BRANDEFENSE COUNTRY REPORT · TÜRKIYE 2026

Brandefense Türkiye Cyber Threat Landscape Report 2026

Identity abuse, supplier incidents and ransomware claims across a connected economy

Odin by Brandefense
Research window: 1 January–21 November 2026, by post date
Version 1.0 · Public Research Edition · TLP:CLEAR · 22 November 2026

250
organisation-domain assessments across twelve sectors

4,131,687
Türkiye-tagged posts in the observation window

3
separate tracks: listings, campaign research and channel claims

30
selected banking and finance domains

CONTENTS

Contents

01	Executive summary	04
	Report map	08
02	Türkiye's digital and security context	09
03	National exposure: 250 selected organisation domains	12
04	What we see on the dark web	21
05	Targeting examples by sector	38
06	Hacktivism and DDoS	44
07	Threat actors and supported relationships	48
08	The fraud economy	59
09	Banking and finance deep dive	65
10	Regulatory and national response	70
11	Outlook	74
12	Action plan	77
A	Appendix A. Method and limits	83
B	Appendix B. Evidence register	85
C	Appendix C. Sources	86
D	Appendix D. Glossary	88
E	Appendix E. Official disclosure register	89
F	Appendix F. Additional claim and market themes	96
	About this report	103

Board and CISO	01 05 11 12
SOC and incident response	04 06 07 12
Identity and infrastructure	03 05 07 12
Fraud and banking	08 09 12
Legal and procurement	05 10 12

About this edition

AI-assisted research and drafting. Claims, official disclosures and analyst interpretations are distinguished throughout. Scope and confidence are explained in Appendix A.

Türkiye's 2026 evidence points to a practical priority: contain identity abuse, prepare for supplier incidents and prove that essential services can recover.

66/100 (C)
National Atlas headline for the selected portfolio

4,131,687
Türkiye-tagged posts, not incidents

157
Ransomware listing claims

250
Selected organisation domains

Contents and reading routes

The report serves security leaders, operations teams, and identity, infrastructure and fraud owners. The twelve chapters move from decisions to evidence, then to accountable actions.

Chapter	Question	First reader
1. Executive summary	Which decisions follow from the evidence?	Leadership
2. Digital context	Which national features matter for security planning?	Leadership
3. Organisation exposure	Which exposure signals need an owner?	Infrastructure
4. Dark-web evidence	What is offered, and what remains unverified?	Threat intelligence
5. Sector examples	How do claims and official disclosures change priorities?	Sector owners
6. Hacktivism and DDoS	What separates an announcement from demonstrated disruption?	Operations
7. Threat actors	Which relationships and attributions are supported?	Threat intelligence
8. Fraud economy	How do identity, accounts and communications connect?	Fraud teams
9. Banking	Which financial controls deserve joint ownership?	Finance and identity
10. Regulatory response	Which duties apply, and which texts remain drafts?	Legal and compliance
11. Outlook	What would change the assessment?	Leadership
12. Action plan	Who acts, and what demonstrates completion?	All owners

Leadership route: Chapters 1, 3, 5 and 10–12. **Operations route:** Chapters 4, 6–7 and 12. **Identity and fraud route:** Chapters 3, 8–9 and 12.

Observed means the material or measurement is held. **Claimed** means a poster or listing asserts something. **Officially reported** means a controller or authority disclosed it, within the stated scope.

An analyst interpretation connects evidence to a decision. It does not supply missing proof about access, attribution, affected people or losses.

CHAPTER 01

Executive summary

01

THIS CHAPTER ANSWERS

Which security decisions does the Türkiye evidence support?

4

decisions with an owner and completion evidence

Four decisions for leaders 06

The year in numbers 06

CHAPTER 01

Executive summary

IN SHORT

Ransomware listings, identity-themed offers and official supplier disclosures require different responses. Ransompedia records 157 Türkiye listings in the window, against 53 in all of 2025. Official notices describe ransomware, mailbox abuse using a previously obtained password, and supplier incidents. Underground offers also recycle older material. The selected portfolio has a national Atlas headline of 66/100 (C). Prioritise identity validation, supplier notification, independent recovery and evidence-based public communications.

This edition combines retained Brandefense Blackhole posts, Ransompedia listings, passive observations and source-checked public reporting. The populations remain separate. A post is not an incident, a listing is not confirmation, and an organisation sample is not a national prevalence estimate [S1][S2][S3][S4].

1. Ransomware listings warrant continuity investment. Türkiye has 157 listings in the stated 2026 window. The same snapshot records 56 for Poland, 46 for Israel, and 20 each for Greece and Romania. These are visibility comparisons, not country risk rankings. Qilin contributes 17 Türkiye listings, Nightspire 15 and Thegentlemen 14 [S3].

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

2. Valid account abuse has an official example. A municipal notification attributes email-account access to a previously obtained password, rather than an email-server vulnerability. It describes mailbox-content export, message-deletion rules, spam and altered signatures. That supports an identity and mailbox investigation, without establishing how the password was first obtained [S15].

3. Supplier access links technical incidents to customer notification. A retail notification estimated 323,052 potentially affected people after an incident at a processor. Another described 592 end customers and 4 management-panel users. An investment-services notice described phishing at a foreign processor, with data export still unconfirmed. These remain separate disclosures [S16][S17][S20].

4. Large advertisements do not measure newly affected people. Selected offers include a claimed 2025 hospital-worker file, a 2023-labelled land dataset and a November cryptocurrency-business offer. The last mixes identities, tables and transaction rows. The advertised units cannot be added together, and none establishes a verified customer-loss figure [S1].

5. Official ransomware reporting preserves an exfiltration boundary. KVKK reported ransomware affecting Yıldız Teknik Üniversitesi's virtualisation infrastructure and servers. Its notice gave approximate potentially affected populations of 140,000 students and 4,500 staff. The university's later statement said investigators had found no evidence of data leaving its systems. Both statements matter [S12][S13][S14].

6. Exposure validation requires separate owners. The selected 250-domain portfolio has a national Atlas headline of 66/100 (C). It contains at least 1,140,618 device associations and 4,649,139 credential-record associations. Current listings concern 171 domains. These are overlapping external signals, not confirmed intrusions [S2].

7. Post volume measures visibility. The Türkiye-tagged total is 4,131,687, while the retained narrative corpus contains 177,648 distinct posts. Country comparisons use the same post-date window. Repeated advertising, market references and unequal visibility prevent a national risk ranking [S1].

8. Campaign research supports gateway and management review. FortiBleed research lists 3,032 devices labelled Türkiye. Separate virtualisation research places Türkiye among its five largest country groups [S94][S96]. These attributed infrastructure observations do not identify unique organisations or connect the campaigns to the report's access advertisements. Validate current assets, access and persistence before declaring a local incident.

Four decisions for leaders

1. **Validate identity signals before disruptive action.** Give identity operations responsibility for matching new credential or access offers to active accounts and recent sessions. Escalate corroborated unauthorised use to incident response; record why unmatched or historical signals were closed.
1. **Put supplier notification into the incident plan.** Identify processors with identity, customer, booking and investment data. Test who receives an initial alert, who preserves evidence, and who decides whether a notification duty has started.
1. **Prove recovery independently of production administration.** Restore an essential service using protected backups and separate recovery credentials. Measure service readiness, data integrity and business sign-off, rather than treating a successful backup job as proof of recovery.
1. **Keep communications tied to verified service and data facts.** Pre-agree a status page, spokesperson and evidence owner. Distinguish an actor's announcement, an observed service problem, and a confirmed disclosure about data handling.

The year in numbers

The figures below describe different populations. Each has its own limit.

157

Türkiye ransomware listings in the 2026 window [S3]

WHAT IT IS NOT

Confirmed attacks, unique victims or total national ransomware activity

53

Türkiye listings in all of 2025 in the same snapshot [S3]

WHAT IT IS NOT

A matched-duration baseline

66/100 (C)

National Atlas headline for the selected portfolio [S2]

WHAT IT IS NOT

A breach percentage, incident probability or sector ranking

4,131,687

Türkiye-tagged posts in the stated window [S1]

WHAT IT IS NOT

Verified incidents or the retained narrative corpus

1,140,618

Device associations, at least, in the selected portfolio [S2]

WHAT IT IS NOT

Unique people or organisation-operated endpoints

4,649,139

Credential-record associations in the selected portfolio [S2]

WHAT IT IS NOT

Unique active accounts or confirmed intrusions

250

Selected organisation domains across twelve sectors [S2]

WHAT IT IS NOT

An official ranking or a representative national sample

177,648

Distinct retained posts in this edition [S1]

WHAT IT IS NOT

The complete country-tagged population or unique incidents

860

Distinct Türkiye-associated payment cards visible in clear text in retained posts [S4]

WHAT IT IS NOT

Card theft, active cards, fraud losses or BRANDEFENSE 's wider card coverage

323,052

A retailer's estimated potentially affected population, reported through KVKK [S16]

WHAT IT IS NOT

A validated count from an underground file

140,000 / 4,500

Approximate student and staff populations in the university notification [S12]

WHAT IT IS NOT

Confirmed exfiltration or a final unique-person total

72 hours

KVKK's interpretation of the notification period to the Board after awareness [S8]

WHAT IT IS NOT

A universal deadline for every cyber reporting obligation

KEY TAKEAWAYS

01

Keep listings, posts and official incidents in separate decision tracks.

02

Validate accounts and supplier access before inferring a system-wide incident.

03

Fund recovery and notification exercises with named business owners.

Report map

Start with the decision you own, then follow its evidence and completion test.

Board and CISO	Which risks justify funding now?	01 05 11 12
SOC and incident response	When does an external claim become an investigation?	04 06 07 12
Identity and infrastructure	Which access paths and dependencies need validation?	03 05 07 12
Fraud and banking	Which identity facts should never authorise a transaction?	08 09 12
Legal and procurement	Who must notify whom, and under which instrument?	05 10 12

Evidence track	What it answers	Boundary
Underground posts	What people advertise, request or announce	Authenticity and outcomes need separate proof
Ransomware listings	What appears in the listing snapshot	Listing dates can differ from intrusion dates
Passive observations	What public-facing configurations show	No proof of successful intrusion or control effectiveness
Official disclosures	What a controller or authority reports	Estimates and investigations can change
Vendor research	What that researcher observed and attributed	Campaign-wide findings need not describe a Turkish victim

CHAPTER 02

Türkiye's digital and security context

THIS CHAPTER ANSWERS

Which national features should shape defensive planning?

90.4%

internet penetration reported for late 2026

2.1 A connected population and many identity touchpoints 10

2.2 Essential services and suppliers 10

2.3 National coordination and current channels 10

2.4 Political framing and attribution 11

2.5 A changing regulatory timetable 11

CHAPTER 02

Türkiye's digital and security context

IN SHORT

Connected services create both business opportunity and identity dependencies. DataReportal's November edition reports 79.5 million internet users and 90.4% penetration. Official cyber coordination is also changing, while new resilience and audit texts remained consultations at the cut-off. Plan around service dependencies, current notification channels and the evidence needed to distinguish access abuse from supplier incidents.

2.1 A connected population and many identity touchpoints

DataReportal published its Digital 2027 Türkiye edition on 5 November 2026. It reports 79.5 million internet users, 85.9 million mobile connections and 61.0 million social-media user identities. These are late-2026 estimates, with social-media identities dated October. Connections and identities do not represent unique people [S5].

The defensive implication is about dependency. A customer can encounter the same organisation through mobile messaging, email, an account portal and a supplier. An accurate name or telephone number can make a fraudulent contact more persuasive. It does not establish the caller's authority.

A digital service inventory should therefore connect applications to identity providers, recovery channels, processors and service owners. A server inventory alone cannot answer who can export customer information, reset an account, or publish a trusted message.

2.2 Essential services and suppliers

This report uses twelve analytical sector cells for the selected portfolio [S2]. They do not designate an organisation legally as critical infrastructure.

The operational question is which dependencies can stop an essential workflow. A payroll process may depend on a bank and an identity provider. A booking process may depend on a processor and a messaging account. Map the actual dependencies before assigning a recovery target.

The official supplier notices in Chapter 5 show why that matters. A controller may first learn about an incident from a processor. A processor's technical investigation and a controller's duty to assess affected people can then proceed on different timelines [S16][S17][S20].

2.3 National coordination and current channels

USOM's public notice directs security notifications, technical content, malicious-link information and CVE-related processes to the Cybersecurity Presidency's site. It also announces the end of a text-format sharing service from 1 June 2026 [S7]. Defenders should verify that their operational contacts and subscribed services remain current.

The Presidency's October PHP notice says national security checks had begun and urgent notifications had been sent to relevant organisations. This is evidence of an official response campaign. It is not a count of successful exploitation in Türkiye [S24].

The May incident-response guidance describes recurring weaknesses in account management, segmentation, remote access and logging. It supports a control review. It does not supply a representative denominator for all Turkish organisations [S33].

2.4 Political framing and attribution

Some retained posts attach political language to data claims. The publication does not adopt those claims, slogans or descriptions. A membership-data offer is treated as an unverified data claim, with the organisation withheld. It supplies no basis for identifying a political sponsor [S1].

The same discipline applies to territorial questions, ethnic or religious identities, regional conflicts, elections and government decisions. An actor's stated motive is the actor's explanation. It does not establish a cause, justify an action or attribute state direction.

The November DDoS material in Chapter 6 is especially limited. One channel announces an intention to select a Turkish target. That is a planning signal for defenders, without evidence here of an attempted attack or disruption [S1].

2.5 A changing regulatory timetable

Law 7545 entered into force on publication on 19 March 2025. The consolidated text includes changes effective on 31 July 2026 [S9]. Read the current text rather than assuming a summary from the law's original adoption still describes every provision.

On 18 November 2026, the Presidency opened resilience and audit drafts for consultation. Both announcements requested comments by 3 December 2026 [S10][S11]. This report treats them as drafts at the cut-off. A consultation date is not an effective date for proposed duties.

KEY TAKEAWAYS

01
Map identity and supplier dependencies alongside servers and applications.

02
Keep national coordination contacts and security information channels current.

03
Attribute political and state-linked claims to their sources and preserve uncertainty.

CHAPTER 03

National exposure: 250 selected organisation domains

03

THIS CHAPTER ANSWERS

Which external signals justify validation across the selected national portfolio?

250

organisation-domain assessments across twelve sectors

3.1 Universe card 13
3.2 The national headline and its decision boundary 14
3.3 Device and credential associations are concentrated 14
3.4 Current market listings require account validation 16
3.5 Mentions and similar domain names are context 17
3.6 Passive controls preserve their own denominators 18
3.7 Turn the portfolio into separate validation queues 20

CHAPTER 03

National exposure: 250 selected organisation domains

IN SHORT

The selected portfolio contains widespread device and credential associations, alongside current market listings. Its national Atlas headline is 66/100 (C). That rating describes this portfolio, not every organisation in Türkiye. The evidence records at least 1,140,618 device associations and 4,649,139 credential-record associations. These are overlapping records, not unique people or confirmed intrusions. Assign owners to current-account validation, employee-device investigation and recovery checks.

3.1 Universe card

The portfolio covers prominent public institutions, service providers and commercial organisations. It supplies a broad cross-sector view while preserving the limits of a selected sample [S2].

Item	Definition
Portfolio	250 selected organisation domains across twelve sectors
Selection	Public institutions, major service providers and prominent sector businesses
Sector cells	Government 50; banking and finance 30; education 30; manufacturing 30
Other cells	Energy, retail and transport 20 each; five further sectors 10 each
Exposure snapshot	21 November 2026
Mention context	19 November 2025–18 November 2026
Passive snapshot	21 November 2026 UTC, corresponding to 22 November locally
Publication	National headline rating and anonymous sector aggregates
Identity limit	Domains can represent brands, institutional services or related legal entities
Inference limit	No national prevalence estimate, organisation ranking or incident probability

The selected domains are the assessment units. Some belong to related organisations or services, and ownership validation remains incomplete for part of the portfolio. Consequently, 250 assessments must not be read as 250 independently owned businesses.

The smallest published sector cell contains 10 selected domains. These denominators support anonymous description; they do not establish representative coverage of each sector's employers, users or economic output.

Exposure observations and passive controls answer different questions. A historical credential record can coexist with a sound current configuration. A published email policy can coexist with an active-account incident. Neither should replace the investigation needed for the other.

3.2 The national headline and its decision boundary

The portfolio's national Atlas headline is 66/100 (C). Higher values indicate greater observed exposure in this portfolio. The rating supports prioritisation for the selected portfolio. It is not the percentage of organisations breached, a probability of future intrusion or a certification of control effectiveness [S2].

Only the national headline rating is published. Sector rows below show observed exposure counts and denominators. They do not rank sectors by a composite score, and no organisation score or identity appears in the report.

The rating belongs to the dated exposure snapshot. The post window, annual mention context and passive snapshot remain separately labelled. They should not be combined into a claim that every signal first appeared during 2026.

A rating can remain elevated after a specific account has been remediated. Historical records, repeated advertising and shared customer devices can persist in external evidence. Closure therefore requires organisation-side validation, with the result attached to the underlying signal.

The practical response is to establish whether an observation relates to an active account, a managed employee endpoint, a customer device or a historical record. Those distinctions determine the owner and the appropriate action.

3.3 Device and credential associations are concentrated

The portfolio contains at least 1,140,618 device associations, including 52,548 employee-device associations. It also contains 4,649,139 credential-record associations. Associations can overlap across domains [S2].

A device associated with a customer-facing service is not automatically an endpoint operated by that service. Likewise, a credential record associated with a domain does not establish that the organisation's own directory or infrastructure was the source.

Sector	Domains	Devices, at least	Employee devices	Credential records
Government	50	196,180	6,273	278,104
Banking and finance	30	175,336	1,643	393,538
Education	30	202,764	24,272	2,863,146
Manufacturing	30	18,231	1,373	186,812
Energy and utilities	20	17,321	466	79,430
Retail and holdings	20	297,274	1,394	143,853
Transport and logistics	20	86,160	745	89,309
Telecom and technology	10	101,887	14,666	453,352

Sector	Domains	Devices, at least	Employee devices	Credential records
Healthcare	10	5,705	371	35,227
Insurance	10	14,488	142	28,527
Hospitality and tourism	10	12,459	599	20,213
Media and entertainment	10	12,813	604	77,628
Total	250	1,140,618	52,548	4,649,139

Devices and employee devices in this table are associations, not distinct national endpoint populations. Employee associations are presented within the device view and must not be added to it. Credential records are a separate population.

Education contributes 2,863,146 credential-record associations. That is 61.6% of the portfolio total. This concentration supports a focused identity-validation workstream; it does not establish that education has the highest current compromise rate.

Retail and holdings contribute at least 297,274 device associations. The education, government, banking and telecom rows also contain substantial device populations. Customer reach, domain use and historical visibility can influence those totals.

A small number of high-volume domains can dominate a sector's sum. A national total consequently cannot serve as an individual organisation's expected exposure. Each participating owner needs the dated evidence relevant to its own accounts and services.

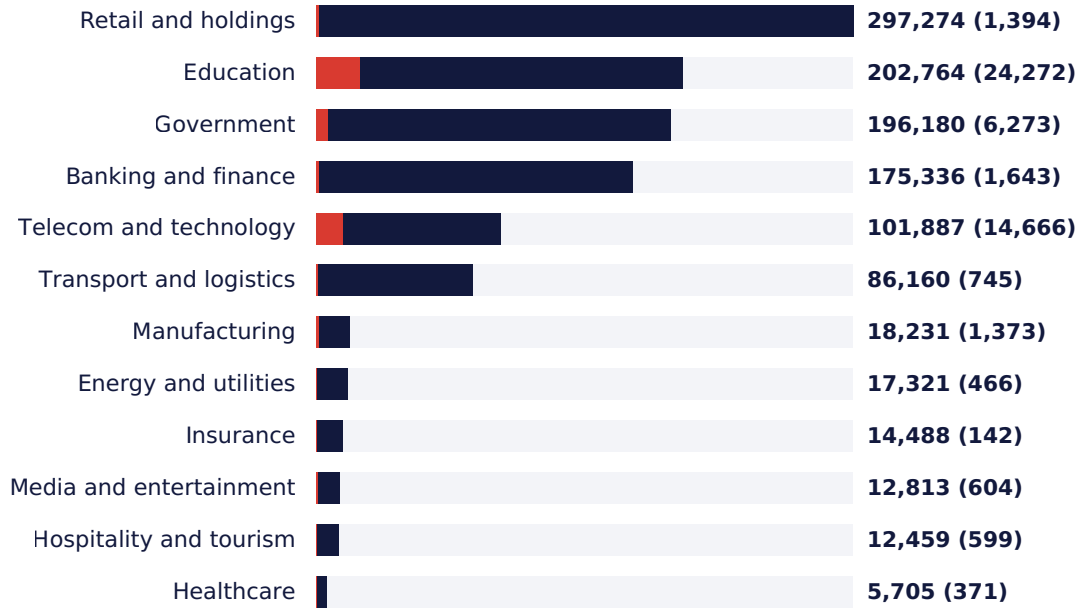
The first validation question is freshness. Establish whether the record concerns an active account, whether its secret has changed, and whether relevant sessions remained usable. The second question is authority: determine what the account could reach at the observation date.

For a corroborated employee endpoint, preserve endpoint and identity evidence before closure. Review sessions, recovery methods, delegated access and privileged activity. A password reset alone does not demonstrate that every route associated with the account has been contained.

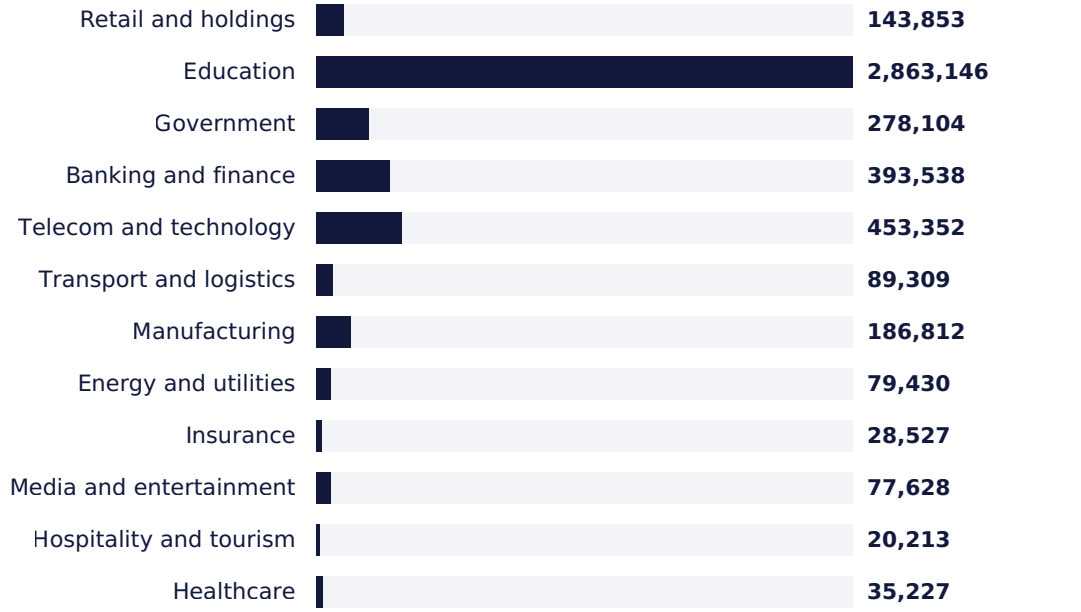
For a customer-device association, the response may sit with fraud, customer support or account protection. Avoid treating the customer as an employee endpoint or opening a bank-infrastructure incident solely because a banking domain appears in external material.

Sector device and credential populations differ in scale and meaning

DEVICE ASSOCIATIONS, AT LEAST (EMPLOYEE ASSOCIATIONS IN CORAL)



CREDENTIAL-RECORD ASSOCIATIONS (SEPARATE SCALE)



Source: Odin by Brandefense, selected 250-domain portfolio, 22 November 2026 [S2]. Associations can overlap and are not confirmed intrusions.

3.4 Current market listings require account validation

Current market listings concern 171 of the 250 selected domains. The same snapshot contains credential-record associations for 242 domains and device associations for 235. These are different signals and can overlap [S2].

Sector	Domains	Currently listed	Documents
Government	50	31	1,100
Banking and finance	30	18	128

Sector	Domains	Currently listed	Documents
Education	30	25	508
Manufacturing	30	12	153
Energy and utilities	20	11	78
Retail and holdings	20	19	233
Transport and logistics	20	15	53
Telecom and technology	10	7	84
Healthcare	10	9	42
Insurance	10	8	20
Hospitality and tourism	10	6	21
Media and entertainment	10	10	176
Total	250	171	2,596

The current-listing column counts domains associated with a current advertisement in the exposure snapshot. It does not count completed sales, tested credentials or organisations with confirmed internal intrusions. A listing requires validation against the relevant account and service.

The document column contains 2,596 document associations across 204 selected domains. A document association does not establish that the material was confidential, unlawfully obtained or downloaded by an adversary. Public documents and repeated material remain plausible explanations.

Listing and document totals are not additive. One organisation can appear in both, while a single credential or document can be associated with several domains. The table does not supply a unique artefact or affected-person count.

Use a current listing to start a bounded investigation. Identify the advertised service, establish whether the account exists and remains active, and compare the claim with current authentication evidence. Record what remains unknown when the advertisement supplies only a title.

Do not contact a seller or test a third party's advertised credentials as part of routine validation. Organisation owners can use their own records and authorised incident processes. A public report should not reproduce material that would make an exposed account easier to use.

Close an unrelated or historical signal with its reason. Retain a separate investigation when present-day unauthorised access is corroborated. This produces useful evidence of disposition without converting every advertisement into a confirmed incident.

3.5 Mentions and similar domain names are context

Organisation mentions supply additional context over the stated annual window. They can concern news, customer discussions, advertising, legitimate services or abuse. A domain appearing in a discussion is not, by itself, evidence of unauthorised access [S2].

98 selected domains have chat mentions and 56 have web mentions in that annual view. The two populations overlap. These counts describe domain visibility, without classifying every mention as an incident.

Lookalike observations require ownership and usage checks. Similar names can belong to an authorised reseller, a related business or an unrelated organisation. Ownership and related-business checks come before an abuse allegation.

A useful escalation combines a plausible impersonation relationship with a harmful use, such as an unauthorised login page or deceptive payment request. Similarity alone supports investigation. It does not justify a published allegation about the registrant.

The same boundary applies to documents and mentions. Prioritise evidence that identifies a current service, an active identity or a harmful user interaction. Keep a lower-confidence contextual observation open or close it explicitly when no further evidence is available.

3.6 Passive controls preserve their own denominators

Passive observations cover 239 DNS-resolving domains. The other 11 selected domains did not supply an interpretable observation for this snapshot. Their absence must not be scored as a failed security control [S2].

Observation	Count	Assessed population
DMARC rejection or quarantine policy	155	239 resolving domains
SPF observed	231	239 resolving domains
DNSSEC delegation record observed	9	239 resolving domains
TLS certificate check valid	214	239 resolving domains
TLS certificate validation unsuccessful	12	239 resolving domains
TLS result unresolved	13	239 resolving domains
Homepage HSTS observed	136	184 answering homepages
Homepage response recorded	184	239 resolving domains
Homepage check inconclusive	55	239 resolving domains

The TLS rows reconcile to the resolving-domain population. An unsuccessful certificate validation is a reason for configuration review, while an unresolved check supplies no certificate verdict. Homepage results likewise preserve the difference between an answering page and an inconclusive observation.

Passive policy observations retain the assessed sector denominators

	DMARC reject / quarantine	SPF observed	DNSSEC delegation	TLS validation
Government	31/45	43/45	0/45	39/45
Banking and finance	21/29	29/29	2/29	25/29
Education	20/29	28/29	0/29	26/29
Manufacturing	14/29	27/29	0/29	25/29
Energy and utilities	14/20	20/20	0/20	16/20
Retail and holdings	11/20	20/20	1/20	20/20
Transport and logistics	14/19	18/19	1/19	17/19
Telecom and technology	6/9	9/9	0/9	7/9
Healthcare	6/10	10/10	1/10	10/10
Insurance	4/9	7/9	0/9	9/9
Hospitality and tourism	7/10	10/10	3/10	10/10
Media and entertainment	7/10	10/10	1/10	10/10

Source: passive observations, 21 November 2026 UTC; 239 observed domains, with sector denominators retained [S2]. Policies do not demonstrate control effectiveness.

A published DMARC rejection policy is a policy signal, not proof that every message is authenticated correctly. A monitoring policy differs from rejection. Configuration owners should check effective and inherited policies before making changes [S34][S35].

A visible SPF record does not demonstrate that every legitimate sender is included. Failure to observe a DKIM record does not establish that signing is absent. Validate the selectors and outbound message headers actually used by the organisation [S35][S36].

A DNSSEC-related observation does not establish protection for every service. A valid TLS certificate confirms a limited certificate check. It does not show that the application is patched or that access is authorised [S37][S38].

Web-header changes also need application context. An absent header may merit review, but a change can disrupt an embedded service or integration. Give the application owner a testable change, an expected result and a rollback plan.

3.7 Turn the portfolio into separate validation queues

The evidence supports separate queues for current-account validation, employee endpoint investigation, customer-account protection and configuration review. Queue ownership should follow the asset and the corroborating evidence. A common national headline does not make these tasks interchangeable.

Signal	Accountable owner	First validation	Completion evidence
Current account advertisement	Identity operations	Account exists and claim matches the service	Dated account disposition and session review
Employee-device association	Endpoint response	Managed device and account relationship	Containment, recovery and identity review
Customer-device association	Fraud and account protection	Customer-account relevance and abuse indicators	Customer protection decision and transaction review
Credential record	Identity operations	Freshness and previous remediation	Active, historical or unrelated disposition
Document association	Information owner	Sensitivity, authorisation and current availability	Confirmed handling decision
Email or web policy observation	Service owner	Effective configuration and dependencies	Tested change or justified exception

Track credible signals awaiting an owner, time to validation and overdue actions. Report how many signals were confirmed, historical, unrelated or unresolved. These outcomes show whether the portfolio produces useful decisions; movement in a headline score alone cannot establish that.

For a supplier-related observation, establish which tenant and business service are affected. Route confirmed data-processing questions to the privacy owner while technical responders assess access and persistence. The notification decision should preserve the distinction between a credible incident and unresolved data export.

KEY TAKEAWAYS

01
The national Atlas headline applies to the selected portfolio, not all Türkiye organisations.

02
Device, credential, listing and document populations require separate validation and cannot be added together.

03
Assign each credible signal to its identity, endpoint, fraud or service owner with dated closure evidence.

CHAPTER 04

What we see on the dark web

04

THIS CHAPTER ANSWERS

What do post volumes establish, and which offers deserve investigation?

4,131,687

Türkiye-tagged posts in the observation window

4.1 Universe card 22
4.2 Monthly volumes and four comparators 23
4.3 Platforms and languages 24
4.4 Crime themes and units 25
4.5 Nine claim dossiers 27
4.6 Demand, older material and sensitive claims 36
4.7 What an incident team should retain 37

CHAPTER 04

What we see on the dark web

IN SHORT

Türkiye-tagged post volume is 4,131,687 in the stated window. The four comparator totals measure the same type of observation, not confirmed incidents or national risk. The retained corpus contains 177,648 distinct posts, including dataset offers, account sourcing and access advertisements. Some describe older material, while large figures mix people, records and transactions. Use volume to understand visibility, then validate the proposition behind each credible offer.

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

4.1 Universe card

The exact tagged-post view and the retained narrative corpus serve different purposes. The former describes reported post volume. The latter supports reading and assessment of individual propositions [S1].

Item	Scope
Window	Posts dated 1 January–21 November 2026
Türkiye-tagged volume	4,131,687 matching posts
Retained corpus	177,648 distinct posts in the assessed archive
Forum population	5,210 retained forum posts
Other platforms	172,438 retained posts
Scope boundary	Different coverage; neither view is presented as a subset of the other
Unit	A post, including replies, relays, advertisements and commentary
Not established	Unique sellers, datasets, completed sales, current access or confirmed incidents

The two views have different coverage and are not presented as nested populations. For example, the 5,210 retained forum posts and the 3,156 Türkiye-tagged forum posts describe different views. Their counts do not establish a subset relationship.

General-context posts can be retained for visibility without an individual incident conclusion.

A country tag can describe a market, a language, a quoted news item or one country within a multinational advertisement. It does not establish that an organisation in Türkiye was targeted or that the author was located there.

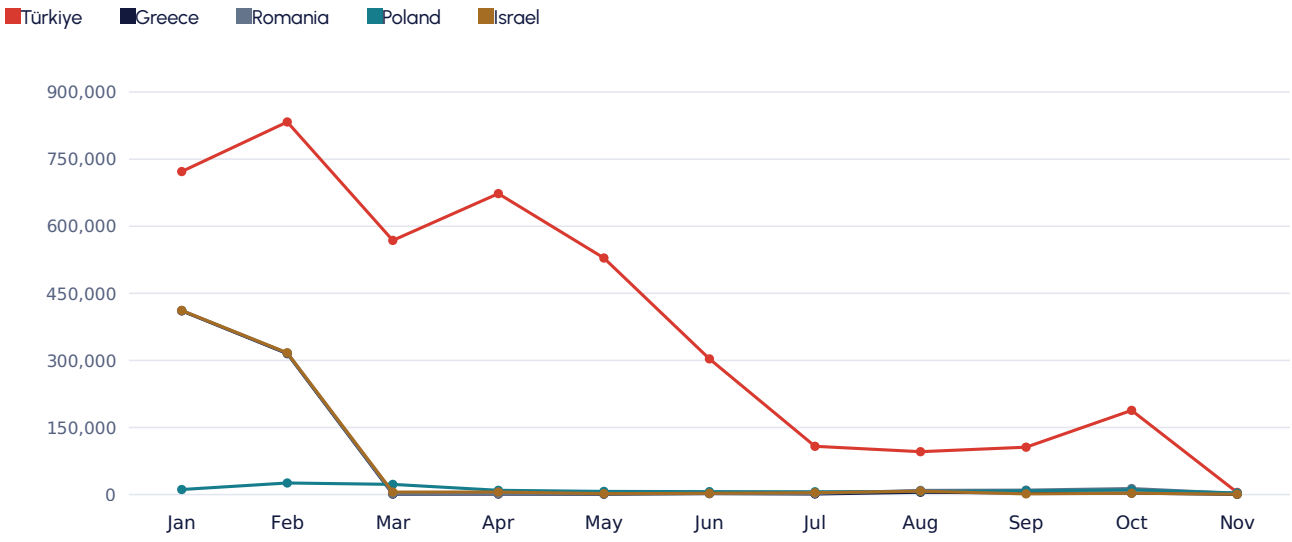
The cutoff-week update covers 15–21 November. It contributes 7 additional distinct posts relative to the earlier retained corpus. The coverage register records the action taken on new material; an update does not prove that every national incident has become visible.

4.2 Monthly volumes and four comparators

The following rows preserve the same post-date window and observation type across countries. November ends at the cutoff and is not a complete month [S1].

Month	Türkiye	Greece	Romania	Poland	Israel
2026-01	722,292	410,726	411,615	11,246	411,657
2026-02	833,137	315,057	316,242	25,871	317,075
2026-03	568,298	963	2,104	22,759	5,569
2026-04	672,924	1,062	2,047	9,476	5,691
2026-05	528,914	846	1,770	7,038	2,105
2026-06	303,371	2,138	2,358	6,502	2,799
2026-07	107,910	1,244	2,468	6,273	4,102
2026-08	95,867	5,165	9,281	6,873	7,590
2026-09	105,939	3,548	9,915	8,431	1,535
2026-10	188,243	3,295	13,436	10,338	2,995
2026-11	4,792	488	2,484	3,560	819
Total	4,131,687	744,532	773,720	118,367	761,937

Country-tagged volumes vary across the shared observation window



Source: Brandefense Blackhole, Türkiye-tagged posts and comparator counts, 1 January–21 November 2026; November partial [S1]. Tagged posts are not incidents.

January contributes 722,292 Türkiye-tagged posts and February 833,137. Together they account for 37.6% of the window total. A large early-year population does not establish that confirmed incidents followed the same distribution.

These are visibility comparisons. They do not adjust for population, internet use, collection coverage, marketplace participation or how often an advertiser repeats an offer. A larger total cannot establish a higher probability of intrusion.

The comparison countries supply descriptive context. Their inclusion conveys no political alignment or judgement about national security performance. The ransomware comparison in Chapter 7 remains a separate listing population.

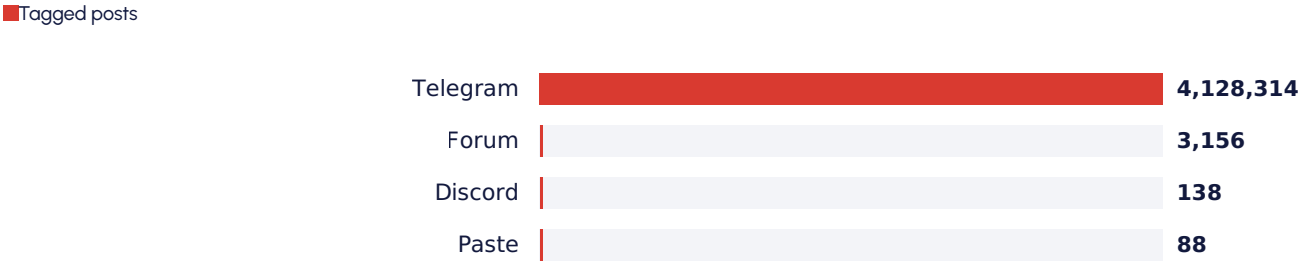
A common movement across countries can reflect visibility or broadly distributed material. A Türkiye-only movement still requires examination of its source composition. Neither pattern alone identifies a new campaign or demonstrates that an existing campaign became more successful.

4.3 Platforms and languages

The following tables describe the Türkiye-tagged view.

Platform	Türkiye-tagged posts
Telegram	4,128,314
Forum	3,156
Discord	138
Paste	88

Platform counts describe tagged visibility rather than confirmed events



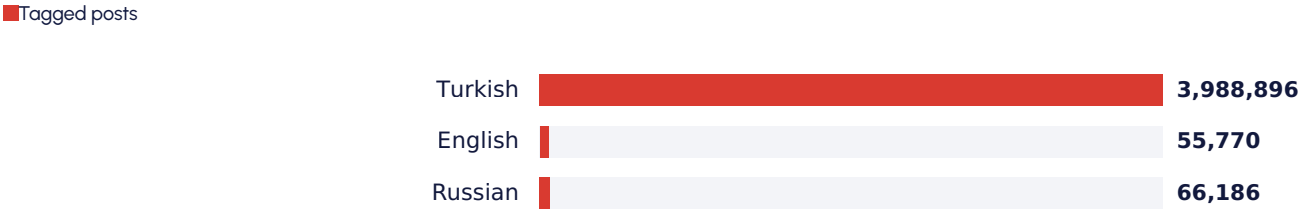
Categories overlap; counts describe posts, not successful attacks. Source: Brandefense Blackhole, Türkiye-tagged posts and comparator counts, 1 January–21 November 2026; November partial [S1]. Tagged posts are not incidents.

The platform counts exceed the national total by 9 posts. They are separate observations and are not treated as an exact partition. Telegram accounts for almost all tagged visibility, so repeated promotional traffic can dominate a national-looking total.

The retained forum population often supplies the context needed to distinguish an offer from replies to an older thread. Replies can repeat the title, amount and attribution without adding independent evidence. Assess the thread's proposition separately from its number of posts.

Language label	Türkiye-tagged posts
TR	3,988,896
EN	55,770
RU	66,186

Language labels describe content and can overlap



Categories overlap; counts describe posts, not successful attacks. Source: Brandefense Blackhole, Türkiye-tagged posts and comparator counts, 1 January-21 November 2026; November partial [S1]. Tagged posts are not incidents.

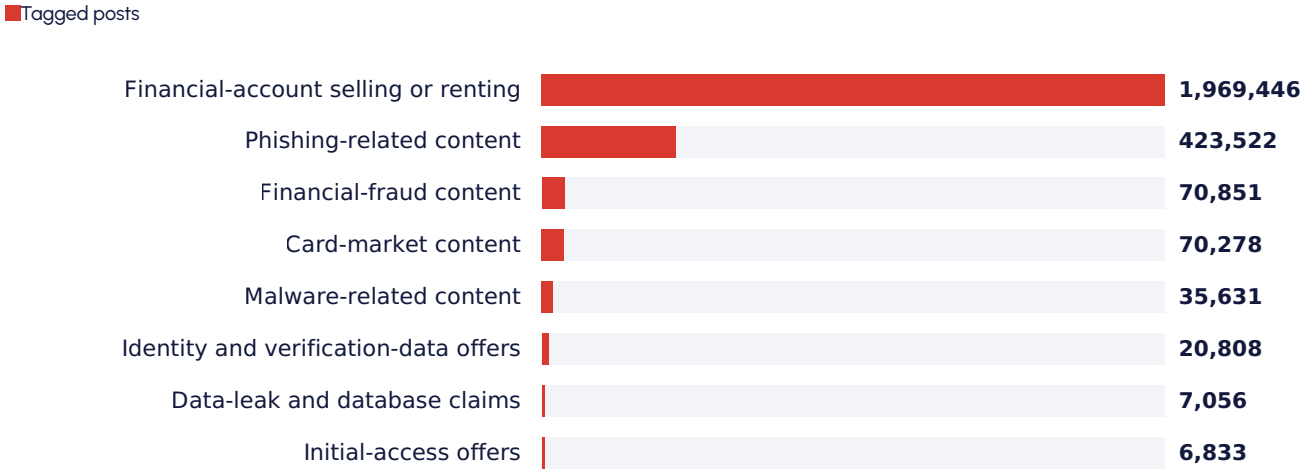
Language is a relevance cue, not a targeting verdict. Turkish-language content can concern another country. Russian- and English-language lists can include Türkiye among several markets. Labels need not be mutually exclusive, so their totals should not be treated as a disjoint population.

4.4 Crime themes and units

Selected content themes show how much of that visibility concerns an advertised capability or market activity [S1]. A theme label does not validate a seller's proposition. Posts can carry several themes, so the rows overlap.

Content theme	Türkiye-tagged posts
Financial-account selling or renting	1,969,446
Phishing-related content	423,522
Financial-fraud content	70,851
Card-market content	70,278
Malware-related content	35,631
Identity and verification-data offers	20,808
Data-leak and database claims	7,056
Initial-access offers	6,833

Market themes overlap and describe posts rather than successful attacks



Categories overlap; counts describe posts, not successful attacks. Source: Brandefense Blackhole, Türkiye-tagged posts and comparator counts, 1 January–21 November 2026; November partial [S1]. Tagged posts are not incidents.

Financial-account selling or renting appears on 1,969,446 posts. Phishing appears on 423,522, while initial-access selling appears on 6,833. These are differently sized conversations, not an intrusion funnel or a measure of criminal revenue.

A post labelled as phishing can advertise a kit, request help or repeat another seller's message. An access listing can lack evidence of current validity. The national volume therefore strengthens the case for coordinated identity and fraud triage, without estimating how many accounts were used.

The table also distinguishes card-market conversation from the narrow card aggregate in Chapter 8. There are 70,278 card-market posts in the national view. That does not establish 70,278 cards, successful charges or affected banks.

The useful distinction is what the poster offers or requests. A dataset advertisement, a data request, a credential list, account sourcing and a DDoS announcement require different validation questions.

Theme	Evidence example	Defensive question
Workforce identity	Older health-workforce file claim, B01	Can retained employment details enable recovery abuse?
Customer records	Payment-software claim, B02	Does a supplier hold the advertised fields?
Property data	Older property-record offer, B03	Can asset knowledge defeat identity verification?
Identity and telephone data	Unverified population figure, B04	Are personal facts treated as authentication?
Financial customer data	Cryptocurrency-business offer, B05	Can identity and fraud owners validate provenance together?

Theme	Evidence example	Defensive question
Remote access	Service-provider VPN offer, B06	Is there matching unauthorised access in current logs?
Account sourcing	Bank and exchange account sets, B07	Do onboarding and payment controls detect linked abuse?

These themes overlap. One advertisement can contain identity data, account records and transactions. Theme totals cannot be added into incidents, and this edition does not establish comparable category trends across the year.

Appendix F records 59 further claim and market themes from the detailed reading. Their access offers, supplier claims, archives and service advertisements complement the case dossiers. Similar subjects do not establish the same file, seller or campaign.

4.5 Nine claim dossiers

A

CASE A

An older workforce claim is posted in 2026

Evidence card B01 | 4 Jan 2026 | Forum | Healthcare workforce

Claim unverified

CLAIM	A 4 January post advertised information about approximately 2.7 million hospital workers. The poster explicitly placed the alleged leak in 2025 [S1].
CHRONOLOGY	A Turkish-language rendering appeared in the retained material the next day. Similar wording supports recirculation of the claim. It does not establish that two posters held the same file.
ESTABLISHED	We hold the post, its field descriptions and the poster's stated date. The publication date belongs inside this report's window; the claimed underlying event does not.
ALTERNATIVE	An older aggregate, repackaged records, inaccurate advertising or genuine non-public data could explain the offer. The advertisement alone cannot choose among them.
LIMIT	Authenticity, source-system ownership, completeness and a new 2026 event are unverified. The advertised scale is not a count measured by Brandefense.
RESPONSE	Healthcare and workforce-data owners should test whether recovery or help-desk procedures accept employment details as proof of identity. Validate any independently obtained notification against internal records.

Bottom line

Do not let employment details authorise account recovery.

Evidence card B01 — 4 Jan 2026

Poster alias withheld | Forum | Forum | English

ORIGINAL

This leak occurred in 2025.

Note. Hospital-worker dataset advertised with a claimed 2025 origin.

Held

The post and claimed scale; a 2026 publication date.

Not established

The source system, authenticity, a new 2026 incident, or a completed transfer.

CASE B

B

A customer-data claim names a software business

Evidence card B02 | 24 Jan 2026 | Forum | Customer services

Claim unverified

CLAIM	A January forum post attributed 93,000 customer records to a payment-software business. It advertised names, telephone numbers and addresses [S1].
CHRONOLOGY	Several retained replies repeat the same account of the alleged event. Repetition adds visibility, without independently validating the source or a new incident.
ESTABLISHED	The retained post contains the claimed volume and field categories. The organisation is withheld because this package has not established both official confirmation and wide reporting.
ALTERNATIVE	The material could relate to a customer, an integration, a supplier export or another source. Similar fields alone do not identify the affected system.
LIMIT	The offer does not demonstrate access to payment processing, card data or a bank network. It does not establish that any advertised file was downloaded or sold.
RESPONSE	Procurement and application owners should identify processors holding those fields. Ask for scoped incident evidence and review export permissions before imposing a broad service shutdown.

Bottom line

Validate processor data flows before attributing a payment-system incident.

Evidence card B02 — 24 Jan 2026

Poster alias withheld | Forum | Forum | English

ORIGINAL

Full Names, Phone Numbers and Addresses.

Note. Customer data attributed to a payment-software business.

Held

The advertised 93,000-record claim and field categories.

Not established

That the business or a payment network was affected as described.

CASE C

C ■ Property records carry an older date label

Evidence card B03 | 5 Feb 2026 | Forum | Property records

Claim unverified

CLAIM	A 5 February offer described a property-record dataset labelled 2023. Its advertised figure was 97,972,190 records [S1].
CHRONOLOGY	The post belongs to 2026, while the seller's date label is older. These dates answer different questions and remain separate.
ESTABLISHED	We hold an advertisement and its exact headline figure. The post does not establish when the underlying information was gathered or first disclosed.
ALTERNATIVE	A collection assembled from multiple periods or sources could contain repeated people or properties. A genuine file could also be described inaccurately. Neither explanation has been verified.
LIMIT	Records are not unique property owners. The claim does not demonstrate current privileged access to a public-sector system or an active lookup service.
RESPONSE	Financial, property and customer-service teams should avoid accepting knowledge of an address or asset as identity proof. Require a separate, trusted verification channel for changes and transactions.

Bottom line

Verify identity independently of address and property knowledge.

Evidence card B03 — 5 Feb 2026

Poster alias withheld | Forum | Forum | English

ORIGINAL

Exact Records: 97,972,190

Note. A land-record offer labelled 2023, posted in 2026.

Held

An advertisement using a land-record theme and its headline figure.

Not established

Its source, freshness, unique people or current access.

CASE D

D ■ An identity-and-phone offer uses an unverified people count

Claim unverified

Evidence card B04 | 25 Oct 2026 | Forum | Identity and communications

CLAIM	A 25 October post advertised identity and mobile-phone information. The poster described its headline figure, 201,593,023, as people [S1].
CHRONOLOGY	Earlier retained advertisements offered other large Türkiye-themed telephone datasets. Similar subjects do not establish a shared file or a common origin.
ESTABLISHED	The headline number and the unit used by the poster are observable. The number is not a population measurement or a Brandefense estimate.
ALTERNATIVE	Repeated identities, several telephone numbers per person, combined historical records or inaccurate marketing could explain the figure. We do not infer which explanation applies.
LIMIT	No unique-person total, current national-system access, completeness or buyer transaction is verified. The size of a claim cannot resolve its authenticity.
RESPONSE	Test account recovery against a caller who knows realistic personal facts. Fraud teams should alert service staff that accurate identity details do not authenticate a requester.

Bottom line

Test recovery against callers who know personal facts.

Evidence card B04 — 25 Oct 2026

Poster alias withheld | Forum | Forum | English

ORIGINAL

201,593,023 people.

Note. The claimant describes the figure as people; that unit is unverified.

Held

The stated figure in an identity-and-phone-data offer.

Not established

A population count, unique individuals or any current national system access.

CASE E

E

A financial dataset offer mixes identities and transactions

Evidence card B05 | 15 Nov 2026 | Forum | Financial services

Claim unverified

CLAIM	A 15 November post offered data attributed to a cryptocurrency business. It claimed a 12 November snapshot, 13 tables, roughly 48 million rows and 566,000 KYC identities [S1].
CHRONOLOGY	The snapshot date is the seller's description. It is not an independently established extraction date, and the post date is not proof of a current intrusion.
ESTABLISHED	The advertisement describes several populations, including identity, account and transaction-related information. They are not interchangeable totals.
ALTERNATIVE	An older export, a test environment, combined sources or fabricated advertising could resemble the description. The retained material does not establish one explanation.
LIMIT	Authentication-related field names do not establish usable secrets or current account control. No customer-loss amount, balance, unauthorised transfer or completed sale is verified.
RESPONSE	Identity, fraud, legal and incident response should share one validation owner. If exposure is corroborated, assess sessions and recovery mechanisms as well as passwords, and protect affected customers proportionately.

Bottom line

Review identity, session and recovery evidence together if exposure is corroborated.

Evidence card B05 — 15 Nov 2026

Poster alias withheld | Forum | Forum | English

ORIGINAL

13 tables

Note. A cryptocurrency-business database offer with several different units.

Held

A post claiming 566k KYC identities, roughly 48M rows and 13 tables.

Not established

Authenticity, valid account access, usable authentication material, or customer losses.

CASE F

F

A VPN advertisement requires current access evidence

Evidence card B06 | 17 Nov 2026 | Forum | Service providers

Claim unverified

CLAIM	A 17 November post offered VPN access associated with a service provider. The requested price was 200 XMR [S1].
CHRONOLOGY	The advertisement supplies a posting date and asking terms. It supplies no independently verified access date, transfer date or period of persistence.
ESTABLISHED	We hold the advertisement. Its requested currency and amount show how the offer was presented, without establishing a market-clearing price.
ALTERNATIVE	The offer might describe expired access, a narrow account, inaccurate company characteristics or a fabricated proposition. None is ruled out by the post.
LIMIT	The affected organisation, valid credentials, privilege level and any downstream customer effect remain unverified. The report does not reproduce identifying business characteristics.
RESPONSE	Remote-access owners should compare credible new signals with account validity, device identity and recent sessions. Escalate matching unauthorised activity; record why unmatched claims were closed.

Bottom line

Compare access offers with active accounts and recent VPN sessions.

Evidence card B06 — 17 Nov 2026

Poster alias withheld | Forum | Forum | English

ORIGINAL

price:200 xmr

Note. An access offer is a validation lead, not a verified entry point.

Held

A service-provider VPN access advertisement and its requested price.

Not established

The organisation, valid access, a sale, or any customer impact.

CASE G

G ■ Regulator-held documents do not establish incidents at every company mentioned

Claim unverified

Evidence card B15 | 21 Nov 2026 | Messaging channel | Financial regulation

CLAIM	A 21 November messaging post claimed access to a financial regulatory body's documents. It described a large archive containing tens of thousands of internal files and company financial filings, with a smaller portion offered [S1].
CHRONOLOGY	The post falls on the reporting cut-off. Its date does not independently establish an intrusion or extraction date. A fresh assertion deserves prompt assessment without becoming a confirmed incident count.
ESTABLISHED	The retained narrative describes regulator decisions, audit reports, correspondence, financial reports and IT-account email. These are the poster's descriptions. The report has not validated the files or their origin.
ALTERNATIVE	A regulator-held collection can contain submissions about many organisations. Their presence would not show access to each submitting company's systems. Repackaged material, a mixed archive or inaccurate descriptions remain possible.
LIMIT	No matching official account was verified during preparation. The entry path, current access, document authenticity and affected-person scope remain unverified. Political rhetoric and the names of the alleged target and document subjects are omitted.
RESPONSE	Regulatory, legal and financial-services owners should compare a credible document signal with their submission records and correspondence controls. Preserve evidence of provenance. Do not declare incidents at every firm mentioned by a poster.

Bottom line

Validate document provenance; do not infer incidents at every submitting firm.

Evidence card B15 — 21 Nov 2026

Poster alias withheld | Messaging channel | Telegram | Turkish

ORIGINAL

kurum içi dosya

TRANSLATION

internal files

Note. A regulator-document claim; no verified extraction or incident at every company mentioned.

Held

A retained post describing a regulatory document collection.

Not established

Authentic documents, current system access, the entry path or separate incidents at submitting firms.

CASE H

H ■ A pumping-control interference claim requires separate validation

Claim unverified

Evidence card B16 | 13 Mar 2026 | Messaging channel | Process-control systems

CLAIM	A 13 March channel post alleged interference with a pumping-station and industrial control panel. It claimed adverse process behaviour and removal of an operator control [S1].
CHRONOLOGY	The date identifies publication. No independently established system-entry, control-change or physical-effect time is available.
ESTABLISHED	The retained post contains a first-person allegation. Its wording does not establish that the poster was the original operator. The country framing does not verify the location of a physical facility.
ALTERNATIVE	Reposting, misrepresentation, old material or an unrelated test interface remain possible. A description of process behaviour does not independently demonstrate manipulation.
LIMIT	The target owner, access route, system changes and operational outcome remain unverified. Political rhetoric is omitted. No third-party control system was tested.
RESPONSE	Relevant asset owners should compare a credible claim with authorised remote-access records, engineering changes and operator evidence. Preserve contradictory evidence and involve the process-safety owner if an unauthorised change is corroborated.

Bottom line

Validate authorised engineering activity before declaring a physical process incident.

Evidence card B16 — 13 Mar 2026

Speaker not established | Messaging channel | Telegram | English

ORIGINAL

the control panel for the pumping station and industrial facility.

Note. A channel narrative alleges control-panel interference; the original operator and target are unverified.

Held
The dated post and its allegation.

Not established
System access, control changes, outage, physical effects or operator identity.

CASE I

An energy-access offer does not establish operational control

Claim unverified

Evidence card B17 | 22 Sep 2026 | Forum | Energy services

CLAIM	A 22 September forum advertisement offers extraction from several systems attributed to an energy-service company. The poster claims an ongoing working relationship, multiple access points and weaknesses of interest to ransomware operators [S1].
CHRONOLOGY	The date identifies publication. No acquisition, account-entry or privilege-change date is independently established. A claimed continuing relationship does not establish continuing unauthorised access.
ESTABLISHED	The retained text contains an access proposition. A brief proof label does not supply a validated demonstration. The poster's relationship, authority and advertised privileges remain unverified.
ALTERNATIVE	Historical, third-party, authorised or misrepresented access remain possible. The text does not link the poster to a ransomware group or establish that a transaction occurred.
LIMIT	An enterprise-system claim is not proof of power-system control, a service outage or a physical effect. The report does not link this offer to Case H or the other control-panel allegations.
RESPONSE	The relevant service owner should reconcile credible account and supplier details with authorised remote access and maintenance records. Preserve contradictory evidence. Escalate corroborated unauthorised access through incident response, with separate operational-safety checks where the affected service warrants them.

Bottom line

Validate service access and authorised relationships before inferring operational control.

Evidence card B17 22 Sep 2026

Alias withheld Forum Forum English

ORIGINAL

I have various access points and vulnerabilities.

Note. An energy-service access advertisement; the claim does not verify current access or operational control.

Held
The dated advertisement and its stated proposition.

Not established
A validated working relationship, privileges, live access, ransomware involvement or physical effects.

4.6 Demand, older material and sensitive claims

B10 explicitly describes a repost of material from 2023. It illustrates a direct dating warning. A newly visible thread can deserve fraud monitoring while contributing no evidence of a new 2026 incident.

B11 advertises over one million membership records attributed to a political organisation. The claim remains unverified. The organisation's identity and loaded actor language are omitted. The evidence supports a data-validation task, without any political or state attribution.

B12 advertises business documents across 2012–2026. That stated span does not identify the date of an intrusion. A long document history and a recent post can coexist without proving recent access [S1].

Evidence card B10 13 Nov 2026

Poster alias withheld Forum Forum English

ORIGINAL

it is from 2023

Note. The poster explicitly describes a repost.

Held
A 2026 post that labels the material as older.

Not established
A new 2026 incident or the authenticity of the underlying file.

Evidence card B11 5 Nov 2026

Poster alias withheld Forum Forum English

ORIGINAL

The database contains [...] member information

Note. An unverified offer of over one million membership entries; actor rhetoric and identifiers are omitted.

Held
A membership-data claim, not a verified political or technical attribution.

Not established
Authenticity, the source system, affected individuals or any political sponsor.

Evidence card B12 17 Oct 2026

Poster alias withheld Forum Forum English

ORIGINAL

Sales documents covering 2012-2026.

Note. A business-document release claim with a long stated time span.

Held
A post advertising business records.

Not established
A current intrusion, completeness or a shared source with other offers.

4.7 What an incident team should retain

For any credible external claim, keep the observation time, proposition, source category and evidence owner in an internal record. Preserve evidence lawfully and minimise personal information. Avoid buying material or attempting advertised access as a validation shortcut.

A useful disposition explains what changed. Examples include an active account disabled after corroboration, a processor confirming the affected tenant, an old incident already remediated, or a claim left unresolved for lack of supporting evidence.

KEY TAKEAWAYS

01
Post dates and underlying incident dates must remain separate.

02
Large dataset figures do not establish unique people, current access or losses.

03
Assign each credible claim a validation owner and a documented outcome.

CHAPTER 05

Targeting examples by sector

THIS CHAPTER ANSWERS

How do verified disclosures and unverified offers translate into sector-specific decisions?

3

different evidence types that must remain separate

5.1 The sector decision table 39
5.2 Ransomware and exfiltration are different propositions 40
5.3 A mailbox case with a stated password route 40
5.4 Supplier notices cannot be added into one campaign 41
5.5 Additional disclosures sharpen the response priorities 41
5.6 Read the response as carefully as the allegation 42

CHAPTER 05

Targeting examples by sector

IN SHORT

Official disclosures show concrete failure paths that broad exposure figures cannot establish. They describe ransomware, account abuse and processor incidents across several sectors. Underground claims add investigation leads. Their counts are not comparable with potentially affected populations in official notices. Use the strongest evidence available for each proposition, then give a sector owner a specific validation task.

5.1 The sector decision table

This table connects an observed proposition to a response. It does not rank sectors or estimate the share of organisations affected.

Sector	Evidence	Meaning	First owner
Education	Official ransomware notice and controller statement [S12][S13]	Recovery and data-export questions require separate evidence	Infrastructure and privacy
Public services	Password-based mailbox abuse [S15]	Review sessions, rules, exports and trusted outbound communications	Identity and messaging
Retail	Processor incident with estimated customer exposure [S16]	Supplier facts can start a controller investigation	Procurement and privacy
Financial services	Phishing at a foreign processor; export unconfirmed [S17]	Validate supplier identity controls and event chronology	Supplier risk and identity
Education services	Ransomware notice involving records about children [S18]	Recovery and careful notification need joint ownership	Service owner and privacy
Food retail	Processor-library exploitation described in a notification [S19]	Review third-party application dependencies	Application security
E-commerce	Customer and administration-account populations [S20]	Separate user groups and administrative access	Platform owner
Membership services	Processor notification with identity and password fields [S21]	Personal facts can assist impersonation	Identity and privacy
Retail services	Supplier notice involving staff and customer categories [S22]	An incident can cross workforce and customer workflows	Service owner
Food delivery	Access incident with population still being assessed [S23]	Keep customer impact open until investigation resolves it	Incident response

Sector	Evidence	Meaning	First owner
Manufacturing	Ransomware listings and document claims [S1][S3]	Listings justify continuity readiness, not a verified intrusion count	Operations and recovery
Banking	Account sourcing and promotion-lead offers [S1]	Fraud controls must cover customer-facing identity abuse	Fraud and identity
Energy services	Unverified multi-system access offer, Case I [S1]	Enterprise access does not establish operational control or a physical effect	Service owner and operational safety

5.2 Ransomware and exfiltration are different propositions

KVKK's 7 October notice described ransomware affecting Yıldız Teknik Üniversitesi's virtualisation infrastructure and the servers running on it. It reported approximately 140,000 students and 4,500 staff as potentially affected. The visitor count and affected personal-data categories were unresolved [S12].

The university's 8 October statement confirmed an attack on 1 October and said investigators had found no evidence of data export [S13]. NTV covered the incident on 8 October [S14]. That combination satisfies this package's naming rule for this case.

Question	Official notification	Controller statement	Assessment
Infrastructure affected?	Ransomware affected virtualisation and servers [S12]	Attack on information infrastructure confirmed [S13]	An officially reported incident
Potential population?	Approximate student and staff figures; visitors unresolved [S12]	No replacement population figure [S13]	Preserve the notification's qualifications
Data exported?	Affected data categories unresolved [S12]	No evidence of export found in the ongoing investigation [S13]	Export is not established by these sources
Actor and entry path?	Not stated [S12]	Not stated [S13]	No attribution or entry-path conclusion

The operational response has two tracks. Restore services and validate integrity. Separately preserve logs, examine export evidence and update privacy assessments. A recovery announcement does not answer the data-export question, and a potential population does not establish that every person's data left the systems.

5.3 A mailbox case with a stated password route

The municipal notification reports unusual outbound email activity detected on 30 September. It attributes access to a previously obtained password. It also reports exported contents from two mailboxes, deletion rules, bulk spam and altered message settings [S15].

This is stronger evidence for a specific identity failure path than an advertisement mentioning a government domain. It still does not identify how the password was obtained. Do not insert a stealer, phishing kit or state-linked operator into that missing step.

A response should cover sessions, rules, delegation, outbound abuse and affected correspondents. Password resets alone cannot demonstrate that an unauthorised forwarding rule or active session has been removed. Confirm closure with the messaging owner.

5.4 Supplier notices cannot be added into one campaign

A retail notice estimated 323,052 potentially affected people after unauthorised access to a processor server. A food-retail notice described exploitation of a third-party software library at a processor, affecting 67,193 people [S16][S19]. Similar supplier language does not establish a shared processor or intrusion.

An e-commerce notice separately described 592 end customers and 4 management-panel users. A jewellery-retail notice gave 964 people. An association notice stated a maximum of 9,462 members [S20][S21][S22]. These are notice-specific populations, with different qualifiers. They are not combined into a national unique-person figure.

The common defensive question is contractual and operational: can a controller quickly determine which data, accounts and tenants a processor incident concerns? The answer requires a current data map, a working contact route and preservation of scoped evidence.

5.5 Additional disclosures sharpen the response priorities

A membership chamber reported SQL injection detected on 2 November, followed by access to and export from its membership database. It said the general accounting system was unaffected [S45]. That boundary matters: application security and privacy teams need evidence about the affected database, while the organisation checks adjacent systems separately. A broad claim about every business system would exceed the notice.

A port operator reported access-control bypass at a supplier help desk, followed by password changes. Its initial affected population was 855 people [S39]. A renal-health services notice described employee voice phishing, one account, a CRM system and an internal directory file [S47]. An international pharmaceutical notice described voice phishing that impersonated IT at a subprocessor [S49]. These are separately disclosed paths. They support checking help-desk identity verification and delegated cloud access, without establishing a common operator.

The customer-service notices also distinguish people from retained conversations. One technical-support notice concerned 624 chat records, with the person count unresolved [S41]. An automotive notice concerned 8,268 chats, again without a resolved person count [S64]. A sports retailer separately reported 541 chat records concerning 383 people [S76]. A conversation can involve several people or repeat one person. No conversion factor is applied.

Record age is a separate issue. An e-commerce notice described 2022 chat records concerning 9,882 people [S43]. A delivery notice described records from the same year concerning 3,217 people [S70]. Those dates label the records. By contrast, an insurer's November notice explicitly dated the unauthorised access itself to 2022 [S44]. The report treats that insurer notice as a disclosure of historical activity, without presenting it as a new 2026 intrusion.

International notices require another boundary. A logistics group's notification identified 10,622 affected employees in Türkiye [S56]. A hotel-group notification reported 9,550 customers without establishing that all were in Türkiye [S79]. Publication by the Turkish authority alone does not turn every foreign-controller population into a Türkiye-only count. Appendix E records these qualifications and the remaining source-read notices.

5.6 Read the response as carefully as the allegation

A 4 November airline statement, reproduced by Memurlar.net, said an internal support-system vulnerability had been fixed. It said the systems supported application development, contained no guest databases and were not used for flight operations [S80]. This establishes what the company said about system scope. The report has not independently verified the advertised data volume, extraction or alleged customer impact.

The regulator's 11 November notice supplies a narrower confirmed notification: unauthorised use of an administration password in the airline's IT request and development system. It dates activity from 12 October and detection to 26 October, with 11,762 staff and users affected [S90]. How the password was obtained remained unresolved. Staff and system users are a different population from passengers; the notice does not validate the advertised customer-data proposition.

Question	Public data allegation	Controller response and official notice	Assessment
Support-system access	An advertisement alleges data possession	Administration-password access reported in the development system [S90]	The notification establishes a reported system incident
Passenger or flight systems	Broader customer impact alleged	Company says guest databases and flight operations were outside these systems [S80]	No independently verified passenger-system impact
Password origin	No verified route	Not established in the notification [S90]	Do not infer phishing, a stealer or an insider

The communications authority's 10 June statement rejected an attack explanation for an online public-service problem and described load and technical work [S81]. This remains an attributed account. Neither an allegation nor its denial substitutes for independent service and forensic evidence.

A telecommunications notification summary dates activity to 10 January and discovery to 26 January [S83]. The original notice has not been read for this package. Its population is not added to the source-read official register, and earlier archive coverage remains incomplete.

A separate legal review, published on 18 September, describes 27 controller notifications issued on 16 September concerning the same e-commerce infrastructure provider. It distinguishes 1 further notification concerning a corporate software service [S93]. This is a secondary review, separate from the original notices read for this report.

The review reports data associated with 424 organisations or entities in Türkiye in that separate case. Organisations are not people, accounts or independently established intrusions. The report does not adopt the review's combined person total: populations across controllers can overlap, while several controller totals remain unknown [S93].

This earlier cohort reinforces the need to preserve each controller's service relationship and evidence boundary. It is not linked here to the later supplier disclosures without matching evidence. Earlier original-notice access gaps remain visible in the coverage register [S93].

KEY TAKEAWAYS

01

Separate service recovery from the investigation of possible data export.

02

A password-based mailbox incident does not establish how the password was obtained.

03

Similar supplier disclosures do not prove a shared campaign or a disjoint national total.

CHAPTER 06

Hacktivism and DDoS

06

THIS CHAPTER ANSWERS

When does an announcement justify readiness, and when does it establish disruption?

1

retained announcement of an intention to select a target

6.1 Timeline of different evidence types 45

6.2 An intention announcement is not an outage measurement 45

6.3 Readiness without amplifying the claim 46

6.4 Communications during uncertainty 47

6.5 System-control allegations need operational evidence 47

CHAPTER 06

Hacktivism and DDoS

IN SHORT

One retained channel announcement says it intends to select a target in Türkiye. A later post advertises admission to a tool channel. Neither establishes a completed DDoS attack. The report has no verified matching official outage account for these posts. Use such material to check readiness and service evidence, while avoiding unsupported claims about actors, motives or impact.

6.1 Timeline of different evidence types

The timeline deliberately separates claims, official statements and publication dates. It does not assert a relationship between the events [S1][S12][S13][S15][S24].

1 Oct 2026	**University incident** Incident date later reported by the university and KVKK [S12][S13]
7 Oct 2026	**Personal-data authority** Ransomware notification published; potential population remains qualified [S12]
8 Oct 2026	**University statement** Ongoing investigation had found no evidence of data export [S13]
21 Oct 2026	**National cyber authority** National response to PHP vulnerabilities announced [S24]
7 Nov 2026	**Channel using the TunisianMaskers label** Intention to select a bank or company in Türkiye, not a verified attack [S1]
20 Nov 2026	**Tool-channel poster** Recruitment mentioning data and DDoS; no demonstrated service outcome [S1]

6.2 An intention announcement is not an outage measurement

B13 uses the TunisianMaskers label and says the channel is considering a bank or company. It does not identify a validated target. Its language is prospective. The report therefore records an announcement, without counting an attempted or successful attack [S1].

The label does not establish the location, nationality, identity or sponsorship of the people behind the channel. No such attribution is made here.

Evidence card B13 — 7 Nov 2026

Channel using the TunisianMaskers label | Messaging channel | Telegram | English and Arabic

ORIGINAL

we think about bank or company

Note. A channel using the TunisianMaskers label announces an intention.

Held
The 7 November announcement.

Not established
An attempted attack, a named target, outage duration or service impact.

Evidence card B14 — 20 Nov 2026

Poster alias withheld | Messaging channel | Telegram | Turkish

ORIGINAL

Aktif tool kanalına alım vardır

TRANSLATION

Admission to the active tool channel is open

Note. Tool-channel recruitment, not evidence that a named organisation was attacked.

Held
A recruitment post mentioning data and DDoS.

Not established
Tool capability, use, operator identity or a connection to B13.

Point	Channel statement	Official account	Evidence boundary
Target	Considering a bank or company in Türkiye, B13	No matching account verified	No organisation-level attribution
Activity	Intention to launch DDoS	No matching account verified	No attempted attack established
Duration	A duration appears in the post	No matching account verified	Not an observed outage
B14 relationship	Separate tool-channel recruitment	No matching account verified	No shared operator or campaign established

6.3 Readiness without amplifying the claim

A credible threat announcement can justify checking mitigation contacts, capacity and a service-monitoring baseline. It should not automatically trigger a public breach statement. Service owners need application-level evidence, including user-visible availability and dependency status.

A website problem can also reflect a supplier outage, configuration change or other operational fault. Correlate traffic, application health and provider information before attributing a disruption. Keep those alternatives open in the incident record.

6.4 Communications during uncertainty

Use separate statements for service availability and data confidentiality. A public page can be unavailable without evidence of data access. An account or dataset claim can require investigation while public services remain available.

When an actor invokes a political issue, record it internally as the actor's framing if relevant to readiness. Avoid repeating slurs, endorsing an explanation or presenting a government decision as a proven cause.

6.5 System-control allegations need operational evidence

A separate May post asserts bank targeting across Türkiye and another market. It supplies no independently verified method, outage or loss. This claim is not counted as a completed DDoS event [S1].

The April telecommunications claim in F58 and October remote-panel claim in F59 require different validation from a website outage. They do not establish control changes or physical consequences. Neither is linked here to Case H. Relevant owners should preserve remote-access and engineering records, reconcile authorised work, and involve operational safety staff when evidence supports unauthorised activity [S1].

KEY TAKEAWAYS

01
An announced intention does not establish an attempted attack.

02
Validate service impact separately from claims and claimed durations.

03
Keep actor framing and political attribution attached to their sources.

CHAPTER 07

Threat actors and supported relationships

07

THIS CHAPTER ANSWERS

Which actor relationships are supported, and where does attribution stop?

3

separate tracks: listings, campaign research and channel claims

7.1 Relationship map 49
7.2 Ransomware listings and group concentration 50
7.3 A locally focused ransomware campaign in vendor research 54
7.4 Espionage research with a country-specific boundary 55
7.5 Channel identity and poster labels 56
7.6 FortiBleed: country-labelled devices and recovery evidence 57
7.7 Virtualisation management: a campaign with a limited country view 57

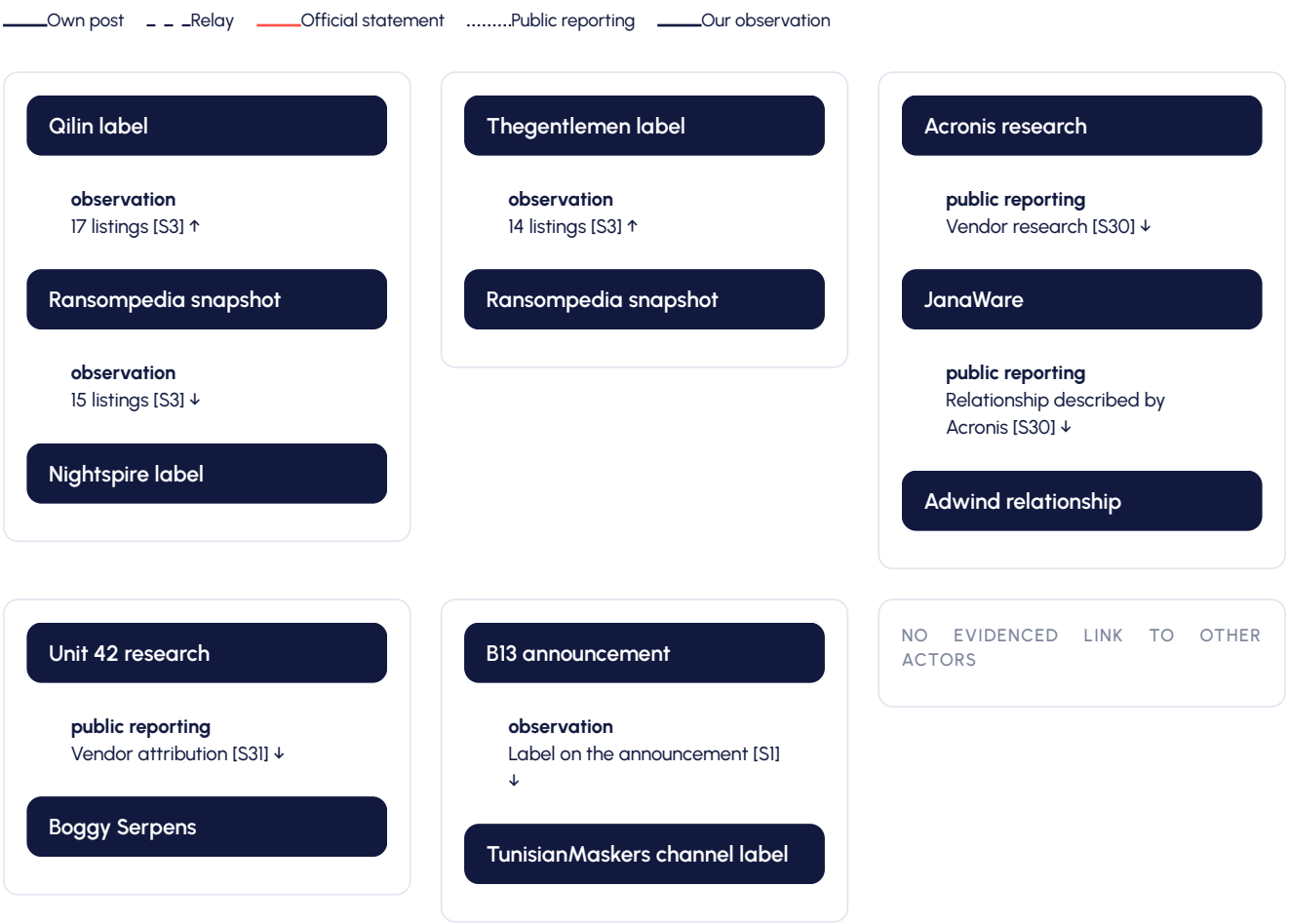
CHAPTER 07

Threat actors and supported relationships

IN SHORT

Ransomware group names come from the listing snapshot. Acronis describes a locally focused operation, while Unit 42 includes Türkiye in broader espionage research. Gateway and virtualisation research add country-labelled infrastructure findings. Channel allegations remain a separate claim track. None establishes a common operator or a national incident total. Use source-specific relationships and validate the assets and services implicated by credible evidence.

7.1 Relationship map

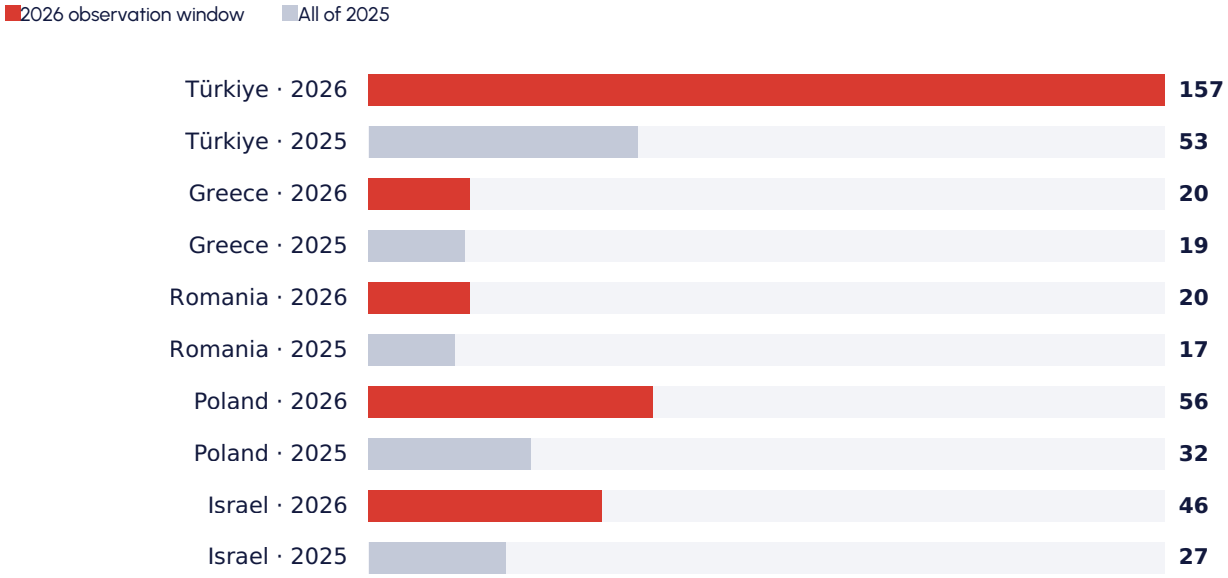


The map contains source-to-proposition relationships, not a criminal hierarchy. Ransompedia supports group labels and listing counts. Acronis supports the JanaWare and Adwind relationship. Unit 42 supports its own Boggy Serpens attribution. B13 supports an announcement by a channel using a particular label [S1][S3][S30][S31].

No retained common element connects the nine case dossiers to one operator. Any depiction of a wider identity-to-fraud chain is an **analytical model**. It represents defensive dependencies, without asserting observed transactions between those posters.

7.2 Ransomware listings and group concentration

Türkiye has more listings than the four selected peers in this snapshot



The 2026 window and all of 2025 have different durations. These are visibility comparisons, not risk rankings. Source: Ransompedia listing snapshot, 1 January–21 November 2026 [S3]. Listings remain claims.

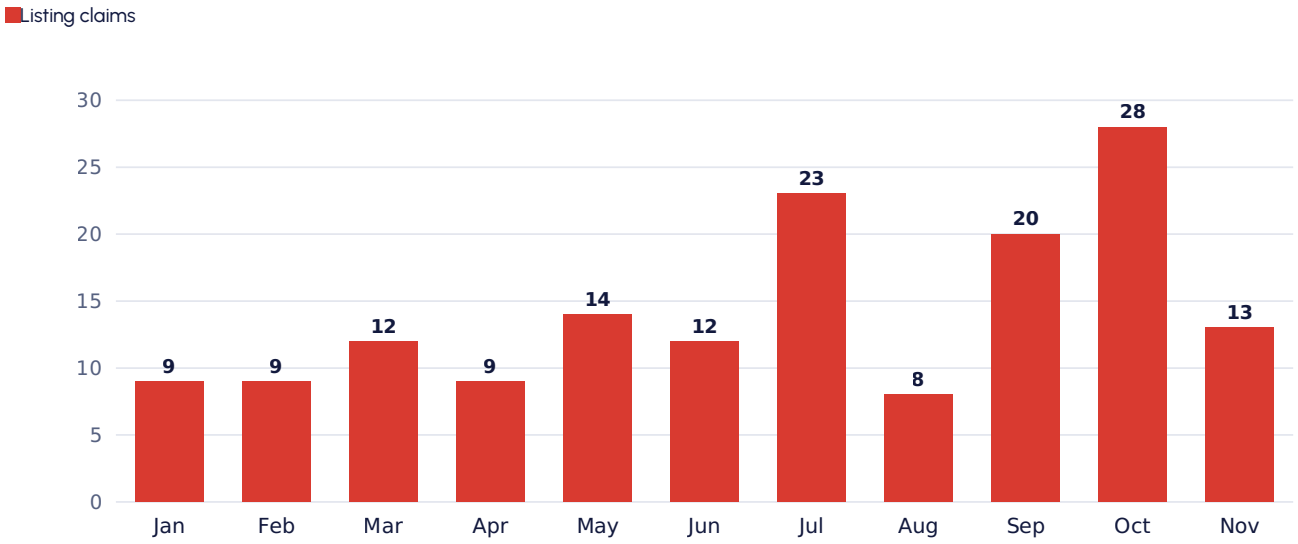
Comparison countries were selected as examples to provide context only; they do not imply a ranking or political assessment.

Country	2026 window	All of 2025
Türkiye	157	53
Greece	20	19
Romania	20	17
Poland	56	32
Israel	46	27

The table compares five countries with differing economic sizes, disclosure practices and visibility. No ranking of attack probability, preparedness or political exposure follows from this table [S3].

The monthly view shows how listing publications are distributed. November ends at the cut-off and is not a full month.

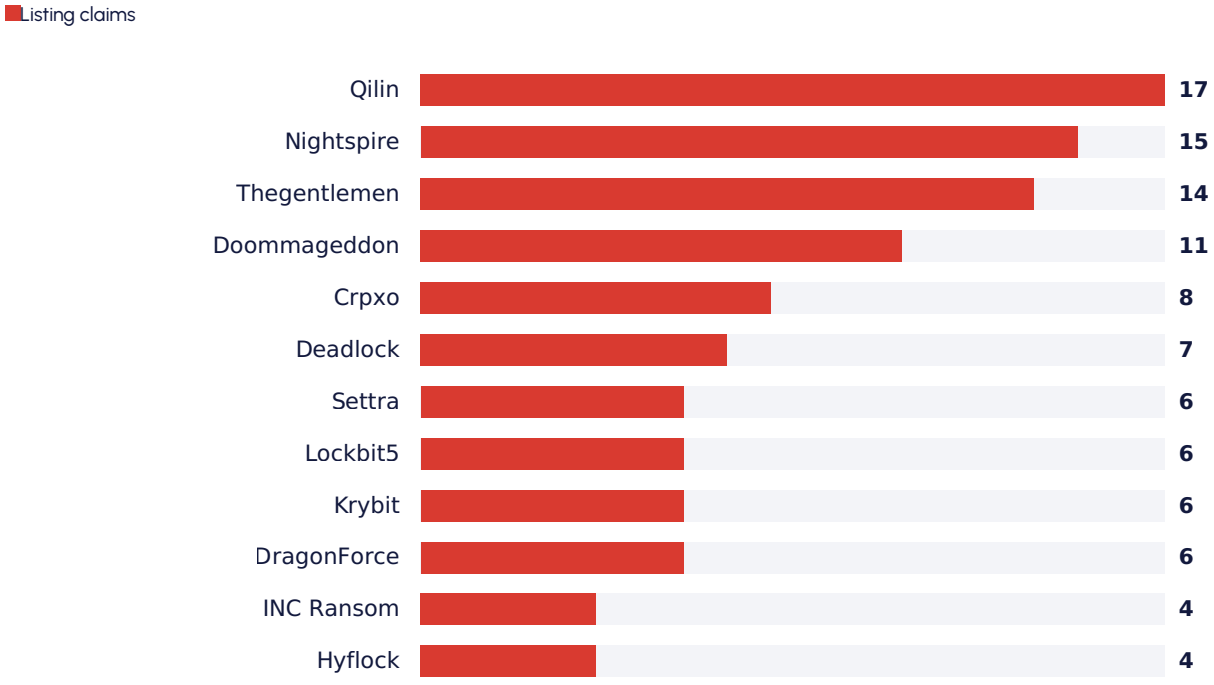
Listing publications peak in October within the observed 2026 window

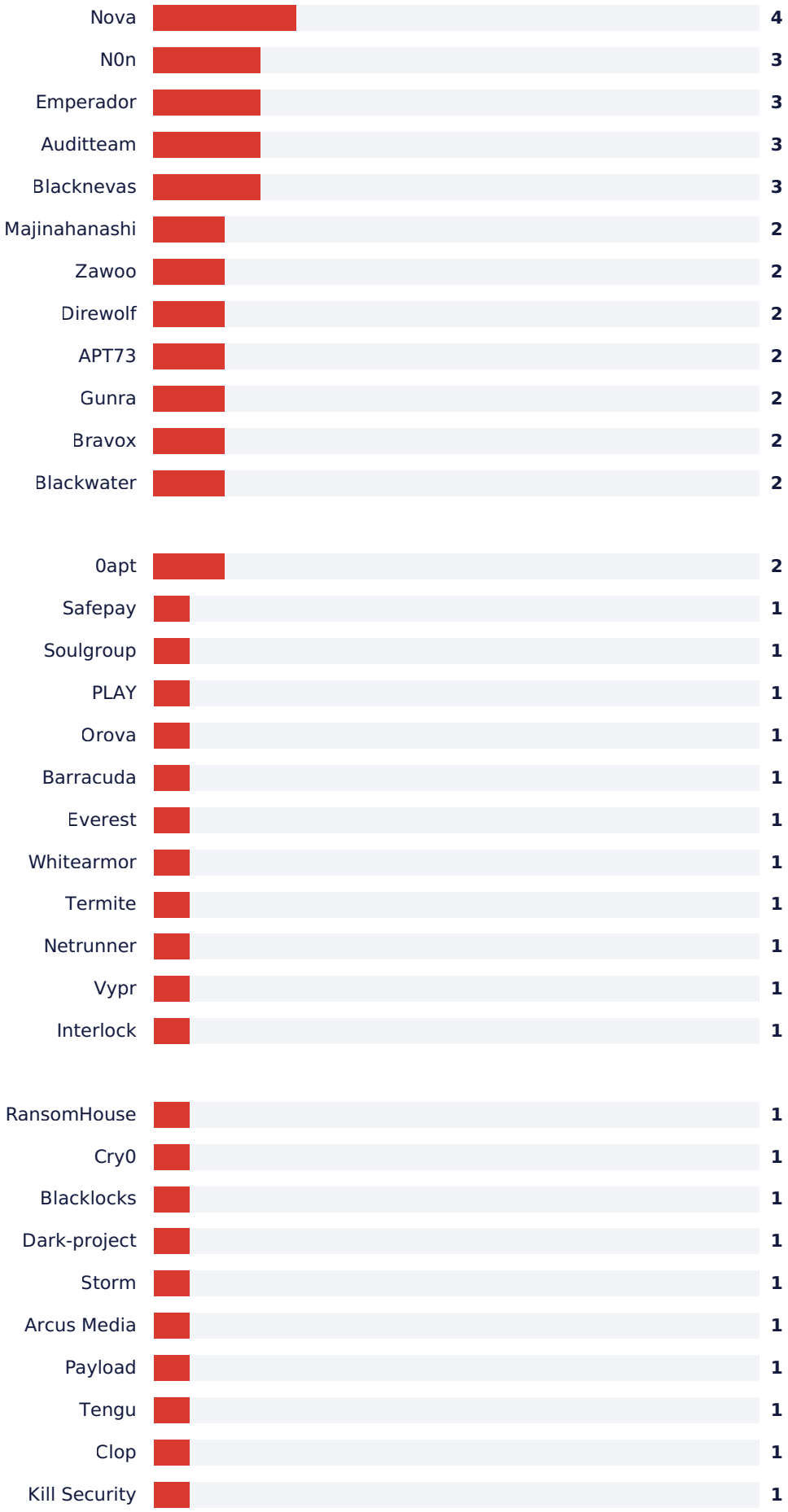


Source: Ransompedia listing snapshot, 1 January–21 November 2026 [S3]. Listings remain claims.

The group view shows the labels most often attached to Türkiye listings. Qilin's 17, Nightspire's 15 and Thegentlemen's 14 total 46 of 157 listings, or 29.3%. The remaining 111 listings use other group labels [S3].

The three largest group labels account for 29.3% of Türkiye listings




Nova 4
N0n 3
Emperador 3
Auditteam 3
Blacknevas 3
Majinahanashi 2
Zawoo 2
Direwolf 2
APT73 2
Gunra 2
Bravox 2
Blackwater 2
0apt 2
Safepay 1
Soulgroup 1
PLAY 1
Orova 1
Barracuda 1
Everest 1
Whitearmor 1
Termite 1
Netrunner 1
Vypr 1
Interlock 1
RansomHouse 1
Cry0 1
Blacklocks 1
Dark-project 1
Storm 1
Arcus Media 1
Payload 1
Tengu 1
Clop 1
Kill Security 1

Source: Ransompedia listing snapshot, 1 January-21 November 2026 [S3]. Listings remain claims.

Qilin

Ransomware listing label | No state or political attribution made

IN TÜRKIYE, 2026

2026
17 Türkiye listings in the Ransompedia snapshot

CLAIMED TARGETS

Organisations described by the listings; identities withheld

SEEN IN PUBLIC REPORTING

[S3] Own listing snapshot; a listing remains a claim

OUR ASSESSMENT

The label supports listing comparison, not a common affiliate, entry path or verified victim outcome.

CONFIDENCE
High for the retained count; incident outcome unverified

Nightspire

Ransomware listing label | No state or political attribution made

IN TÜRKIYE, 2026

2026
15 Türkiye listings in the Ransompedia snapshot

CLAIMED TARGETS

Organisations described by the listings; identities withheld

SEEN IN PUBLIC REPORTING

[S3] Own listing snapshot; a listing remains a claim

OUR ASSESSMENT

The label supports listing comparison, not a common affiliate, entry path or verified victim outcome.

CONFIDENCE
High for the retained count; incident outcome unverified

Thegentlemen

Ransomware listing label | No state or political attribution made

IN TÜRKIYE, 2026

2026
14 Türkiye listings in the Ransompedia snapshot

CLAIMED TARGETS

Organisations described by the listings; identities withheld

SEEN IN PUBLIC REPORTING

[S3] Own listing snapshot; a listing remains a claim

OUR ASSESSMENT

The label supports listing comparison, not a common affiliate, entry path or verified victim outcome.

CONFIDENCE
High for the retained count; incident outcome unverified

Group labels do not establish the precise malware, entry path, affiliate or outcome for a listed organisation. Nor does one group's presence in several countries establish a connected campaign across them.

7.3 A locally focused ransomware campaign in vendor research

Acronis's 14 April research describes JanaWare delivered through a modified Adwind Java RAT. It reports Turkish-language and location checks, phishing-delivered Java archives, and observed ransom demands of 200–400 USD. Its historical assessment reaches back to at least 2020. It does not provide a national victim count [S30].

JanaWare

Acronis research designation

Ransomware campaign in vendor research | No state attribution made

IN TÜRKIYE, 2026

2026-04-14
Acronis research published

CLAIMED TARGETS

Turkish users and smaller organisations, per Acronis

SEEN IN PUBLIC REPORTING

[S30] Acronis describes a modified Adwind relationship

OUR ASSESSMENT

Use the source-scoped campaign example for attachment and recovery planning. No national victim total is established.

CONFIDENCE
Vendor observations; national scale unknown

For defenders, the useful planning question is whether smaller offices and suppliers can resist unexpected executable attachments and recover independently. The operational test is a controlled exercise using benign files and a real restore, with service-owner sign-off.

7.4 Espionage research with a country-specific boundary

Unit 42's 16 March assessment includes Türkiye in campaigns spanning April 2025–February 2026. It attributes Boggy Serpens, also called MuddyWater, to Iran's Ministry of Intelligence and Security [S31].

Boggy Serpens

MuddyWater, per Unit 42

Espionage attribution in vendor research | Unit 42's attribution, not the authors' independent attribution

IN TÜRKIYE, 2026

2026-03-16
Unit 42 assessment published

CLAIMED TARGETS

Türkiye appears in the wider campaign geography

SEEN IN PUBLIC REPORTING

[S31] Vendor attribution; historical remote-management behaviour and a separate process-hollowing example; Türkiye timing unresolved

OUR ASSESSMENT

The report preserves the distinction between a wider campaign and a verified Turkish incident.

CONFIDENCE
Source attribution;
TURKISH
event date unresolved

Unit 42 describes trusted-account abuse in recent activity. Its remote-management examples appear in a discussion of early campaigns. This is historical actor behaviour, with timing in the stated window and Türkiye-specific application unestablished [S31]. The campaign map does not supply a confirmed 2026 Turkish incident count.

TECHNIQUES NAMED IN THE VENDOR RESEARCH, BY TACTIC

Command and control	Defense evasion
T1219 Remote access software; historical actor behaviour; window and Türkiye application unestablished [S31]	T1055.012 Process hollowing; vendor payload example [S31]

Techniques explicitly linked by Unit 42. This is not a verified technique set at a Turkish victim. [S31]

The matrix preserves each technique's source-specific time scope. It is not a verified technique set at a Turkish victim.

Tactic	Technique	Source scope	Defensive use
Command and control	T1219, remote access software	Historical behaviour; window and Türkiye application unestablished [S31]	Review authorised remote-management installations and their operators
Defense evasion	T1055.012, process hollowing	Payload example in the same research [S31]	Assess endpoint visibility for unexpected process behaviour

7.5 Channel identity and poster labels

Channel using the TunisianMaskers label

Label in the retained announcement

DDoS intention announcement | No location, nationality, political or state attribution made

IN TÜRKIYE, 2026

2026-11-07
Prospective target-selection announcement, B13

CLAIMED TARGETS

Considering a bank or company; no validated target

SEEN IN PUBLIC REPORTING

[S1] Retained announcement B13; no matching official outage account verified

OUR ASSESSMENT

An intention is observed. An attempted attack, target and service impact are not established.

CONFIDENCE
High for the announcement; outcome unverified

The dataset and access cards withhold seller aliases where they add contact or identification value without helping the reader's decision. The public evidence register retains stable card IDs. Repeated wording supports similar advertising, not common ownership, theft or a completed sale [S1].

The same restraint applies to a politically themed membership claim. The text of an advertisement does not identify a state sponsor or justify a political label for the alleged victim.

7.6 FortiBleed: country-labelled devices and recovery evidence

Hudson Rock's June research reports 73,932 firewall URLs across 194 countries and 21,632 affected domains. Its country table lists 3,032 devices for Türkiye [S94]. These are attributed research measures. URLs, domains and devices are different units; none is a count of the selected organisations or a verified national incident total.

NCSC advises checking asset ownership and signs of compromise, preserving useful evidence before resetting affected devices, and investigating reachable systems [S95]. These actions support a recovery decision. Password changes alone do not establish removal of persistent access. No link between this campaign and the report's separate access advertisements is established.

7.7 Virtualisation management: a campaign with a limited country view

QUIRSO's August research reports 361 IP addresses with reported unauthorised access across 47 countries and includes Türkiye among the five largest country groups [S96]. Addresses are not unique companies. Reported remote-access persistence is a campaign finding, without a verified Turkish organisation count or local ransomware outcome.

The associated CVE-2026-59310 concerns code execution through the vCenter Syslog service. The NVD record identifies affected versions [S97]. Apply the appropriate vendor fix for the deployed branch and investigate unauthorised persistence. Research attribution is not adopted as an independently established actor identity.

NVD also lists Cloud Foundation, vSphere Foundation and Telco Cloud products. Their owners should use the product-specific vendor matrix [S97][S99].

The vendor response matrix identifies affected branches and their applicable fixes [S99]. Earlier builds on the relevant branch require remediation. It lists no workaround. Product bundles and extended-support deployments need the vendor's specific guidance.

Affected vCenter branch	Vendor fixed version or action
9.1.x.x	9.1.0.0300
9.0.x.x	9.0.2.0100
8.0	8.0 U3k or 8.0 U2f, for the applicable branch
7.0	Contact vendor support if an extended-support contract applies

Secondary channel relays also repeat ransomware listings and business descriptions [S1]. They do not independently verify exfiltration or interruption. They have not been added to the separate 157-listing snapshot merely because they appeared in another channel.

KEY TAKEAWAYS

01
Ransomware group counts describe listing labels and preserve listing uncertainty.

02
Campaign-wide vendor findings cannot establish every Turkish target's date or entry path.

03
Supported relationships take precedence over an inferred criminal hierarchy.

CHAPTER 08

The fraud economy

08

THIS CHAPTER ANSWERS

How do identity data, account sourcing and communications create fraud opportunities?

15,000 TL

a bank-account asking term in one retained advertisement

8.1 Bank and exchange account sourcing 60

8.2 Payment-card material: a narrow view 61

8.3 Telephone services and identity verification 61

8.4 Lead lists and prices in context 62

8.5 Police campaign reporting 63

8.6 Reused records inside a software service 64

CHAPTER 08

The fraud economy

IN SHORT

Retained advertisements connect personal information with account sourcing, telephone services and customer leads. They show offers and demand, without establishing completed transactions. Official police reporting supplies a separate view of alleged criminal activity. Treat identity facts as untrusted authentication material, connect onboarding to transaction monitoring, and give fraud and security teams one escalation route.

8.1 Bank and exchange account sourcing

B07 asks for sets of bank and cryptocurrency-platform accounts. Its stated terms include 15,000 TL per bank account and 5,000 TL per exchange account. Those are asking terms in a post, not observed payments or national market prices [S1].

Evidence card B07 — 18 Feb 2026

Poster alias withheld | Forum | Forum | Turkish

ORIGINAL

Banka başı ödeme 15k

TRANSLATION

Payment per bank 15k

Note. An account-sourcing advertisement; quoted prices are asking terms.

Held
A request for bank and exchange account sets.

Not established
A genuine supplier, usable accounts, completed payment or a bank intrusion.

The advertisement matters because opening an account and controlling its later use are different security questions. A correctly identified customer can still be recruited to make an account available to another party. A stolen account can also enter a similar transaction flow.

The evidence does not establish which mechanism applies to the advertised accounts. Fraud controls should test several routes: related accounts, unusual beneficiary changes, rapid onward transfers and inconsistent device behaviour. A suspicious pattern requires investigation, not an automatic attribution to a particular customer.

8.2 Payment-card material: a narrow view

SCOPE OF THE CARD FIGURES

These figures cover only payment cards that appeared in clear text in the dark-web posts retained for this report. Brandefense detects stolen cards through many other methods outside this edition. The figures do not measure card theft, active cards, fraud loss or total Brandefense card coverage.

The retained population contains 860 distinct Türkiye-associated payment cards across 733 posts. The issuer-attributed and country-only groups are reported separately below. Their association does not establish an incident at an issuing bank [S4].

Group	Distinct cards
Issuer-attributed	578
Country-only association	282
Total	860

The proportionate response is issuer-side validation. Check whether a card is active, whether it has already been replaced, and whether supporting fraud evidence exists. A public-post appearance alone should not determine a blanket reissue decision.

8.3 Telephone services and identity verification

B08 advertises messaging numbers and eSIM services, with asking terms including 850 TL and 100 USD for different services. It does not establish access to an existing subscriber's number or the defeat of a mobile operator's controls [S1].

Evidence card B08 16 Feb 2026

Poster alias withheld Forum Forum Turkish

ORIGINAL

FİYAT = 850 TL

TRANSLATION

PRICE = 850 TL

Note. A messaging-number and eSIM advertisement.

Held
The advertised service and price; no purchase was made.

Not established
SIM ownership, access to an existing number or bypass of an operator control.

A telephone number is therefore a communications attribute, not sufficient proof of identity. Recovery procedures should consider number changes and the reliability of the enrolled channel. High-impact changes need an independent check that an unauthorised caller cannot satisfy merely by quoting personal facts.

The same principle applies to KYC information. Possession of a document image or accurate identity details is not the same as control of an existing account. Case E shows why identity data and account-related material should be evaluated together.

8.4 Lead lists and prices in context

B09 advertises 2,151 banking-promotion leads. The post establishes a marketing-themed offer, without establishing a bank-system incident, source consent or data freshness [S1].

Evidence card B09 9 Oct 2026

Poster alias withheld Forum Forum English

ORIGINAL
2.151 UNİTS

TRANSLATION
2,151 units

Note. A bank-promotion lead list; it is not evidence of a bank-system incident.

Held
A lead-list offer using a banking theme.

Not established
The list source, consent, freshness or bank-system access.

The table preserves the differences between the advertised products and currencies.

Card	Advertised subject	Asking term	Interpretation limit
B06	VPN access	200 XMR	No observed sale or validated access
B07	Bank account	15,000 TL	No observed payment or usable account verified
B07	Exchange account	5,000 TL	Separate asking term, not a sum per person
B08	Messaging-number service	850 TL	No subscriber-number access established
B08	eSIM service	100 USD	Different product; no currency conversion implied
B09	Banking-promotion leads	Price not established here	No verified provenance or bank intrusion

Do not convert an asking price into criminal revenue. The post may describe a negotiable amount, an incomplete package or a service that was never delivered. This report records no test purchase and no completed transaction.

8.5 Police campaign reporting

The Interior Ministry's 26 October notice reports 275 suspects detained in operations across 35 provinces. It describes alleged fraud, payment intermediation and unauthorised access to mobile-banking and gaming accounts, among several offence categories [S32].

The same notice reports 5,062 cybercrime operations and 21,378 detained suspects from 1 January to 22 October 2026. These are official operational statistics. They are not a count of cyberattacks, proven offences, unique victims or convictions [S32].

The notice also contains access-restriction statistics. They are not needed for this report's defensive conclusions and are not reproduced. The report takes no position on government access decisions.

The practical connection is between customer contact, identity checks and transaction controls. A fraud report should preserve the contact channel and account chronology, alongside technical evidence. Security and fraud teams should avoid opening separate investigations that cannot exchange findings.

The cutoff-week check adds a 16 November police notice. It reports 167 suspects detained during operations centred on 12 provinces, covering several alleged cybercrime categories. Phishing and unauthorised mobile-banking account access appear among them. The notice reports 32 remands and 31 judicial-control decisions. These are procedural counts, not convictions or a count of bank-system intrusions [S91].

A separate 14 November notice describes an investment-themed fraud investigation across 7 provinces, with 12 suspects detained. It reports 3.2 billion lira in account movements. Turnover is not verified victim loss, recovered money or criminal profit. Fraud teams should test the handoff from a credible customer report to transaction review and evidence preservation [S92].

The two notices are separate campaign reports. Their suspects and transactions cannot be assumed disjoint or linked to the account advertisements retained for this report. Neither notice validates a particular seller's claimed capability.

8.6 Reused records inside a software service

A 17 September press report describes 5 suspects detained in a software-company investigation. It reports a lookup interface covering non-members and records leaked previously from different sources [S98]. This is attributed reporting, without an original police case record in the package. Detention is not conviction. The report does not establish a new national-register intrusion or a working connection to the live register.

For buyers of data-enrichment or compliance software, a field label is insufficient evidence of provenance. Require the supplier to explain authority, retention, permitted users and access records. Investigate unexplained information about people outside the agreed service population. The document and receipt advertisements in F57 also justify independent verification of high-impact identity or payment changes [S1].

KEY TAKEAWAYS

01
Account-sourcing advertisements are not evidence of completed account transfers.

02
Card figures describe a narrow retained-post population, not national fraud loss.

03
Join identity, communications and transaction evidence under one escalation owner.

CHAPTER 09

Banking and finance deep dive

THIS CHAPTER ANSWERS

Which external banking signals belong with identity, fraud and supplier owners?

30

selected banking and finance domains

9.1 The financial portfolio and issuer subset differ 66

9.2 The issuer-matched exposure view 67

9.3 Clear-text card observations remain a narrow view 67

9.4 Supplier identity is part of the financial control surface 68

9.5 Four workflows to test together 68

9.6 Board reporting without false precision 69

CHAPTER 09

Banking and finance deep dive

IN SHORT

The banking and finance portfolio has at least 175,336 device associations and 393,538 credential-record associations. Current market listings concern 18 of its 30 selected domains. These observations require account validation; they do not establish bank infrastructure intrusions. The issuer-matched subset and clear-text card observations have narrower scopes. Test a joint identity, fraud and supplier workflow, with separate evidence for account validity, transaction abuse and data handling.

9.1 The financial portfolio and issuer subset differ

The selected portfolio contains 30 banking and finance domains. The exposure-to-card view matches 14 issuer domains within that portfolio. It does not turn all 30 assessments into card issuers or establish a complete list of licensed banks [S2][S4].

Financial portfolio measure	Observation	Decision boundary
Selected domains	30	Purposive portfolio, not a banking-system census
Device associations, at least	175,336	Customer and employee relationships can overlap
Employee-device associations	1,643	Validate managed endpoint and account ownership
Credential-record associations	393,538	Historical or repeated records can remain visible
Domains with current market listings	18	Advertisement, not a tested active account
Document associations	128	Sensitivity and authorisation remain unverified

Employee-device associations are presented within the device view. They must not be added to the device total. Credential and document records have their own units, and the same record can relate to several domains.

The financial portfolio accounts for 8.5% of credential-record associations across the 250-domain national portfolio. That share describes the retained exposure population. It does not measure financial fraud, the number of active customer accounts or the sector's share of national cyber incidents.

A high-volume customer-facing service can produce many device associations outside its managed estate. The first task is to establish whether a credible observation concerns a customer, an employee, a supplier or another context. The owner and response follow that distinction.

9.2 The issuer-matched exposure view

The following table concerns only the 14 matched issuer domains. It must not be compared with the full financial portfolio without retaining its smaller denominator [S2][S4].

Matched issuer measure	Observation
Matched issuer domains	14
Domains with non-employee device associations	14
Non-employee device associations	165,078
Domains with employee-device associations	12
Employee-device associations	1,533
Domains with current listings	12
Issuer domains with observed clear-text cards	12

The non-employee device figure is a service-associated population. It is not a count of bank-operated customer endpoints, independent customers or people with confirmed account abuse. Several banks can appear in material associated with the same device.

The largest 3 issuer-domain populations contribute 35.9% of the matched non-employee device associations. This concentration supports allocating validation capacity where the evidence is largest. It does not rank banks by control quality or establish that their systems produced the records.

For current listings, identity operations should establish service relevance and active-account status. Endpoint responders should separately determine whether an employee association concerns a managed device and whether it remains relevant. Fraud teams should investigate any corroborating customer-account or transaction signal.

A case can move between those teams as evidence develops. Preserve the original observation date, the account relationship and the reason for escalation. A joined table helps coordinate work; it does not supply the missing proof linking an advertisement to a current intrusion.

9.3 Clear-text card observations remain a narrow view

SCOPE OF THE CARD FIGURES

These figures cover only payment cards appearing in clear text in posts retained for this report. Brandefense detects stolen cards through other methods outside this edition. The figures do not measure card theft, current validity, fraud loss or total Brandefense coverage.

The enlarged retained corpus contains 860 distinct Türkiye-associated cards in 733 posts. The disjoint groups contain 578 issuer-attributed cards and 282 country-only cards. Country-only observations cannot be assigned to a named bank in the exposure view [S4].

The matched issuer view contains 579 card-to-issuer associations. Its largest 3 issuer counts contribute 66.3% of those associations. A card can have repeated or conflicting issuer context; the disjoint national card total remains the governing distinct-card number.

A card's appearance does not identify the source of exposure. It could concern a customer device, a merchant, another processor or historical material. This report does not establish an issuer infrastructure incident from a card observation.

Customer protection should follow the issuer's authorised validation and fraud processes. Record whether the account remains active, whether protective action is needed, and whether transaction evidence supports abuse. Avoid equating an externally posted status label with a current issuer verdict.

9.4 Supplier identity is part of the financial control surface

The investment-services notification describes phishing aimed at a foreign processor's staff. It says unauthorised access reached a multi-factor single-sign-on platform. Whether data was exported was unconfirmed. The notice also states limits on the information involved [S17].

For a financial organisation, the useful test is whether its processor can explain which tenant, accounts and data the event concerns. A supplier's general statement that MFA exists does not answer whether recovery, enrolled devices and active sessions were investigated.

Do not treat this notice as proof that all MFA was technically defeated. It describes a particular incident and leaves mechanism and export questions open. Require scoped evidence before applying the same conclusion elsewhere.

9.5 Four workflows to test together

Account recovery. Use synthetic customer identities to test whether public or historically exposed personal facts can authorise a high-impact change. A successful test means the approved process rejects the unauthorised request and records the reason.

New payees and payment changes. Test an urgent request delivered through a believable message. Require an independent, previously enrolled verification route. Record whether the operator can override the control and who reviews that decision.

Supplier notification. Start with a processor reporting a possible identity incident but incomplete data-export evidence. Check whether legal, fraud and security teams can preserve different questions without delaying a necessary initial notice.

Session containment. After a corroborated account incident, demonstrate that the relevant sessions, recovery routes, mailbox rules and delegated access have been reviewed. Closing only the password-reset ticket is insufficient completion evidence.

9.6 Board reporting without false precision

A useful board dashboard measures validation, containment, recovery and notification. Examples include the number of credible signals awaiting an owner, time to disposition, completion of a recovery exercise and unresolved supplier dependencies.

Keep the exposure, card and ransomware populations separately labelled and dated. Use their own denominators when reporting a change. Compare successive snapshots only after checking that the assessed scope remains comparable.

KEY TAKEAWAYS

01
The financial portfolio, issuer-matched view and clear-text card population have different denominators.

02
Validate active identities, employee devices and customer abuse through their respective owners.

03
Link supplier, session and recovery evidence before treating a joined external signal as a confirmed banking incident.

CHAPTER 10

Regulatory and national response

10

THIS CHAPTER ANSWERS

Which duties are in force, and which November texts remain proposals?

72 hours

KVKK Board notification period after awareness

10.1 Official instruments and applicability 71
10.2 Notification clocks need an event chronology 72
10.3 Statutory sanctions require precise labels 72
10.4 An operational compliance exercise 73

CHAPTER 10

Regulatory and national response

IN SHORT

The personal-data notification clock and the Cybersecurity Law's reporting duty are different obligations. Law 7545 requires covered service providers to report detected vulnerabilities or cyber incidents without delay. KVKK's decision interprets notification to the Board as no later than 72 hours after awareness. November resilience and audit texts remained consultations. Map the applicable duties with legal counsel and test an initial notification while facts are incomplete.

10.1 Official instruments and applicability

The table summarises the sources read for this edition. Legal owners should determine applicability to their organisation and the current implementing instruments [S8][S9][S10][S11].

Instrument	Status and scope	Duty or significance	Practical owner
Law 6698, Article 12, and decision 2019/10	Personal-data breach notification framework	Notify the Board without delay, no later than 72 hours after awareness; notify affected people as soon as reasonably possible after identification [S8]	Privacy and legal
Law 7545, Articles 2 and 7	In force from 19 March 2025; broad cyber-space scope with stated exclusions	Covered entities must report detected vulnerabilities or cyber incidents to the Presidency without delay [S9]	Legal and incident response
Law 7545, Article 8	Statutory audit powers and cooperation duties	Maintain required access and infrastructure within the notified period for a lawful audit [S9]	Legal and infrastructure
Law 7545, Article 18	Cybersecurity products and companies	Export and control-changing transactions have notification or approval requirements as specified [S9]	Legal and corporate governance
Resilience draft	Consultation opened 18 November 2026	Proposed graded cyber obligations and incident-team responsibilities; not treated as enacted duties [S10]	Compliance and security
Audit draft	Consultation opened 18 November 2026	Proposed audit procedures and risk-based oversight; not treated as enacted duties [S11]	Compliance and assurance

The Cybersecurity Law's scope exclusions concern specified intelligence activities and activities under the laws named in Article 2. They are not a blanket exemption for all public bodies. Article 7(c)'s procurement wording specifically concerns public institutions and critical infrastructure [S9].

The November consultation announcements both request comments by 3 December 2026. Neither announcement supplies an effective date for the proposed duties [S10][S11]. Keep drafts in the forward-looking compliance register, separate from obligations already in force.

10.2 Notification clocks need an event chronology

KVKK decision 2019/10 interprets the law's phrase about prompt notification as 72 hours after awareness for notice to the Board. It allows staged information where all required facts are not available together. A justified delay must be explained [S8].

The same decision calls for notification to affected people as soon as reasonably possible after they are identified. It also requires a processor to inform the controller without delay. An overseas controller can have notification responsibilities where the specified Türkiye-related conditions apply [S8].

Do not wait for a final person count or a completed forensic report before assessing these duties. Start an event chronology that records detection, internal escalation, awareness, supplier notice and subsequent findings. Legal owners should record why a particular clock applies.

The Cybersecurity Law separately requires covered entities to notify detected vulnerabilities or cyber incidents without delay [S9]. That wording should not be replaced with a general 72-hour cyber incident deadline. A sector-specific duty may also apply and requires its own assessment.

10.3 Statutory sanctions require precise labels

The following are bands written in the consolidated law, not a calculation of an indexed amount payable in 2026. They should not be applied mechanically to a particular organisation [S9].

Provision	Conduct	Statutory band	Qualification
Article 16(10)	Failure to fulfil Article 7(1)(a), (b) or (c) duties	1,000,000–10,000,000 TL	Distinct from the Article 18 band
Article 16(10)	Failure to fulfil Article 18 duties	10,000,000–100,000,000 TL	Product and company obligations have their own scope
Article 16(11)	Failure to fulfil Article 8(4) audit obligations	100,000–1,000,000 TL	The commercial-company rule differs
Article 16(11)	Same audit obligations for commercial companies	Up to 5% of gross sales	Statutory minimum 100,000 TL; audited annual financial statements specified

Article 16 also contains criminal provisions with different elements and exceptions. Article 17 governs administrative-penalty procedure. This report does not infer an offence or sanction from an advertisement, listing or the absence of a particular public statement.

The consolidated law records an amendment effective on 31 July 2026. That matters when comparing older summaries with the current Article 16 wording [S9]. No claim about a particular enforcement case is made here.

10.4 An operational compliance exercise

Start with an incomplete supplier alert: an account was accessed, some customer fields may be involved, and data export is unresolved. Ask the team to identify the controller, processor, affected service and evidence owner.

Then test the initial-notice process. Can the organisation explain known facts, uncertainties, containment and the next update? Can it preserve a dated rationale for the applicable duty without waiting for every question to close?

Finally, separate public communication from legally required reporting. A public status message, a regulator notice and a customer notice have different purposes and recipients. Record the decision and approval owner for each.

KEY TAKEAWAYS

01
The KVKK clock starts from awareness and differs from reporting without delay under Law 7545.

02
November consultations remain drafts in this edition.

03
Use the current consolidated law and keep statutory penalty bands separate from payable amounts.

CHAPTER 11

Outlook

11

THIS CHAPTER ANSWERS

Which judgements support planning, and what evidence would change them?

5

bounded judgements with revision signals

11.1 Key judgements 75

11.2 Evidence that would change priorities 75

11.3 Conditional planning scenarios 76

CHAPTER 11

Outlook

IN SHORT

The strongest planning signals concern continuity, identity validation and supplier readiness. Underground activity can keep older identity information useful for impersonation, while listings and official disclosures remain different evidence streams. The selected exposure portfolio supports anonymous sector validation, with no national prevalence estimate. Treat the scenarios below as planning assumptions and change priorities when current account, supplier or service evidence changes.

11.1 Key judgements

Confidence applies to the proposition stated in each row. It does not certify every claim made by an actor or every future outcome.

Judgement	Confidence	Basis and limit	Revision signal
Continuity planning deserves priority	High for the planning need	Listings and official ransomware disclosures; no national attack total [S3][S12][S18]	Repeated recovery failures or new verified service dependencies
Identity validation needs joint ownership	High for the control need	Official mailbox account abuse and supplier identity notice [S15][S17]	Corroborated sessions, recovery changes or unauthorised exports
Large data offers will continue to require triage	Medium	Repeated offers and explicitly older material; no sale frequency inferred [S1]	Independent provenance or a fresh controller confirmation
Supplier notification can determine response speed	Medium	Several notices begin with processor information; no single shared campaign established [S16][S20][S21]	A supplier cannot identify affected tenants or contact owners
Exposure validation needs several owners	High for the control need	Selected device, credential and listing populations; no sector assurance ranking [S2]	Current account matches, managed endpoint evidence and validated supplier relationships

11.2 Evidence that would change priorities

A current account match. A credible offer that matches an active account or recent unauthorised session should move from intelligence triage into incident response. An old, remediated account should receive a documented closure rather than an automatic repeat reset.

An official correction. A controller can revise affected populations or data categories as an investigation develops. Reconcile new statements against the earlier account. Do not silently retain a superseded headline number.

A supplier scope failure. If a processor cannot identify affected tenants or export paths, the controller may need stronger containment and a broader impact assessment. That decision should follow the actual service and contractual relationship.

A verified service disruption. A DDoS announcement becomes materially different when service telemetry and provider information establish an impact. Preserve the distinction between the claimed traffic, measured availability and the business consequence.

A changed exposure snapshot. A new dated observation can alter validation priorities when its account and service context is established. Check whether the portfolio and observation scope remain comparable. Reassess the evidence before updating an approved headline.

11.3 Conditional planning scenarios

These are planning assumptions, not forecasts of attack probability or financial loss.

If this occurs	Planning response	Evidence needed to close
A credible dataset claim names a processor	Convene privacy, procurement and incident response	Tenant scope, affected fields and a dated notification decision
A valid employee session appears unauthorised	Contain the account and assess related access	Session revocation, endpoint review and owner-approved recovery
A channel announces a Turkish DDoS target	Check mitigation readiness and application monitoring	Correlated service and provider evidence, or a documented no-match finding
Ransomware affects a shared infrastructure service	Activate independent recovery and business prioritisation	Tested restoration, integrity checks and business sign-off
A customer is contacted using accurate identity facts	Use an independent verification route	Fraud assessment and confirmation through a trusted channel

KEY TAKEAWAYS

01
Change priorities when current evidence changes, not when a claim becomes louder.

02
Treat future scenarios as planning assumptions with clear closure evidence.

03
A changed exposure snapshot requires a fresh review of account and service context.

CHAPTER 12

Action plan

12

THIS CHAPTER ANSWERS

What should owners complete in thirty, sixty and ninety days?

90

days to demonstrate recovery and response readiness

12.1 Thirty, sixty and ninety days 78

12.2 Technical reference for the national PHP notice 80

12.3 By role 80

12.4 How Brandefense can help 81

CHAPTER 12

Action plan

IN SHORT

Begin with ownership, identity validation and notification readiness. Then test supplier access and restore an essential service. Close the programme with evidence that a business owner can assess. The schedule is a proposed plan, not a legal deadline. Trigger urgent containment earlier whenever a credible signal is corroborated by current account or service evidence.

12.1 Thirty, sixty and ninety days

The lanes connect each task to a completion artefact. Adapt the calendar to actual service criticality.

1Days 1–30	
Assign every credible external identity or access signal an owner	
OWNER SOC and identity	COMPLETION EVIDENCE Dated record with validation outcome and escalation decision
Validate active accounts and recent sessions when evidence matches	
OWNER Identity and incident response	COMPLETION EVIDENCE Account scope, session review and containment sign-off
Inventory processors holding customer, workforce and identity information	
OWNER Procurement and privacy	COMPLETION EVIDENCE Service-to-processor map with tested incident contacts
Distinguish the KVKK notification clock from other incident duties	
OWNER Legal and privacy	COMPLETION EVIDENCE Scenario chronology and approved initial-notice route
Confirm current national cyber coordination channels	
OWNER Incident response	COMPLETION EVIDENCE Contact test and internal runbook update
Review externally reachable PHP services against current vendor guidance	
OWNER Application and infrastructure owners	COMPLETION EVIDENCE Supported release evidence and worker restart verification [S24][S25][S26][S27][S28][S29]

2Days 31–60

Test recovery using protected backups and separate recovery access

OWNER
Infrastructure and business continuity

COMPLETION EVIDENCE
Restored service, integrity result and business acceptance

Exercise a processor identity incident with incomplete export evidence

OWNER
Supplier risk, privacy and SOC

COMPLETION EVIDENCE
Tenant scope, notification decision and next-update owner

Test customer recovery against realistic personal facts

OWNER
Fraud and customer operations

COMPLETION EVIDENCE
Failed unauthorised recovery attempt and recorded control outcome

Review mailbox rules, delegation and active sessions after corroborated abuse

OWNER
Messaging and identity

COMPLETION EVIDENCE
Closure checklist covering every affected control surface

3Days 61–90

Exercise a DDoS announcement followed by uncertain service symptoms

OWNER
Operations and communications

COMPLETION EVIDENCE
Correlated service evidence and approved status statement

Audit privileged supplier access and offboarding

OWNER
Procurement and identity

COMPLETION EVIDENCE
Removed obsolete access and approved exceptions

Review draft regulations without treating proposals as enacted duties

OWNER
Legal and compliance

COMPLETION EVIDENCE
Current obligation register with status and source dates

Review the programme with business owners

OWNER
CISO and leadership

COMPLETION EVIDENCE
Open risks, acceptance decisions and tested recovery evidence

12.2 Technical reference for the national PHP notice

The national notice on 21 October called for urgent review and updates [S24]. NVD records CVE-2026-109618 and CVE-2026-109619. The vendor advisories provide the branch-specific minimum fixes below [S25][S26][S27][S28].

Branch	Affected range shown	Minimum fix for both records
PHP 8.2	Before 8.2.35	8.2.35
PHP 8.3	Before 8.3.36	8.3.36
PHP 8.4	Before 8.4.27	8.4.27
PHP 8.5	Before 8.5.12	8.5.12

These are minimum fixes for the two specified records, not a recommendation to stop at those versions. Use current supported vendor releases and guidance, including worker restarts. Older branches require a supported migration or verified vendor remediation [S29]. No Turkish victim is attributed to either flaw by this report.

12.3 By role

Leadership should ask which service has been restored in an exercise, which supplier dependencies remain unresolved, and which credible signals lack an owner. A rising post count is not a substitute for those answers.

Security operations should keep the claim, observation and corroboration fields distinct. Record alternative explanations and close the loop with identity, privacy and business owners. Preserve evidence without distributing unnecessary personal information.

Infrastructure and identity teams should prove that containment removes sessions and delegated access as well as passwords. Test separation of production and recovery administration. Confirm a remediation result against the actual service.

Fraud and customer operations should test independent verification, account recovery and new-payee controls. Use realistic synthetic scenarios. Ensure the operator cannot override a failed check without an accountable exception.

Legal, privacy and procurement should maintain the event chronology, controller-processor map and current duty register. Draft proposals, statutory rules and contractual notice commitments need separate labels.

12.4 How Brandefense can help

Bring your domains, brands, critical services and security priorities to a Brandefense discussion. Use this report's cases to frame questions about external signals, validation and response ownership. Ask for scope, dates and evidence boundaries alongside any result.

Request a demo

KEY TAKEAWAYS

01
Give each action an accountable owner and reviewable completion evidence.

02
Treat corroborated current access as an urgent trigger before the planning calendar expires.

03
Complete recovery, supplier and notification exercises with business-owner sign-off.

APPENDICES

Appendices

A–F

THIS CHAPTER ANSWERS

Which populations and limitations define this edition?

4

distinct primary evidence populations

Appendix A. Method and limits 83
Appendix B. Evidence register 85
Appendix C. Sources 86
Appendix D. Glossary 88
Appendix E. Official disclosure register 89
Appendix F. Additional claim and market themes 96

Appendix A. Method and limits

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

A.1 Window and dates

The post window is 1 January–21 November 2026. November is partial. Exposure observations are dated 21 November; annual mention context ends on 18 November. Passive observations were collected on 21 November UTC, corresponding to 22 November locally.

Public sources were read during preparation on 22 November in Türkiye local time. Publication, claimed acquisition, intrusion, discovery and notification dates can differ. A post published during 2026 can describe data associated with an earlier event.

A.2 Underground posts

Brandefense Blackhole supplied the post observations. The Türkiye-tagged volume is 4,131,687. The separate retained narrative corpus contains 177,648 distinct posts. The assessed country-related archive supports reading of individual propositions [S1].

The archive and the tagged-post view have different coverage. Neither is presented as a subset of the other. A post can be a reply, relay, advertisement or commentary. Post counts therefore do not establish unique incidents, datasets, sellers or affected people.

Monthly country and comparator rows use the same stated post-date window. Visibility, tagging and source participation can differ between countries and periods. No attack-probability ranking, national prevalence estimate or causal trend is inferred from those totals.

Short quotations are authentic excerpts with omissions and protective labels where needed. Contact routes, victim indicators and personal sample rows are withheld. Stable public card identifiers permit reconciliation without exposing the underlying records.

A.3 Selected organisations and passive observations

The portfolio comprises 250 selected organisation domains in twelve sectors. Selection is purposive. Domains can represent brands, institutional services and related legal entities. Ownership and independence remain incompletely validated for part of the portfolio; the sample does not represent every organisation in Türkiye [S2].

Published sector cells contain 10–50 selected domains. Passive observations cover 239 resolving domains. Missing and inconclusive results remain distinct from the presence or absence of a configuration. A failed observation does not establish successful exploitation.

A.4 Organisation exposure

Atlas supplies the national headline rating of 66/100 (C) for the selected portfolio. Only that national rating is published. Anonymous sector tables describe device, employee, credential, listing and document observations. They do not disclose organisation scores or provide sector security rankings [S2].

Device figures describe observed associations. Customer devices are not automatically organisation-operated endpoints. Credential and document records can repeat across sources or domains. Employee-device associations are presented within the device view and must not be added to it.

A market listing is an advertisement, not a completed sale or proof of an active account. A document or mention can be public, historical or unrelated to abuse. Similar domain names require ownership and harmful-use validation before a phishing allegation.

The financial portfolio contains 30 selected domains. The issuer-matched subset contains 14 domains and retains its own denominator. Joining exposure and card observations supports coordinated validation; it does not establish a causal relationship or identify the system from which a record originated.

A.5 Card material

The figures cover only payment cards appearing in clear text in posts retained for this report. Brandefense detects stolen cards through other methods outside this edition. These figures do not measure card theft, current validity, fraud loss or total Brandefense coverage [S4].

The disjoint national groups contain 578 issuer-attributed cards and 282 country-only cards, totalling 860 across 733 posts. Issuer associations can overlap. Appearance does not establish an issuer infrastructure incident or a valid transaction capability.

A.6 Ransomware

Ransompedia supplies the accepted listing snapshot for Türkiye and the four comparators. Listings are dated by publication. Listings are claims. They can repeat organisations, and listing dates need not identify intrusion dates [S3].

The Türkiye total is 157 listings. The 2025 comparator contains 53 across a full year; the 2026 window ends at the stated cutoff. Unequal duration and differences in visibility and country classification prevent a matched-period growth claim or national risk ranking.

A.7 Public reporting and incident coverage

Official controller disclosures, national cyber notices, police reporting, vendor research and press reporting supply distinct evidence. The package contains 57 source-read controller notifications. Campaign announcements, underground claims and listing records are separate populations; they cannot be added into a unique national incident count.

Some earlier archive links redirect or remain unreadable. Those leads retain explicit actions in the coverage register. A missing or unread source is not evidence that an event did not occur. The cutoff-week check covers 15–21 November and records newly discovered official campaign material separately.

External observations and reported statements do not replace an organisation's investigation. A faithfully recorded advertisement can still contain an inaccurate underlying assertion. The report therefore preserves unresolved provenance and outcome questions.

A.8 Confidence and political neutrality

High confidence can attach to a retained observation or a faithfully reported official statement. It does not automatically attach to the assertion inside a criminal advertisement. Medium confidence identifies a bounded interpretation. Unverified means supporting evidence is insufficient; it does not establish fabrication.

The report takes no position on governments, territorial questions, ethnicity, religion, elections or access decisions. State attributions remain the cited source's. Actor slurs and loaded framing are omitted. The Turkish edition preserves the same qualifications.

Appendix B. Evidence register

The seventeen post cards identify the evidence used in the main chapters. Post dates are not intrusion dates. Poster aliases are withheld except where a channel label is necessary to understand the specific announcement [S1].

Card	Posted	Venue	Alias	Language	Chapter
B01	2026-01-04	forum	Withheld	English	4
B02	2026-01-24	forum	Withheld	English	4
B03	2026-02-05	forum	Withheld	English	4
B04	2026-10-25	forum	Withheld	English	4
B05	2026-11-15	forum	Withheld	English	4
B06	2026-11-17	forum	Withheld	English	4
B07	2026-02-18	forum	Withheld	Turkish	8
B08	2026-02-16	forum	Withheld	Turkish	8
B09	2026-10-09	forum	Withheld	English	8
B10	2026-11-13	forum	Withheld	English	4
B11	2026-11-05	forum	Withheld	English	4
B12	2026-10-17	forum	Withheld	English	4
B13	2026-11-07	telegram	Channel label	English and Arabic	6
B14	2026-11-20	telegram	Withheld	Turkish	6

Card	Posted	Venue	Alias	Language	Chapter
B15	2026-11-21	telegram	Withheld	Turkish	4
B16	2026-03-13	telegram	Not established	English	4
B17	2026-09-22	forum	Withheld	English	4

Appendix C. Sources

All external facts are limited to supporting passages read at source. A site-root citation marked as withheld protects an organisation that does not meet the public naming rule. Full source provenance is retained privately. Own research is identified separately from public webpages.

S1: Brandefense Blackhole, retained Türkiye-related posts. Own retained research; public aggregates in this report. Verified on 2026-11-22.

S2: Odin by Brandefense, selected-organisation exposure and passive observations. Own retained research; public aggregates in this report. Verified on 2026-11-22.

S3: Ransompedia, Türkiye and comparator listing snapshot. Own retained research; public aggregates in this report. Verified on 2026-11-22.

S4: Brandefense Blackhole, payment-card aggregate view. Own retained research; public aggregates in this report. Verified on 2026-11-22.

S5: DataReportal, Digital 2027: Turkey, 5 November 2026. Source. Verified on 2026-11-22.

S7: USOM, service transition notice. Source. Verified on 2026-11-22.

S8: KVKK, breach notification decision 2019/10. Source. Verified on 2026-11-22.

S9: Legislation Information System, consolidated Cybersecurity Law 7545. Source. Verified on 2026-11-22.

S10: Cybersecurity Presidency, resilience draft consultation, 18 November 2026. Source. Verified on 2026-11-22.

S11: Cybersecurity Presidency, audit draft consultation, 18 November 2026. Source. Verified on 2026-11-22.

S12: KVKK, Yıldız Teknik Üniversitesi notification, 7 October 2026. Source. Content corroborated on 2026-11-22; live availability unconfirmed.

S13: Yıldız Teknik Üniversitesi, public statement, 8 October 2026. Source. Verified on 2026-11-22.

S14: NTV, reporting on the university incident, 8 October 2026. Source. Verified on 2026-11-22.

S15: KVKK, municipal email-account incident, 21 October 2026. Source (article URL withheld). Verified on 2026-11-22.

S16: KVKK, retailer supplier incident, 30 September 2026. Source (article URL withheld). Verified on 2026-11-22.

S17: KVKK, investment-services supplier identity incident, 30 September 2026. Source (article URL withheld). Verified on 2026-11-22.

S18: KVKK, education foundation ransomware notification, 21 October 2026. Source (article URL withheld). Verified on 2026-11-22.

S19: KVKK, food retailer supplier notification, 21 October 2026. Source (article URL withheld). Verified on 2026-11-22.

S20: KVKK, e-commerce service notification, 27 October 2026. Source (article URL withheld). Verified on 2026-11-22.

S21: KVKK, membership association supplier notification, 23 September 2026. Source (article URL withheld). Verified on 2026-11-22.

S22: KVKK, jewellery retailer supplier notification, 23 September 2026. Source (article URL withheld). Verified on 2026-11-22.

S23: KVKK, food-delivery business incident, 7 October 2026. Source (article URL withheld). Verified on 2026-11-22.

S24: Cybersecurity Presidency, national PHP response, 21 October 2026. Source. Verified on 2026-11-22.

S25: NVD, CVE-2026-109618. Source. Verified on 2026-11-22.

S26: NVD, CVE-2026-109619. Source. Verified on 2026-11-22.

S27: PHP security advisory GHSA-w8hw-w9fx-j79w. Source. Verified on 2026-11-22.

S28: PHP security advisory GHSA-6wmf-4rv5-p3rp. Source. Verified on 2026-11-22.

S29: PHP, 2026 news archive and release guidance. Source. Verified on 2026-11-22.

S30: Acronis Threat Research Unit, JanaWare research, 14 April 2026. Source. Verified on 2026-11-22.

S31: Unit 42, Boggy Serpens Threat Assessment, 16 March 2026. Source. Verified on 2026-11-22.

S32: Interior Ministry, cybercrime operation notice, 26 October 2026. Source. Verified on 2026-11-22.

S33: Cybersecurity Presidency, common incident-response gaps, May 2026. Source. Verified on 2026-11-22.

S34: RFC Editor, RFC 7489: DMARC. Source. Verified on 2026-11-22.

S35: RFC Editor, RFC 7208: SPF. Source. Verified on 2026-11-22.

S36: RFC Editor, RFC 6376: DKIM. Source. Verified on 2026-11-22.

S37: RFC Editor, RFC 4033: DNSSEC. Source. Verified on 2026-11-22.

S38: RFC Editor, RFC 8446: TLS. Source. Verified on 2026-11-22.

S39: KVKK, port operator notification, 2026-10-27. Source (article URL withheld). Verified on 2026-11-22.

S40: KVKK, customer-service technology business notification, 2026-10-07. Source (article URL withheld). Verified on 2026-11-22.

S41: KVKK, technical-support business notification, 2026-11-04. Source (article URL withheld). Verified on 2026-11-22.

S42: KVKK, customer-service operations business notification, 2026-10-07. Source (article URL withheld). Verified on 2026-11-22.

S43: KVKK, e-commerce business notification, 2026-11-04. Source (article URL withheld). Verified on 2026-11-22.

S44: KVKK, insurer notification, 2026-11-11. Source (article URL withheld). Verified on 2026-11-22.

S45: KVKK, membership chamber notification, 2026-11-11. Source (article URL withheld). Verified on 2026-11-22.

S46: KVKK, university notification, 2026-10-21. Source (article URL withheld). Verified on 2026-11-22.

S47: KVKK, renal-health services business notification, 2026-10-21. Source (article URL withheld). Verified on 2026-11-22.

S48: KVKK, international travel business notification, 2026-11-04. Source (article URL withheld). Verified on 2026-11-22.

S49: KVKK, international pharmaceutical business notification, 2026-11-11. Source (article URL withheld). Verified on 2026-11-22.

S50: KVKK, education-services foundation notification, 2026-09-23. Source (article URL withheld). Verified on 2026-11-22.

S51: KVKK, food-delivery business notification, 2026-10-07. Source (article URL withheld). Verified on 2026-11-22.

S52: KVKK, hotel operator notification, 2026-11-04. Source (article URL withheld). Verified on 2026-11-22.

S53: KVKK, construction business notification, 2026-10-07. Source (article URL withheld). Verified on 2026-11-22.

S54: KVKK, hotel operator notification, 2026-11-04. Source (article URL withheld). Verified on 2026-11-22.

S55: KVKK, hotel operator notification, 2026-11-04. Source (article URL withheld). Verified on 2026-11-22.

S56: KVKK, international logistics group notification, 2026-11-11. Source (article URL withheld). Verified on 2026-11-22.

S57: KVKK, food-delivery business notification, 2026-10-07. Source (article URL withheld). Verified on 2026-11-22.

S58: KVKK, healthcare-investment business notification, 2026-10-07. Source (article URL withheld). Verified on 2026-11-22.

S59: KVKK, hotel operator notification, 2026-11-11. Source (article URL withheld). Verified on 2026-11-22.

S60: KVKK, beverage producer notification, 2026-11-04. Source (article URL withheld). Verified on 2026-11-22.

S61: KVKK, international airline notification, 2026-11-11. Source (article URL withheld). Verified on 2026-11-22.

S62: KVKK, clothing retailer notification, 2026-10-07. Source (article URL withheld). Verified on 2026-11-22.

S63: KVKK, hotel operator notification, 2026-11-04. Source (article URL withheld). Verified on 2026-11-22.

S64: KVKK, automotive retailer notification, 2026-11-04. Source (article URL withheld). Verified on 2026-11-22.

S65: KVKK, healthcare provider notification, 2026-10-21. Source (article URL withheld). Verified on 2026-11-22.

S66: KVKK, online leisure service notification, 2026-10-07. Source (article URL withheld). Verified on 2026-11-22.

S67: KVKK, health-products retailer notification, 2026-10-21. Source (article URL withheld). Verified on 2026-11-22.

S68: KVKK, online leisure service notification, 2026-10-07. Source (article URL withheld). Verified on 2026-11-22.

S69: KVKK, food retailer notification, 2026-10-21. Source (article URL withheld). Verified on 2026-11-22.

S70: KVKK, delivery business notification, 2026-11-04. Source (article URL withheld). Verified on 2026-11-22.

S71: KVKK, clothing retailer notification, 2026-09-23. Source (article URL withheld). Verified on 2026-11-22.

S72: KVKK, hotel operator notification, 2026-10-21. Source (article URL withheld). Verified on 2026-11-22.

S73: KVKK, travel agency notification, 2026-11-04. Source (article URL withheld). Verified on 2026-11-22.

S74: KVKK, hotel operator notification, 2026-11-04. Source (article URL withheld). Verified on 2026-11-22.

S75: KVKK, online retailer notification, 2026-09-23. Source (article URL withheld). Verified on 2026-11-22.

S76: KVKK, sports retailer notification, 2026-11-04. Source (article URL withheld). Verified on 2026-11-22.

S77: KVKK, medical-device business notification, 2026-11-04. Source (article URL withheld). Verified on 2026-11-22.

S78: KVKK, food-delivery business notification, 2026-10-07. Source (article URL withheld). Verified on 2026-11-22.

S79: KVKK, international hotel group notification, 2026-10-21. Source (article URL withheld). Verified on 2026-11-22.

S80: Memurlar.net, airline statement, 4 November 2026. Source (article URL withheld). Verified on 2026-11-22.

S81: Directorate of Communications, online public-service statement, 10 June 2026. Source (article URL withheld). Verified on 2026-11-22.

S83: DataGuidance, telecommunications notification summary, 5 February 2026. Source (article URL withheld). Verified on 2026-11-22.

S85: KVKK, online retailer notification, 2026-09-23. Source (article URL withheld). Verified on 2026-11-22.

S86: KVKK, international exchange-services business notification, 2026-09-30. Source (article URL withheld). Verified on 2026-11-22.

S87: KVKK, clothing retailer notification, 2026-10-07. Source (article URL withheld). Verified on 2026-11-22.

S88: KVKK, diversified business group notification, 2026-10-07. Source (article URL withheld). Verified on 2026-11-22.

S89: KVKK, insurer notification, 2026-10-07. Source (article URL withheld). Verified on 2026-11-22.

S90: KVKK, airline notification, 2026-11-11. Source (article URL withheld). Verified on 2026-11-22.

S91: Interior Ministry, cybercrime operations in twelve provinces, 16 November 2026. Source. Verified on 2026-11-22.

S92: Interior Ministry, investment-themed fraud operation, 14 November 2026. Source. Verified on 2026-11-22.

S93: MC Legal, review of twenty-eight controller notifications, 18 September 2026. Source. Verified on 2026-11-22.

S94: InfoStealers (Hudson Rock), FortiBleed research, 17 June 2026. Source. Verified on 2026-11-22.

S95: UK National Cyber Security Centre, Fortinet campaign guidance, 18 June 2026. Source. Verified on 2026-11-22.

S96: QUIRSO, virtualisation-management exploitation research, 10 August 2026. Source. Verified on 2026-11-22.

S97: NVD, CVE-2026-59310 record. Source. Verified on 2026-11-22.

S98: Sabah, software-company investigation report, 17 September 2026. Source (article URL withheld). Verified on 2026-11-22.

S99: Broadcom, vCenter security response matrix, updated 19 August 2026. Source. Verified on 2026-11-22.

S100: IETF, RFC 6797: HTTP Strict Transport Security (HSTS). Source. Verified on 2026-11-22.

Appendix D. Glossary

Term	Plain meaning
Claim	Something a poster or listing asserts, requiring separate verification

Term	Plain meaning
Controller	The party determining the purposes and means of personal-data processing
Processor	A party processing personal data on the controller's behalf
SSO	A shared sign-in arrangement used to access connected services
MFA	Authentication requiring more than one type of evidence
KYC	Identity checks used when establishing or maintaining a customer relationship
Session	A continuing authenticated interaction, which can outlast a password change
DMARC	A published domain policy for handling messages that fail relevant email authentication checks
SPF	A domain's declaration of authorised email-sending infrastructure
DKIM	Email signing that lets a recipient check a message signature
DNSSEC	DNS signing intended to support authenticity and integrity checks
TLS	A protocol protecting a connection, separate from application authorisation
HSTS	HTTP Strict Transport Security: a website policy telling browsers to use HTTPS for later connections [S100]
DDoS	Distributed traffic intended to exhaust service availability
SOME	A cyber incident response team in the Turkish coordination framework
Ransomware listing	A public extortion-site entry, treated here as a claim
Analytical model	A labelled interpretation connecting defensive dependencies without asserting observed transactions

Appendix E. Official disclosure register

This register adds 47 source-read controller notices to the 10 notices discussed earlier, for 57 official notifications. It is a disclosure register, not a count of distinct attacks. The date column is the Board decision date. Underlying activity, discovery and publication can fall on different dates. Some notices concern foreign controllers or historical activity. Their appearance here does not establish a new intrusion in Türkiye. No affected-person figures are added together.

The earlier notices are the university, municipal mailbox, retail supplier, investment-services supplier, education foundation, food retailer, e-commerce service, membership association, jewellery retailer and food-delivery business [S12][S15][S16][S17][S18][S19][S20][S21][S22][S23].

Names remain withheld under the same publication rule used in the main report. Source identifiers permit reconciliation without making the role descriptions identifying. These are selected disclosures found during preparation; earlier archive coverage remains incomplete.

Source	Board decision	Organisation role	Stated evidence and boundary
[S50]	2026-09-23	Education-services foundation	Web-hosting supplier incident notified 2026-09-12; 68 customers. Identity, contact and password-hash fields reported.
[S71]	2026-09-23	Clothing retailer	Processor-library exploitation notified 2026-09-10; 85,722 people. Identity, contact and transaction-security categories.
[S75]	2026-09-23	Online retailer	Unauthorised e-commerce supplier database access notified 2026-09-14. Supplier estimated 473,284 end customers and 54 management-panel users; controller could not establish the exact population.
[S40]	2026-10-07	Customer-service technology business	Ransomware detected 2026-09-30; workforce, applicant and call-record categories. Export not established; population unresolved.
[S42]	2026-10-07	Customer-service operations business	Ransomware detected 2026-09-30; workforce, applicant and call-record categories. Separate controller notice; do not count it as a separate technical event without corroboration.
[S51]	2026-10-07	Food-delivery business	Unauthorised processor-system access notified 2026-09-30. Customer and workforce data categories; population under assessment.
[S53]	2026-10-07	Construction business	External access and encryption detected 2026-10-03. Personal-data scope and population remain under investigation.
[S57]	2026-10-07	Food-delivery business	Unauthorised processor-system access notified 2026-09-30. Customer and workforce categories; population unresolved.

Source	Board decision	Organisation role	Stated evidence and boundary
[S58]	2026-10-07	Healthcare-investment business	External access and encryption detected 2026-10-03. Personal-data scope and population remain under investigation.
[S62]	2026-10-07	Clothing retailer	Processor-library vulnerability; supplier notice 2026-09-29. Customer and management-account password hashes among the reported fields; population unresolved.
[S66]	2026-10-07	Online leisure service	Call-centre processor encryption detected 2026-09-30; voice and call-detail records. No export evidence initially found; unauthorised access not ruled out; population unresolved.
[S68]	2026-10-07	Online leisure service	Call-centre processor encryption detected 2026-09-30; voice and call-detail records. Separate controller notice; no confirmed export or affected-person figure.
[S78]	2026-10-07	Food-delivery business	Unauthorised processor-system access notified 2026-10-01. Customer and workforce identity, contact, location, transaction and financial categories; population unresolved.
[S46]	2026-10-21	University	Application vulnerability; 109 people affected. Detected 2026-10-14 following a national cyber-centre notification; identity, contact and location categories.
[S47]	2026-10-21	Renal-health services business	Employee voice phishing; one account, a CRM system and an internal directory file involved. Start 2026-08-04; detection 2026-10-06. Population unresolved.
[S65]	2026-10-21	Healthcare provider	Ransom note and encrypted database reported. Health, identity, contact and financial records potentially involved; encrypted files prevented an initial population count. The notice supplies an incomplete detection date.

Source	Board decision	Organisation role	Stated evidence and boundary
[S67]	2026-10-21	Health-products retailer	Processor-library exploitation notified 2026-09-10; 50,636 people. Identity, contact and password-hash fields reported.
[S69]	2026-10-21	Food retailer	Processor-library exploitation notified 2026-10-07. Maximum possible population: 15,303 end customers and 18 management-panel account holders, stated separately.
[S72]	2026-10-21	Hotel operator	Suspected account access affecting corporate email and infrastructure; categories, dates, export and affected population under investigation. Do not promote possible access into confirmed export.
[S79]	2026-10-21	International hotel group	Employee-account social engineering; access dated 2026-06-05–2026-06-06, detected on the first day. 9,550 customers; the notice does not establish a Türkiye-only population.
[S39]	2026-10-27	Port operator	Supplier help-desk access bypass and password changes; activity began 2026-10-12 and was detected 2026-10-19. Initial population: 855 people.
[S41]	2026-11-04	Technical-support business	Unauthorised access to processor-held chat material. 624 chat records; affected people not yet counted. Records and people are different units.
[S43]	2026-11-04	E-commerce business	Processor-held chat records dated 2022 accessed without authorisation; 9,882 people. The record age does not date the intrusion.
[S48]	2026-11-04	International travel business	Web-reservation application flaw; possible access concerning at most 2,392 people. Malicious customer emails observed 2026-10-10, technical evidence found 2026-10-12.

Source	Board decision	Organisation role	Stated evidence and boundary
[S52]	2026-11-04	Hotel operator	Unauthorised processor-system access detected 2026-10-25. Customer identity, contact and transaction categories; population unresolved.
[S54]	2026-11-04	Hotel operator	Unauthorised processor-system access detected 2026-10-23. Customer identity, contact and transaction categories; population unresolved.
[S55]	2026-11-04	Hotel operator	Unauthorised processor-system access detected 2026-10-26. Customer identity, contact and transaction categories; population unresolved.
[S60]	2026-11-04	Beverage producer	Unauthorised processor-system access detected 2026-10-23. Customer identity, contact and transaction categories; population unresolved.
[S63]	2026-11-04	Hotel operator	Unauthorised processor-system access detected 2026-10-26. Customer identity, contact and transaction categories; population unresolved.
[S64]	2026-11-04	Automotive retailer	Unauthorised access to processor-held chats; 8,268 chat records, affected people unresolved. Limited samples include names, phones, vehicle plates and appointments.
[S70]	2026-11-04	Delivery business	Unauthorised access to processor-held chat records dated 2022; 3,217 people. Older record dates do not establish an older intrusion.
[S73]	2026-11-04	Travel agency	Unauthorised processor-system access detected 2026-10-24. Customer identity, contact and transaction categories; population unresolved.
[S74]	2026-11-04	Hotel operator	Unauthorised processor-system access detected 2026-10-23. Customer identity, contact and transaction categories; population unresolved.

Source	Board decision	Organisation role	Stated evidence and boundary
[S76]	2026-11-04	Sports retailer	Unauthorised access to cloud customer-service processor records: 541 chat records concerning 383 people. Counts describe different units.
[S77]	2026-11-04	Medical-device business	Access began 2026-10-14, detected 2026-10-23; some data exported. Business contacts mainly involved; patient identifiers, device details and hearing-test material possibly included. Population unresolved.
[S44]	2026-11-11	Insurer	Historical supplier disclosure: unauthorised access dated 2022-01-15 and 2022-02-14. Included as a disclosure inside the window; excluded from any new-event interpretation for 2026.
[S45]	2026-11-11	Membership chamber	SQL injection detected 2026-11-02; membership-database access and export reported. Database stopped; general accounting system reported unaffected. Population unresolved.
[S49]	2026-11-11	International pharmaceutical business	IT-impersonation voice phishing at a subprocessor affected cloud accounts. At most 18 people in the processing population; actual affected population under investigation. Some pseudonymised health/genetic material potentially involved.
[S56]	2026-11-11	International logistics group	Unauthorised access to an employee-survey processor analytics system detected 2026-11-02; 10,622 employees in Türkiye affected.
[S59]	2026-11-11	Hotel operator	Attack detected 2026-10-27 blocked a server and guest wireless network. Guest personal information reportedly obtained; population unresolved.

Source	Board decision	Organisation role	Stated evidence and boundary
[S61]	2026-11-11	International airline	Reservation-processor access dated 2023-08-10–2026-09-23; supplier notice received 2026-11-03. Population unresolved. Publication in Türkiye does not locate the intrusion there.
[S85]	2026-09-23	Online retailer	Processor notice received 2026-09-14; 4,989 end customers and 20 management-panel account holders. Identity, contact and password-hash fields reported.
[S86]	2026-09-30	International exchange-services business	Application-upload subsystem lacked URL authentication; automated access obtained application documents. Start 2026-09-04; detection 2026-09-09; 7,591 customers. A Türkiye-only population is not established.
[S87]	2026-10-07	Clothing retailer	Ransomware activity dated 2026-09-28–2026-09-29, detected on the latter date. Entry path, affected groups, categories and population unresolved.
[S88]	2026-10-07	Diversified business group	External access and encryption started and were detected 2026-10-03. Workforce, user and customer categories; affected population could not be estimated.
[S89]	2026-10-07	Insurer	Processor incident detected 2026-09-30; one day of voice recordings encrypted. 161 call recordings inaccessible; no conversion to a person count.
[S90]	2026-11-11	Airline	Unauthorised use of an administration password in an IT request/development system; password acquisition route unresolved. Start 2026-10-12; detection 2026-10-26; 11,762 staff and users, identity/contact categories.

Appendix F. Additional claim and market themes

These themes consolidate further retained narratives alongside the nine detailed cases. They are source claims and market propositions, not additional confirmed incidents. Dates identify retained posts or their observed range. Different rows can overlap; several posts can repeat one offer. The private coverage register preserves each assessed item and its publication disposition.

The register omits personal sample rows, contact routes and identifying victim characteristics. Sparse filenames, unsupported secondary reports, foreign-target claims and unnecessary sensitive personal allegations receive explicit exclusions in the coverage record. Those exclusions do not establish that an alleged event did not happen.

Reference	Post dates	Role or topic	Proposition in the retained narrative	Evidence boundary
F01	2026-01-04	Electronic-money services	A post alleges release of a payment-service backend's source code. [S1]	Code possession, production access and customer-data impact are unverified.
F02	2026-01-06	Transport records	An offer describes a large transport-related record collection and promises more terminal data. [S1]	Provenance, unit meaning and any relationship to an operational system remain unresolved.
F03	2026-01–2026-02	Telecommunications	Advertisements offer operator-panel or API access; a later seller dispute claims a connection to a regulator notice. [S1]	The seller asserts the linkage. No common source, continuing access or causal sequence is independently established.
F04	2026-01–2026-05	Education systems and accounts	Posts allege education-portal access, official-account social engineering and broader university access. [S1]	Separate narratives do not verify institutional reach, a shared operator or the poster's claimed entry route.
F05	2026-01-23–2026-01-24	Municipal transport	A repeated claim describes 2,255 vehicles and operational, location and video-device reference fields. [S1]	No live stream access or control of vehicles is demonstrated.
F06	2026-01–2026-11	Public-service accounts	Posts offer credentials, account logs or access to individual public-service accounts. [S1]	Account material does not establish a breach of the service infrastructure; some offers explicitly refer to older dates.

Reference	Post dates	Role or topic	Proposition in the retained narrative	Evidence boundary
F07	2026-01–2026-11	Identity and lookup markets	Offers combine identity, family, address, property, employment and education records with lookup services or offline installations. [S1]	Different archives and service claims cannot be added into unique people or one new intrusion.
F08	2026-01–2026-11	Historical dataset circulation	Several catalogues or reposts explicitly label their material with earlier years. [S1]	Publication in the reporting window does not make the underlying acquisition a new event.
F09	2026-02-17	Insurance services	A seller claims privileged access across several insurers and sector-information services. [S1]	A list of brands is not a list of confirmed incidents; credentials and privileges remain unverified.
F10	2026-01–2026-11	Account credentials and payment cards	Offers describe identity-linked credentials, card material and mobile-banking password data. [S1]	These claims do not demonstrate an intrusion into bank infrastructure or successful transactions.
F11	2026-02–2026-11	Individuals and online accounts	Service menus advertise account intrusion, impersonation, harassment and personal-data lookup capabilities. [S1]	A capability advertisement supplies no verified victim, successful action or national incident count.
F12	2026-02–2026-11	Online retail	Distinct posts offer a customer dump, allege extortion, claim database access or describe payment-data theft. [S1]	The narratives are not linked into one campaign. Claimed legal correspondence and access remain unverified.
F13	2026-02-25	Gaming and hosting services	A DDoS seller claims gaming outages and routing effects during its own tests. [S1]	Self-reported effects are not independently measured outages; no infrastructure testing was undertaken for this claim.
F14	2026-03–2026-04	Fixed-line customers	Complaint-management data and separate customer-data reuploads carry earlier date labels; some source claims point to a third party. [S1]	Different advertised volumes and datasets are not reconciled into one incident or a mobile-customer population.
F15	2026-04–2026-11	Advertising and cash-out markets	Advertisements offer card-funded advertising and payment cash-out services. [S1]	Advertised spending, bypass capability and proceeds are not verified losses or proof of platform intrusion.

Reference	Post dates	Role or topic	Proposition in the retained narrative	Evidence boundary
F16	2026-04–2026-11	Marketplace users	Posts describe seller impersonation, staged fees, task-earning lures and verified-account stock. [S1]	Brand impersonation and account trading do not establish access to the legitimate platform's customer database.
F17	2026-04-19–2026-04-23	Parcel-delivery customers	A scraping narrative and a separate code example concern receiver and shipment fields. [S1]	The same affected system, authorisation failure, bulk extraction and acquisition date are not established.
F18	2026-06–2026-07	Diplomatic and cross-border documents	Repeated offers describe a diplomatic-mission archive in Türkiye and a separate foreign defence-related package. [S1]	Source, sensitivity and continuing access remain claims. Do not assign the separate package's contents to a Turkish organisation.
F19	2026-06-24	Payment terminals	A seller includes Türkiye in a multi-country remote-access offer for POS or cash-register systems. [S1]	No affected inventory or usable access is verified; no card-loss figure follows from the offer.
F20	2026-07–2026-08	Identity and telephone records	Posts advertise 145 million identity-and-telephone records. [S1]	Rows are not unique people. The relationship to the separate Case D collection is unverified.
F21	2026-07–2026-08	Hospital patients	Offers describe 20,000 patient records with clinical, appointment and payment-related fields. [S1]	Provenance and acquisition date are unverified; this is separate from the older workforce claim in Case A.
F22	2026-08-30	Non-profit services	A broker offers Exchange webmail access with claimed system privileges. [S1]	The advertised privilege and organisational characteristics are not verified and are not reproduced as identifiers.
F23	2026-09	Contact lists and identity documents	Offers market Turkish contact records and include Turkish passports in a multi-country archive. [S1]	Source, age, quantity, consent and shared origin remain unresolved.
F24	2026-08–2026-11	Betting-platform customers	Different offers describe customer datasets or multi-brand collections; one file is expressly labelled a repost. [S1]	A catalogue's brand count does not establish that every listed platform suffered a new incident.

Reference	Post dates	Role or topic	Proposition in the retained narrative	Evidence boundary
F25	2026-09-14	News-media records	A post claims a newspaper database dump obtained roughly a month earlier. [S1]	Volume, origin and access demonstration are absent from the narrative.
F26	2026-09-17	Personal-data platform	An author claims a platform exposing personal and psychometric information about Turkish citizens. [S1]	The narrative is incomplete. Meaning, source, consent and actual reach are unresolved.
F27	2026-10-09	Donors and retail customers	A post advertises 5,945 donor or customer entries with transaction-related fields. [S1]	Entries are not independently established unique people; source and acquisition date are unverified.
F28	2026-10-17	Mobility and service providers	An offer mixes customer, driver, workforce, vehicle and service-request tables across several years. [S1]	Table populations can overlap; they cannot be added into a unique-person total. B12 supplies the selected post evidence.
F29	2026-10-20	Vehicle records	An offer claims a vehicle-plate record collection. [S1]	Provenance, acquisition date and authenticity are unverified; sample plates and personal records are omitted.
F30	2026-11-02–2026-11-04	Public-facing applications	Access listings include Turkish-domain entries; one university entry is marked sold. [S1]	A seller's status label does not verify active access, a transaction or data loss.
F31	2026-11-05	Manufacturing remote access	A broker advertises VPN access to a manufacturing environment with high privileges. [S1]	Privileges, current validity and advertised business characteristics remain unverified; this is distinct from Case F.
F32	2026-11-14	Industrial manufacturing	An offer claims 690 GB and more than one million corporate-network files; another narrative offers an industrial database. [S1]	The offers are not linked. Sizes, file uniqueness, origin and current access remain unverified.
F33	2026-11-14	Web applications across sectors	A multi-site list alleges application flaws, administration access and possible server-side file execution. [S1]	No testing was performed to validate these targets; a list is not a verified vulnerability or incident inventory.

Reference	Post dates	Role or topic	Proposition in the retained narrative	Evidence boundary
F34	2026-11-16	Online community	A poster claims access to a local cyber-community website and references a video. [S1]	The narrative does not establish proof, loss scope or wider infrastructure impact.
F35	2026-11-19	Legal-services documents	A post alleges a legal-services document leak and claims bank-client relationships. [S1]	A claimed client relationship does not establish access to client-bank systems or authentic documents.
F36	2026-05-26	Veterinary records	A post offers records about veterinary professionals. [S1]	Volume, provenance, acquisition date and person scope require separate validation.
F37	2026-10-07	Communications-consent services	A post alleges data exposure associated with a consent-management system. [S1]	The platform association, population and active access remain unverified.
F38	2026-10-17	Financial-services archive	A financial or cryptocurrency-related archive offer mixes documents, database files and transaction records. [S1]	Files, identities and transactions are different units. No sum of unique customers or verified live access is supplied.
F39	2026-10-20	Telephone lookup compilation	A global lookup advertisement claims a large Türkiye-related subset. [S1]	Country-labelled rows do not establish unique people, a fresh source or a national-system intrusion.
F40	2026-01–2026-11	Bank, wallet and marketplace accounts	Repeated posts offer accounts for sale or rent, sometimes with identity, device or SIM material. [S1]	Repeated offers are not repeated intrusions. Consent, completed transfers and functional access are unverified.
F41	2026-03–2026-11	Restaurant customers	Several posts describe restaurant-customer or order datasets. [S1]	Source, local attribution and row-to-person meaning are unresolved in some narratives; no common event is assumed.
F42	2026-01–2026-11	Membership and administration records	Posts advertise political-membership and administrator records. [S1]	Names and loaded language are omitted. Source, authenticity and common dataset identity remain unverified.

Reference	Post dates	Role or topic	Proposition in the retained narrative	Evidence boundary
F43	2026-06–2026-07	Public-service email-related market	A repeated multi-country service advertisement claims local availability and email-related services. [S1]	No functioning official account, agency incident or state sponsorship is established; repetition is not independent evidence.
F44	2026-11-19	Traffic and betting records	A seller lists traffic-accident-report and betting datasets alongside account inventory. [S1]	The two dataset labels do not establish two incidents; provenance and possession are unverified.
F45	2026-01–2026-11	Impersonation tools	Advertisements offer banking, shopping and public-service-themed phishing or impersonation kits. [S1]	The legitimate brands are impersonated subjects; no intrusion into their infrastructure or common operator is established.
F46	2026-01-04–2026-01-19	Fixed-line customers	Reposted customer-data narratives combine an older acquisition story with a claim of renewed application access. [S1]	Conflicting population claims are unresolved. Repetition does not verify fresh access or a new customer population.
F47	2026-01-04	Defence supplier documents	A post claims possession of a large archive attributed to a defence supplier and describes employee email as its source. [S1]	Authenticity, acquisition date, employee-account access and continuing access remain unverified. Political messaging is not attributed to a state.
F48	2026-01–2026-03	Documents, communications and cash conversion	Separate advertisements seek company or residence documents and offer undocumented internet telephony or cryptocurrency-to-cash services. [S1]	Consent, provenance, functioning service and completed transactions are unverified. The advertisements are not linked to one operator.
F49	2026-01-21	Social-platform users	A post offers a Turkish user dataset and describes collection spanning 2022–2026. [S1]	Source, affected population, current access and the relationship to previously circulated archives remain unresolved.
F50	2026-01-22	Vehicle and insurance records	An offer claims 36,046 vehicle entries with insurance-related fields and says collection ended when the source became unavailable. [S1]	Entries are not unique owners. Origin, acquisition date, completeness and live interface access are unverified.

Reference	Post dates	Role or topic	Proposition in the retained narrative	Evidence boundary
F51	2026-01-31–2026-02-03	Subscription-payment abuse	Posts advertise regional subscription-payment methods using Turkish location and payment labels. [S1]	No valid card, completed charge, service entitlement or intrusion into the legitimate platform is verified.
F52	2026-04-13	Bank and company lookup tools	An advertisement claims automated bank-account and company-information lookup using a password or tax identifier. [S1]	The advertised functions, source and live account reach remain unverified. Demonstration fields are not evidence of bank-infrastructure access.
F53	2026-05-03	Address records	An offer claims 15,203,213 Turkish citizen-address records and describes acquisition days before posting. [S1]	Freshness, provenance, consent and unique-person meaning are unverified. The row claim is not a national victim count.
F54	2026-11-15	Forestry workforce records	A repost offers identity, telephone and competency fields associated with forestry workers and expressly labels the alleged leak 2021. [S1]	Publication in 2026 does not establish a new acquisition. Authenticity, population and consent remain unverified.
F55	2026-01-05–2026-01-07	Consumer impersonation and advance fees	An anecdote describes a courier-themed call. A separate lure demands registration or tax payments for an alleged prize. [S1]	Completed payment, genuine institutional involvement and common authorship remain unverified.
F56	2026-02-24	Alleged misuse of restricted records	A channel relays accusations of insiders disclosing restricted personal records. [S1]	The underlying investigation and original reporting were not independently established. The relay does not establish misconduct, a conviction or a new system intrusion.
F57	2026-02–2026-04	Document and payment-receipt editing	Mixed service catalogues advertise identity-document, licence, form, diploma and payment-receipt editing. [S1]	Functionality, authorisation and completed verification bypass are unverified. A claimed database insertion is not established access. No common operator is assumed.

Reference	Post dates	Role or topic	Proposition in the retained narrative	Evidence boundary
F58	2026-04-23	Telecommunications management	A channel claims control of a provider management system serving 5 divisions. [S1]	Claimed divisions are not separate companies or verified incidents. Access, control changes, operator identity and service effects remain unverified.
F59	2026-10-23	Remote process-control panels	A relay attributes an access claim covering 161 remote-control systems to an unnamed researcher. [S1]	Original proof, ownership, unique facilities, unauthorised changes and physical outcomes are unverified. No link to Case H is established.

About this report

Odin by Brandefense prepared this country report for security leadership, operations, infrastructure, identity, fraud, privacy and supplier-risk teams. It combines own retained evidence with source-checked context. It does not disclose victim indicators, personal rows, access routes or internal research mechanics.

The package is prepared for the series' separate editorial and publication workflow. Selected-portfolio limits and incomplete earlier-source coverage remain visible. The English master governs the interpretation of its translated edition.

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