S2]

11.2 Signals that would change the assessment

New evidence	What changes	First owner action
A matching active account and suspicious session appear	Listing moves from market observation to an internal incident lead	Identity team preserves logs and assesses containment
A controller or regulator confirms data access	Public claim becomes a confirmed disclosure within its stated scope	Privacy officer updates risk and reporting decisions
A sample's fields match authorised internal records	Authenticity assessment strengthens for those records	Data owner checks provenance without downloading advertised material
Service telemetry shows disruption during a claim	Availability impact can be measured independently	Operations records duration and affected functions
An old dataset is shown to have been remediated	Repeated advertising need not trigger the same disruptive response	Incident team links the claim to prior closure evidence
A supplier confirms a narrower scope	Partner exposure assessment can narrow	Third-party owner updates the data-sharing inventory

No single signal identifies the operator. A reused alias, matching headline or shared venue does not establish common control. Where relationships remain hypothetical, the report labels them as an analytical model.

11.3 Conditional scenarios

Scenario A: an advertised account is still usable

This planning assumption applies when an identity or remote-access signal appears. The trigger is internal evidence of usable stolen authentication material or unauthorised activity. The identity team should contain the affected access and preserve evidence immediately. A historic record alone does not establish that trigger. Close the targeted investigation when account and session evidence supports the disposition and any required remediation is verified.

Scenario B: a public claim coincides with service pressure

The trigger is independent evidence of customer impact, unusual traffic or unauthorised change. Operations should engage the agreed mitigation and recovery route. Communications should publish only facts cleared through the incident process. A claim screenshot alone does not establish downtime. End the heightened availability response when measured service functions meet agreed recovery criteria. Keep unresolved data or identity investigations open.

Scenario C: a supplier-held dataset appears in an offer

The trigger is a credible connection to the organisation's own data or contract. The supplier-risk and privacy teams should establish which records were shared and what customers may be affected. A project name in an advertisement does not establish access to a principal's network. Close the supplier workstream when data owners establish scope and verify required remediation, or document why the material does not match. Retain an unresolved decision otherwise.

11.4 What leadership should measure next

Measure completed decisions rather than the volume of alerts. Useful outcomes include time to a listing disposition, time to contain usable access, restoration evidence and the fraction of critical suppliers with tested notification routes. These are proposed management measures, not claims about current Saudi performance.

An improvement in these measures is evidence of a more reliable response process. It is not, on its own, evidence that attack attempts declined. The same distinction applies when fewer posts appear in a later period.

KEY TAKEAWAYS

01

Confidence belongs to a proposition, with a clear supporting source.

02

Conditional scenarios need observable triggers and a stopping condition.

03

Measure validated access, customer impact and completed response decisions.

CHAPTER 12

Action plan

12

THIS CHAPTER ANSWERS

What should start now, and what evidence should leaders expect over 30, 60 and 90 days?

15

owned actions with explicit completion evidence

12.1 Immediate triggers and a 30/60/90 programme 78

12.2 By role 80

12.3 Validation paths for the SOC 81

12.4 How Brandefense can help 82

CHAPTER 12

Action plan

IN SHORT

Begin with identity triage, customer-data response and continuity. These are supported by the reported credential campaigns, the confirmed mobile-app disclosure and public extortion listings. The schedule builds lasting capability. It never delays containment, customer protection or mandatory reporting when a credible incident appears. Give each action one accountable owner and a record showing what was tested. Review unresolved evidence with leadership rather than closing a ticket on an assumption.

12.1 Immediate triggers and a 30/60/90 programme

The programme starts when the organisation adopts it. Any credible evidence of usable stolen access, unauthorised activity or customer harm triggers the incident process immediately. The day ranges below are implementation targets proposed by this report. They are not statutory deadlines.

10–30

A01: Establish a route for market and device-association alerts; test an authorised synthetic alert and validate received signals

ACCOUNTABLE OWNER
Identity leader

COMPLETION EVIDENCE
Monitored domain scope, tested on-call handoff and dispositions for received alerts

A02: Where usable stolen authentication material or suspicious access is found, contain affected access immediately

ACCOUNTABLE OWNER
Incident commander

COMPLETION EVIDENCE
Session and account actions, retained logs and a documented recovery decision

A03: Review enterprise login and recovery journeys against phishing and password-spray evidence

ACCOUNTABLE OWNER
Identity engineering

COMPLETION EVIDENCE
Tested authentication paths, exception register and monitored sign-in events

A04: Map mobile-app customer data and test access separation with authorised test accounts

ACCOUNTABLE OWNER
Application owner

COMPLETION EVIDENCE
Approved data-flow map and recorded access-control test results

A05: Exercise one critical restore and establish initial legal applicability and the incident-notification decision tree

ACCOUNTABLE OWNER

Continuity leader

COMPLETION EVIDENCE

Restore evidence, legal/compliance-approved entity/instrument/recipient/trigger map, awareness-time record and current reporting contacts

231–60

A06: Establish sustained monitoring of service and supplier impersonation

ACCOUNTABLE OWNER

Digital-risk owner

COMPLETION EVIDENCE

Monitored scope, escalation path and a sample case taken through closure

A07: Assess email authentication without inferring missing observations are absent controls

ACCOUNTABLE OWNER

Messaging owner

COMPLETION EVIDENCE

Validated policies for sending domains and documented exceptions

A08: Join support, identity and payment-fraud cases when events concern the same transaction

ACCOUNTABLE OWNER

Fraud leader

COMPLETION EVIDENCE

Case-linking process and an end-to-end synthetic recovery test

A09: Review critical supplier data-sharing and notification dependencies

ACCOUNTABLE OWNER

Third-party risk owner

COMPLETION EVIDENCE

Data categories, access responsibilities and tested escalation route per critical supplier

A10: Rehearse independent service-status verification during an extortion or DDoS claim

ACCOUNTABLE OWNER

Operations leader

COMPLETION EVIDENCE

Telemetry-backed status, mitigation contact and approved factual communications

361–90

A11: Audit the initial NCA, SAMA and personal-data applicability map established under A05

ACCOUNTABLE OWNER

Compliance leader

COMPLETION EVIDENCE

Approved instrument-to-entity map and tracked remediation owners

A12: Test high-risk payment and account-recovery changes with safe synthetic scenarios

ACCOUNTABLE OWNER

Fraud engineering

COMPLETION EVIDENCE

Detection results and evidence that unauthorised changes are stopped or escalated

A13: Remove unnecessary supplier access and reduce shared administrative dependencies

ACCOUNTABLE OWNER

Infrastructure leader

COMPLETION EVIDENCE

Reviewed privileges, documented exceptions and recovery test

A14: Close a sample of advisory tickets against actual asset and version evidence

ACCOUNTABLE OWNER

Vulnerability leader

COMPLETION EVIDENCE

Applicable assets, remediation confirmation and accepted exceptions

A15: Review unresolved claims and prior incident remediation with leadership

ACCOUNTABLE OWNER

CISO

COMPLETION EVIDENCE

Decision register, overdue owners and lessons incorporated into response plans

Actions A01 and A02 are different. Monitoring establishes visibility; containment responds to validated risk. An old credential record, a customer-domain association or a market headline alone should not be treated as proof of a currently usable employee account.

Actions A04 and A08 also address different boundaries. The app owner controls access to stored data. Fraud teams assess the person, device and payment journey. A successful app test does not establish that support recovery or a new-payee flow is safe.

12.2 By role

Role	First decision	Ask for	Avoid
Board and executive team	Fund the response capabilities justified by business criticality	Evidence from A05 and the unresolved register in A15	Treating an alert count as a loss estimate
CISO	Establish one incident command route across technical and business teams	A01–A03 owners and escalation evidence	Declaring a public claim resolved without a factual assessment
SOC	Separate attempted authentication from successful sessions and follow-on activity	Tenant sign-in, mailbox, remote-access and service telemetry	Blocking every shared service solely because it appears in research

Role	First decision	Ask for	Avoid
Identity team	Determine whether the signalled account and authentication material are usable	Account scope, session evidence and prior remediation	Assuming MFA status settles the investigation
Fraud and customer support	Protect affected transactions and give customers a safe response channel	Linked chronology, consent and payment change evidence	Sending a customer back to the suspicious message
Privacy and legal	Determine notification conditions and preserve the decision chronology	A05 and A11 records	Waiting for perfect technical certainty before assessing duties
Procurement and suppliers	Confirm which shared data and access are relevant	A09 and A13 evidence	Treating a contractor claim as proof every partner was accessed

12.3 Validation paths for the SOC

These are investigation questions, not deployable detection rules. They require locally authorised telemetry and tuning.

Signal	Validate first	Escalate when	Closure record
Many accounts fail authentication	Legitimate identity-service changes, account scope and time distribution	Attempts align with suspicious successful access or other corroboration	Investigated accounts, sessions and alternative explanation
An enterprise login lure is reported	Message provenance and the user's actual interaction	Authentication material was supplied, an unapproved session exists or malicious content was opened	Containment, endpoint assessment and user communication
A data-sale claim names a supplier	Relevant contract and data-sharing scope	Credible material matches protected records or supplier confirmation arrives	Data owner assessment and reporting decision
A disruption claim circulates	Independent availability and transaction telemetry	Service impact or unauthorised configuration is verified	Duration, functions, mitigation and recovery
A new payment destination follows recovery	Recovery evidence and customer authorisation	Changes fail trusted verification or abuse is detected	Payment disposition, customer contact and linked incident case

An escalation trigger is not a reason to discard other evidence. Teams should preserve contradictory findings and reassess scope. An unverified public claim can remain open as a watch item while a separately confirmed internal event is contained.

12.4 How Brandefense can help

Brandefense brings together cyber threat intelligence, digital risk protection and external attack-surface management. For the decisions here, relevant work includes monitoring credential listings and impersonation, tracking extortion claims and supporting prioritisation of external exposure. Product observations still require validation against the customer's environment.

Start with a defined scope: the domains, brands, critical services and suppliers that matter to the organisation. Agree who receives findings, which evidence starts an investigation and how closure is recorded. The value is a usable decision path, rather than a larger alert total.

Request a demo

KEY TAKEAWAYS

01

Begin the programme now and respond to credible incident evidence immediately.

02

Every action has one owner and observable closure evidence.

03

Keep monitoring, validation, containment and legal reporting as distinct decisions.

APPENDICES

Appendices

A–E

THIS CHAPTER ANSWERS

What do the observations measure, and where do their limits begin?

1 January–22 November 2026

post-time window for the main observation set

Appendix A. Scope, sources and confidence 84
Appendix B. Public evidence-card register 88
Appendix C. Sources 89
Appendix D. Glossary 91
Appendix E. Additional reviewed claim themes 93

Appendix A. Scope, sources and confidence

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

A.1 Time and evidence populations

The report's main window is 1 January–22 November 2026 by post time. The recent section covers 8–22 November. Research took place while the cut-off day was in progress. A post may describe earlier material, and publication time does not establish intrusion time.

The evidence populations remain separate: country-associated posts, retained content, forum records, advertisements, claim dossiers, posting identities, selected domains, card observations and ransomware listings. Their totals are not added into a national attack count.

A.2 Dark-web observations

Odin by Brandefense uses Brandefense Blackhole observations of posts, including forum and chat material. The country-associated volume is 748,946 posts. The content view contains 33,458 distinct posts across retained sets, including 220 country-tagged forum posts and 5,043 Arabic-associated posts. [S1]

Coverage varies by month and source. The material does not represent every venue or every Saudi-related discussion. These observations do not establish national prevalence or changes in attack frequency.

The observations can include multi-country advertisements, unrelated names and historic material. A country association is not proof of targeting.

Every displayed post card maps to a retained private source record. Quotations preserve a short authentic narrative fragment. Public cards omit personal records, credentials, contacts, victim identifiers and active criminal links. A translation is separate from the original excerpt.

A.3 Organisation portfolio and exposure

The portfolio has 250 candidate primary domains in ten merged sector cells of 25. Selection reflects public roles and significant Saudi operations. It is not a published top-250 ranking, an independent-entity census or a statistically representative sample. Ownership, operating status and group overlap remain limitations. [S3]

The 22 November 2026 exposure snapshot has complete results for 249 of the 250 selected domains. The national Atlas headline for this assessed population is 52/100. Only the national rating is published. The remaining domain stays unknown and is excluded from exposure denominators.

Device, credential, document and listing counts describe observations held at the snapshot, including older records. Annual mentions cover 19 November 2025–18 November 2026; similar-name candidates cover a separate 30-day window. A listing is an advertisement, and a domain association does not establish a confirmed intrusion. [S3]

A.4 External domain-control observations

Complete external domain-control results are unavailable for publication. No control-prevalence or hygiene-index result is inferred. A missing observation must remain unknown rather than becoming a failed control. [S4]

External domain-control observations describe a service at its check time. They do not certify the whole organisation's security or prove domain ownership. Email-policy, certificate-status and web-header findings require separate assessed denominators.

A.5 Card material

These limited payment-card observations do not establish current validity, completed fraud, issuer-system compromise or national fraud losses. They do not support an issuer-security ranking. A distinct card record is one unique payment-card number associated with a Saudi issuer prefix in the main report window; posts may repeat a record or list several records. [S5]

These limits apply wherever card observations are mentioned, including the financial-services chapter. No card-by-month trend or issuer ranking is published.

A.6 Ransomware and extortion listings

Ransompedia supplies 30 Saudi-labelled listings in the window. The comparison uses the same window for the UAE, Qatar, Kuwait and Oman. Listing dates must not be treated as intrusion dates. [S2]

A listing is a criminal claim. A listing does not establish official victim confirmation, encryption, operational disruption or financial loss. Country labels, industry fields and target names may require further validation. Target labels are not necessarily independent legal entities.

A.7 External reporting and legal texts

External statements are attributed to their source. Controller statements establish that a disclosure was made and support the propositions the controller confirmed. A newspaper relay establishes reported claims within its own limits. Vendor research supports the observed campaign behaviour it describes.

The official legal and control texts were read for the specific provisions cited. The report does not substitute for entity-specific advice or a regulator's current instructions. Publication, effective and incident dates are kept separate.

The only CVE discussed is CVE-2026-0326. Its NVD record and vendor advisory were checked on 22 November 2026. The fixed-release table follows the vendor. No Saudi exploitation is inferred from that vulnerability record. [S14][S15]

A.8 Incident coverage

Incident coverage spans retained forum material, public reporting and official notices. These observations support the specific propositions attributed to each source.

Some official archives were not available for the whole window. The available evidence therefore does not establish an exhaustive national census. Missing coverage is not evidence that no event occurred.

NCA's 2025 achievements page reports more than 2,000 cyber incidents detected and responded to. That official figure measures a different population from the 2026 dark-web and leak-site observations in this report, and no comparable 2026 NCA total is established here for a like-for-like comparison. [S34]

An individual operator can publish a consistent multi-year series under its own definitions. For example, stc Group's 2025 ESG metrics record 8,405 attempted and 15 actual cyberattacks for stc KSA in 2024, and 10,313 attempted and 16 actual cyberattacks in 2025. That series illustrates a bounded single-operator comparison rather than a national incident rate. [S35]

The reviewed public sources establish one named controller disclosure among the detailed case dossiers. Other cases remain source-reported campaigns, advertisements, demand or unverified claims. The report does not claim that these are all incidents affecting Saudi Arabia.

A.9 Confidence and the decision boundary

Label	Meaning	Example
High for observation	A retained record directly supports the proposition	A seller posted an offer
Source-reported	A named publisher reports the behaviour or account	Vendor-observed password spraying
Official disclosure	An organisation or authority confirms the stated proposition	The mobile-app customer-data disclosure
Unverified outcome	The claimed target effect lacks independent support here	Access, theft, duration or sale asserted by a poster
Analytical model	A labelled interpretation for planning	A possible relationship between identity context and payment fraud

A plausible alternative remains visible beside each case. A controller confirmation can narrow uncertainty without validating every surrounding claim. An unsupported conclusion is removed rather than compensated for by a confidence label.

KEY TAKEAWAYS

01

Each population has its own unit, time and coverage limit.

02

A retained claim and a confirmed target outcome are different propositions.

03

Use the evidence boundary to choose the next proportionate validation step.

Appendix B. Public evidence-card register

The cards appear beside their relevant discussion. Their dates are post dates, not established incident dates. The private evidence map supports source traceability without publishing source links or victim identifiers.

Card	Post date	Venue	Alias	Language	Chapter
B01	2026-01-17	Forum	zer0sintt	English	4
B02	2026-01-30	Forum	alwayslearning	English	4
B03	2026-02-02	Forum	l0rd0f	English	4
B04	2026-02-13	Forum	agent7001	English	4
B05	2026-02-23	Forum	ryhem	English	4
B06	2026-02-27	Forum	sexyskin	English	4
B07	2026-04-19	Forum	Unnamed poster	English	4
B08	2026-06-08	Forum	Unnamed poster	English	4
B09	2026-09-15	Forum	Unnamed poster	English	4
B10	2026-09-28	Forum	Unnamed poster	English	4
B11	2026-03-24	Chat channel	313 Team	English	6
B12	2026-08-06	Chat channel	313 Team	Arabic	6
B13	2026-09-11	Chat channel	313 Team	English	6
B14	2026-10-02	Chat channel	313 Team	Arabic	6
B15	2026-05-03	Forum	Unnamed poster	English	5
B16	2026-07-18	Forum	FandyUAE	Russian	8
B17	2026-04-03	Chat channel	Unnamed poster	Arabic	8
B18	2026-03-04	Chat channel	Unnamed poster	Arabic	6
B19	2026-11-09	Forum	Unnamed seller	English	4

Appendix C. Sources

Source numbers that do not appear were retired during review and are not cited. Own-data entries identify the retained observation set; public URLs are not provided for private source material. External entries record the date and the supporting read status. A site-root citation marked "article URL withheld" protects the unnamed target.

S1: Odin by Brandefense: Saudi dark-web observations. Own observation set; private sources withheld. Verified on: 2026-11-22. Read status: own data.

S2: Ransompedia: Saudi Arabia and Gulf comparison. Own observation set; private sources withheld. Verified on: 2026-11-22. Read status: own data.

S3: Atlas exposure ratings and Blackhole domain associations. Own observation set; private sources withheld. Verified on: 2026-11-22. Read status: own data.

S4: Odin by Brandefense: external domain-control observations. Own observation set; private sources withheld. Verified on: 2026-11-22. Read status: own data.

S5: Odin by Brandefense: payment-card observations. Own observation set; private sources withheld. Verified on: 2026-11-22. Read status: own data.

S6: NCA: Essential Cybersecurity Controls ECC-2:2024. https://cdn.nca.gov.sa/api/files/public/upload/86e09090-44e4-481f-bc28-355673607654_ECC--2024-EN.pdf Verified on: 2026-11-22. Read status: web PDF read.

S7: SDAIA: Implementing Regulation of the Personal Data Protection Law. https://dgp.sdaia.gov.sa/wps/wcm/connect/2a9a4744-a2ae-444f-bad2-6dacde843637/The%2Bimpelementing%2Bregulation%2Bof%2Bthe%2Bpersonal%2Bdata%2Bprotection%2Blaw.pdf?CACHEID=ROOTWORKSPACE-2a9a4744-a2ae-444f-bad2-6dacde843637-pcruNj.&CONVERT_TO=url&MOD=AJPERES Verified on: 2026-11-22. Read status: web PDF read.

S8: SAMA: Cyber Security Framework. https://rulebook.sama.gov.sa/en/cyber-security-framework-2 Verified on: 2026-11-22. Read status: web text read.

S9: SAMA: Counter-Fraud Fundamental Requirements. https://rulebook.sama.gov.sa/en/counter-fraud-fundamental-requirements Verified on: 2026-11-22. Read status: web text read.

S10: SAMA: Fraud Prevention section 3.2. https://rulebook.sama.gov.sa/en/32-fraud-prevention Verified on: 2026-11-22. Read status: web text read.

S11: Unit 42: regional cyber-risk brief, updated 17 April 2026. https://unit42.paloaltonetworks.com/iranian-cyberattacks-2026/ Verified on: 2026-11-22. Read status: web text read.

S12: Check Point Research: Microsoft 365 password-spray campaign. https://blog.checkpoint.com/research/iran-nexus-password-spray-campaign-targeting-cloud-environments-with-a-focus-on-the-middle-east/ Verified on: 2026-11-22. Read status: web text read.

S13: Saudi CERT security alerts index. https://nca.gov.sa/en/cert/ Verified on: 2026-11-22. Read status: web text read.

S14: Palo Alto Networks: CVE-2026-0326 advisory. https://security.paloaltonetworks.com/CVE-2026-0326 Verified on: 2026-11-22. Read status: web text read.

S15: NVD: CVE-2026-0326. https://nvd.nist.gov/vuln/detail/CVE-2026-0326 Verified on: 2026-11-22. Read status: NVD record read.

S16: Saudi Press Agency: GASTAT household ICT use in 2026. https://spa.gov.sa/en/N2715791 Verified on: 2026-11-22. Read status: official statement text read.

S17: Saudi Exchange: issuer disclosure of limited mobile-app customer-data access. https://www.saudiexchange.sa/wps/portal/saudiexchange/newsandreports/issuer-news/issuer-announcements/issuer-announcements-details/?anCat=1&anId=95974&cs=4260&locale=en Verified on: 2026-11-22. Read status: official statement text read.

S18: Mubasher: issuer statement on customer-data incident. https://english-old.mubasher.info/news/4624554/The-United-International-Transportation-Company-Budget-Saudi-Announces-a-Limited-Cyber-security-Incident-Involving-a-Portion-of-the-Data-of-Certain-Customers-of-the-Budget-Saudi-Mobile-Application-/ Verified on: 2026-11-22. Read status: Live body read.

S19: The National: relayed construction-sector data claim. https://www.thenationalnews.com/ (article URL withheld) Verified on: 2026-11-22. Read status: Article body read; article URL withheld.

S20: SPA: police notice on fraudulent service advertisements, 16 April. https://www.spa.gov.sa/en/N2563378 Verified on: 2026-11-22. Read status: official statement text read.

S21: SPA: police notice on fraudulent service advertisements, 23 April. https://www.spa.gov.sa/en/N2569817 Verified on: 2026-11-22. Read status: official statement text read.

S22: SPA: police notice on fraudulent service advertisements, 3 May. https://www.spa.gov.sa/en/N2576669 Verified on: 2026-11-22. Read status: official statement text read.

S23: SPA: police notice on fraudulent services and counterfeit wristbands, 10 May. https://www.spa.gov.sa/en/N2582285 Verified on: 2026-11-22. Read status: official statement text read.

S24: SPA: police notice on fraudulent service advertisements, 19 May. https://spa.gov.sa/en/N2590305 Verified on: 2026-11-22. Read status: official statement text read.

S25: SPA: SDAIA prior-year privacy enforcement decisions. https://spa.gov.sa/en/N2489505 Verified on: 2026-11-22. Read status: official statement text read.

S26: Saudi CERT: Microsoft alert 2026-8020. https://nca.gov.sa/en/cert/8145/ Verified on: 2026-11-22. Read status: Original live alert body read.

S27: Saudi CERT: Google alert 2026-8026. https://nca.gov.sa/en/cert/8153/ Verified on: 2026-11-22. Read status: Original live alert body read.

S28: ArabicTrader: reporting of official mobile-app incident disclosure. https://www.arabictrader.com/en/news/stock-market/219537/saudi-budget-reveals-stock-market-of-a-limited-hack-through-its-electronic-application Verified on: 2026-11-22. Read status: Live body read.

S29: Brandefense: capabilities and demo. https://brandefense.io/request-a-demo/ Verified on: 2026-11-22. Read status: Live body read.

S30: MITRE ATT&CK: Password Spraying T1110.003. https://attack.mitre.org/techniques/T1110/003/ Verified on: 2026-11-22. Read status: Live body read.

S31: NCA: Critical Systems Cybersecurity Controls CSCC 2:2026. https://cdn.nca.gov.sa/api/public/cms/files/14828b9c-c1d5-4c6c-9b06-b6564f3ed17a_CSCC---2-2026-AR-.pdf Verified on: 2026-11-22. Read status: Official Arabic PDF read; version, introduction and scope.

S32: Dataminr: regional football-data advertisement. https://www.dataminr.com/ (article URL withheld) Verified on: 2026-11-22. Read status: Article body read; article URL withheld.

S33: Microsoft: Microsoft Digital Defense Report 2026, published 1 October 2026. https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/2026-Microsoft-Digital-Defense-Report.pdf Verified on 23 November 2026 (2026-11-23). Read status: web PDF read.

S34: National Cybersecurity Authority (NCA): Key Achievements (2025 milestones). https://nca.gov.sa/en/nca-achievements/ Verified on 23 November 2026 (2026-11-23). Read status: web text read.

S35: stc Group: 2025 Sustainability Report, ESG Metrics, published 26 June 2026. https://www.stc.com/content/dam/groupsites/stc-sustainability-report-2025/esg-metrics/ Verified on 23 November 2026 (2026-11-23). Read status: web text read.

Appendix D. Glossary

Term	Meaning in this report
Atlas	The external exposure rating used for the assessed portfolio in this report
National headline	One Atlas value for the whole assessed portfolio; no organisation or sector rating is published
Device association	An external record linking a device to a service domain; ownership and present access require validation
Advertisement	A seller's posted offer, without a verified transaction
Account demand	A buyer request, without proof of supply or valid access
Credential record	An observed authentication-related record; current validity requires assessment
Current listing	Authentication material advertised when observed; not proof of a usable account
Dataset claim	An assertion about records or files, whose origin and count may be unverified
Controller	The party that determines the purpose and manner of personal-data processing
Data subject	The person to whom personal data relates
Password spraying	Trying a small set of passwords across many accounts
MFA	Authentication requiring more than one independent factor
ERP	Enterprise resource planning, a class of business-management systems
CRM	Customer relationship management, including systems that hold customer interactions and records
DDoS	Distributed denial of service, an attempt to disrupt service availability
DMARC	A domain's policy and reporting mechanism for email authentication
SPF / DKIM	Sender-authorisation and message-signature mechanisms used in email authentication
DNSSEC	DNS data authentication using a signed chain of trust
TLS	Encryption and authentication for network connections

Term	Meaning in this report
Ransomware listing	A leak-site claim; it does not establish encryption or confirmed intrusion
Analytical model	A planning interpretation explicitly separated from established operational links

Appendix E. Additional reviewed claim themes

These entries extend the detailed cases. They are advertisements, demands, relays or unresolved leads, not additional confirmed intrusions. Some overlap each other, a case dossier or a listing. Dates are source-post dates unless the entry specifies research publication. No national incident total is derived. [S1]

ID / date	Broad theme	Evidence boundary	First owner decision
T01 · 2026-03-01	Bank-service targeting/status sequence	Repeated messages and timeout wording; no independently measured outage	Financial service owner: verify availability
T02 · 2026-03-03	Telecommunications website claim	Target/check-link format; no network-access evidence	Operations: establish affected functions
T03 · 2026-03-06	Public-website target list	Several targets in one message; not confirmed incidents	Service owners: verify status independently
T04 · 2026-04-04 / 2026-04-05	Public-body credential/data claims	A self-branded sequence promised data publication; access unverified	Identity and data owners: assess internal matches
T05 · 2026-07-06	Healthcare data-sale relay	Secondary advertisement; origin and recency unresolved	Privacy: validate the data relationship
T06 · 2026-08-03	Industrial public-body network claim	Configuration and vulnerability assertions do not validate access	Infrastructure: assess authorised records
T07 · 2026-07-21	Health-extortion country-scope lead	Saudi scope unestablished; excluded from Saudi incident assertions	Do not assign a Saudi victim
T08 · 2026-03-22	Credential demand	Buyer request; no acquisition or valid access established	Identity: review recovery and monitoring
T09 · 2026-04-03 / 2026-07-26	Loyalty-account offers	Separate sellers; no airline-system access or fulfilment established	Fraud: assess relevant customer activity
T10 · 2026-06-24 / 2026-07-06	Licensing-exam service advertisements	Multi-country capability claim; no exam-body intrusion established	Service integrity: validate relevant reports
T11 · 2026-01-04	Regional cybersecurity supplier claim	Claimed Saudi client material does not establish every client was accessed	Supplier risk: determine shared-data scope
T12 · 2026-01-14	Firewall-access advertisement	No access tested; organisation and capability unverified	Identity and infrastructure: validate relevant signals
T13 · 2026-01-16 / 2026-01-20	Healthcare-supplier archive thread	Possible overlap with a listing; hidden archive and replies do not corroborate	Supplier owner: scope relationship before counting an incident

ID / date	Broad theme	Evidence boundary	First owner decision
T14 · 2026-01-22 / 2026-01-26	Telecommunications dataset offers	Repeated offers and different asking prices; age and uniqueness unresolved	Data owner: assess provenance and prior remediation
T15 · 2026-02-14 / 2026-02-15	Phone-number dataset claim	Seller explicitly calls the material unverified; records are not verified people	Privacy: require stronger provenance evidence
T16 · 2026-02-28	Leisure/fitness membership-data offer	Potential relation to Case J; no independently verified new event	Customer-data owner: compare scope
T17 · 2026-03-13	Transport-application code and destruction claim	Source code, deletion and disruption asserted; no target confirmation	Application and operations: assess each proposition separately
T18 · 2026-03-17	Private healthcare data claim	Contact and demographic fields; volume and acquisition date unsubstantiated	Data owner: validate relevant fields
T19 · 2026-03-26	Business membership-service data claim	Contact, membership and log descriptions; freshness and access unverified	Service owner: assess exports and permissions
T20 · 2026-03-13 / 2026-04-10	Application SQL-data claims	Possible repost; a current-year title does not establish current access	Application owner: establish provenance
T21 · 2026-04-12 / 2026-04-13	Contact/customer database circulation	Several copies of one theme; freshness and uniqueness unverified	Privacy: assess matched data rather than post volume
T22 · 2026-04-13	Customer dataset with conflicting titles	Conflicting quantities remain unresolved; no figure selected as fact	Data owner: resolve provenance before scope
T23 · 2026-04-12	Sparse Saudi-associated dataset title	Insufficient narrative for origin, recency or a distinct event	Retain as an unresolved claim
T24 · 2026-03-17	Digital-service disruption claim	Self-label and check links; no measured outage	Operations: verify customer functions
T25 · 2026-05-05 / 2026-05-07	Global resume/document listing	Country-labelled subset; not a Saudi organisation incident or verified people	Data owner: assess only a relevant match
T26 · 2026-01-14 / 2026-05-01	Older global scraped-lead dataset	Later replies recirculate global material; no Saudi-only total or new intrusion	Link to prior scope rather than a new event
T27 · 2026-02-24	Mixed-country energy/engineering relay	Overlaps a retained listing; claimed material not necessarily Saudi-only	Supplier owner: determine which records apply

ID / date	Broad theme	Evidence boundary	First owner decision
T28 · 2026-02-23	Contractor-document relay	Overlaps Case I; industrial-document wording does not prove control-system access	Engineering security: validate data and permissions
T29 · 2026-09-12	ServerKillers public-website target list	Self-branded claim; no independently measured impact	Operations: verify each relevant service
T30 · 2026-10-26	DARKSTORM public-website target list	A list is not proof of multiple outages or internal access	Service owners: establish status and scope
T31 · 2026-09-10	Public-sector document relay	Possible relation to an earlier archive; file identity unestablished	Records owner: assess provenance and prior handling
T32 · 2026-10-21	Construction-data claim relay	Overlaps Case B; no independent confirmation or new event established	Supplier risk: retain the existing scoped investigation
T33 · 2026-09-28	Health application handling donor information	Dataset claim; authenticity, age, uniqueness and current access unverified	Privacy and application owner: assess a relevant data match
T34 · 2026-11-09 / 2026-11-10	Contractor session-access advertisement	Four repeated posts form Case P; no session or advertised material tested	Identity and supplier owner: validate scope and preserve evidence
T35 · 2026-10-14	Regional payment-processing service claim	Merchant/transaction data and a technical entry route asserted; no confirmation or loss established	Payment and data owners: assess relevant records without testing access
T36 · 2026-04-27, research publication	Regional football-data advertisement	Researcher-described archive includes Saudi-associated material; no confirmed Saudi system access or affected-person total	Personnel-data and supplier owners: validate relevant document relationships

A separate researcher account described a regional football-data advertisement. Saudi-associated material does not establish access to a Saudi organisation or a Saudi-specific affected population. No political framing or actor affiliation is adopted. [S32]

About this report

This is the Saudi Arabia edition of the Brandefense Country Report 2026 series, prepared by Odin by Brandefense. It serves security leaders, SOC teams, service owners, fraud teams and legal or compliance functions.

Brandefense brings together cyber threat intelligence, digital risk protection and external attack-surface management. The report's product observations remain evidence for investigation and prioritisation. They do not replace an organisation's own identity, service or incident records. [S29]

The Arabic edition translates the English master and preserves its numerical, source and claim boundaries. Where the editions differ, the English edition prevails.

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