BRANDEFENSE COUNTRY REPORT · AZERBAIJAN 2026

Brandefense Azerbaijan Cyber Threat Landscape Report 2026

Exposure, underground markets and hacktivist pressure on a strategic energy and transit state

Odin by Brandefense
Research window: 1 January-18 November 2026
Version 1.2 · Public Research Edition · TLP:CLEAR · First published 19 November 2026

80 of 250
organisations had a credential listed for sale on the day of the check

6,172-6,901
cleaned posts remain from 49,097 tagged posts

>100 vs 1,825
state domains targeted (official) vs sites the attacker claimed offline

5 of 22
card-issuing banks with a current credential listing, the first item to triage

CONTENTS

Contents

01	Executive summary	04
	Report map	08
02	Azerbaijan's digital and geopolitical context	09
03	National exposure: 250 leading organisations	13
04	What we see on the dark web	21
05	Targeting examples by sector	37
06	Hacktivism and DDoS	44
07	Threat actors	53
08	The fraud economy	68
09	Banking and finance deep dive	73
10	Regulatory and national response	76
11	Outlook	80
12	Action plan	83
A	Appendix A. Method	90
B	Appendix B. Evidence register	94
C	Appendix C. Sources	96
D	Appendix D. Glossary	100
	About this report	102

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

About this edition

Prepared by Odin by Brandefense from Brandefense Blackhole, Ransompedia and Atlas data. Analysis and first drafts by AI agents (Anthropic Claude); findings reviewed by Brandefense analysts before release. Method summary in Appendix A.

CHAPTER 01

Executive summary

01

THIS CHAPTER ANSWERS

What happened in 2026, what matters most for Azerbaijani organisations, and what should leaders decide first?

4

decisions for leaders, each tied to evidence in the chapters

Four decisions for leaders 06

The year in numbers 07

CHAPTER 01

Executive summary

IN SHORT

For the 250 leading Azerbaijani organisations we assessed, the main measured exposure is identity, not ransomware: infected-device and credential associations, and credentials listed for sale. The most visible incident was an officially reported DDoS attack on state domains that a group described in press reporting as pro-Iranian claimed. The most consequential documented intrusion was state-linked espionage against energy. Act in this order: confirm you receive your credential listings and validate each one; re-test internet-facing mail and edge servers; then pre-agree DDoS statements and harden account recovery.

This report combines three of Brandefense's own data sources with verified public reporting. **Brandefense Blackhole** supplied 49,097 posts tagged as concerning Azerbaijan and a further 36,495 distinct posts found by Azerbaijani keywords and organisation names. It also supplied infected-device and credential records for 250 selected organisations, and card material that appeared in clear text in posts. **Ransompedia** supplied ransomware leak-site listings for Azerbaijan and three regional comparators. **Atlas** exposure ratings were computed for the 250 organisations. These are separate populations and are never added together.

1. Ransomware is close to absent from the evidence; identity exposure is not. Ransompedia holds one accepted Azerbaijani listing in its entire history (2025) and none dated 1 January-18 November 2026. Georgia has five, Armenia two and Kazakhstan none in the same 2026 window.

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

By contrast, 190 of the 250 organisations we assessed have infected devices associated with their domains (38,554 in total), and 222 have historical credential records (168,031 records). These counts are all records held on 19 November 2026, whatever their capture date: they are cumulative, not 2026-only. They can involve staff, students or customers. These are association counts: whether any login or session is still usable, and who it belongs to, requires validation. [S1][S3][S6]

2. 80 of 250 organisations had a credential listed for sale when checked. Each listed credential was linked to the organisation's domain and offered on credential markets that Brandefense monitors. The national Atlas headline for the 250 organisations is 48 out of 100 (§3.2). A listing tells a defender to look for an active account; it does not say how many accounts or whose. [S4]

3. A hacktivist-claimed DDoS hit state domains; authorities reported disruption at several agencies. On 13 October 313 Team (self-styled Islamic Cyber Resistance in Iraq), a group described in press reporting as pro-Iranian, claimed a DDoS campaign against Azerbaijani government infrastructure. It cited what it described as a ban on the hijab in schools and universities. It claimed 47 IP ranges, more than 2.5 Tbps and 1,825 government websites offline. The State Service for Special Communication and Information Security reported a cyberattack by a foreign hacker group on more than 100 state domains from about 22:00 that evening. It said several agencies' online resources were disrupted and that measures were taken to limit the impact.

On 16 October the National Cybersecurity Agency described DDoS attacks on 13-15 October against government, media, diplomatic-mission and other resources. It said a commercial DDoS service sold on Telegram was used and noted that 313 Team had claimed responsibility. The actor's traffic and outage figures remain unverified claims. [S2][S10][S11][S23]

4. The most consequential documented intrusion was espionage, not crime. Bitdefender attributes, with moderate-to-high confidence, a three-wave intrusion into an Azerbaijani oil and gas company to the China-linked FamousSparrow group. It ran from late December 2025 to late February 2026. The attackers entered through a vulnerable (ProxyNotShell-exploitable) Microsoft Exchange server and returned through it after remediation attempts. An Azerbaijani parliamentary official attributed a February 2025 attack on media outlets to APT29, a group the official described as Russian-linked. Neither appeared in the 2026 leak-site and forum data we searched; the evidence for both came from vendor research and an official statement. [S12][S13]

5. Four notable Azerbaijan-specific offers advertised population datasets. They are an 817,241-row student file (January), a "1 million" citizen file (August), a "state register of individuals" of 4.58 million rows for 2,000 USD (August) and a claim against a state service platform (October). None is independently verified, and some government-themed threads recirculate 2013-era material. Each still matters for fraud and impersonation because identity data does not expire the way passwords do. In November a breach-forum seller also offered 800,000 passenger records attributed to an Azerbaijani transport company; neither the company nor the authorities had confirmed it by our cut-off (Case F in Chapter 4). [S1][S31]

Four decisions for leaders

1. **Treat current credential listings as an incident trigger, not a statistic.** Route every current market listing tied to your domains to the identity team and record a disposition within 5 working days. Escalate to incident response if an active account without multi-factor authentication (MFA) is found. 80 of 250 organisations had one when we checked (§3.4). To act on it, arrange monitoring of credential listings and infected devices for your domains from day 1, through an internal team or a provider (§12.1).
2. **Patch and isolate internet-facing mail and edge servers as an espionage control.** The FamousSparrow case entered through ProxyNotShell (CVE-2022-41040 and CVE-2022-41082), Exchange flaws disclosed in 2022, and re-entered after remediation. Treat "still exploitable after remediation" as the test, including where a mitigation rule replaced the patch (§7.2).
3. **Prepare for hacktivist claims that outrun the facts.** Agree in advance who confirms service status publicly during a hacktivist campaign, and pre-arrange upstream mitigation for citizen-facing portals. 313 Team published its claims hours before the first official statement we found.
4. **Join identity, fraud and security operations around citizen data.** Population datasets do not reveal a breached system, but they power impersonation, SIM-swap and account-recovery fraud. Test recovery and payment-change processes with synthetic cases.

The year in numbers

0

Ransompedia accepted ransomware listings for Azerbaijan dated 1 Jan-18 Nov 2026 (1 all-time)

WHAT IT IS NOT

Not proof that no Azerbaijani organisation was extorted; unlisted and unpublished cases are invisible

49,097

Blackhole posts tagged as concerning Azerbaijan, 1 Jan-18 Nov 2026

WHAT IT IS NOT

Not a count of attacks; 69% fall in February-March and are dominated by one bulk-advertising bot family

6,172-6,901

posts left after removing bot templates, spam and news mirrors from the tagged set

WHAT IT IS NOT

Not unique incidents; in an informal one-reviewer check of 30 cleaned posts, 18 of 30 were crime posts genuinely concerning Azerbaijan (not a corpus-wide rate)

>100 / 1,825

state domains targeted on 13-14 October (official statement) / websites the attacker claimed to have taken offline

WHAT IT IS NOT

Different measures; neither independently verified, and not a ratio

250

leading public and private organisations assessed with Atlas methodology

WHAT IT IS NOT

Not a random sample; not a national prevalence estimate

38,554

infected devices associated with those 250 domains (2,764 classified as employee devices); cumulative, all records held on 19 Nov 2026

WHAT IT IS NOT

Not 2026-only, not unique people, not verified current infections; devices are not deduplicated across organisations

168,031

historical credential records for the same domains (breach databases, stealer logs, combolists); cumulative, regardless of capture date

WHAT IT IS NOT

Not 2026-only; not unique accounts or active passwords

80 of 250

organisations with a credential listed for sale at the time of the check

WHAT IT IS NOT

Not a count of accounts or of confirmed breaches

657

distinct Azerbaijan-associated payment cards seen in clear text in collected dark-web posts (529 attributed to a named Azerbaijani bank, 128 labelled only as Azerbaijani)

WHAT IT IS NOT

Not a fraud-loss figure; narrow scope (§8.2)

66%

of the 250 organisations enforcing DMARC (164)

WHAT IT IS NOT

Not a measure of phishing success or delivery security

Report map

Twelve chapters, five reader paths. Start with the row that matches your role; each chapter opens with the question it answers, and chapters 2-12 close with three takeaways.

Board and executives	What happened, how exposed are we, and what should we decide?	01 03 12
CISO and security leads	Which exposures are ours, which actors matter, and which controls come first?	03 06 07 09 10 12
SOC and threat intelligence	What did the actors post, how are they connected, and which techniques did espionage use?	04 06 07 08 12 A B
Fraud and customer protection	How are Azerbaijani identities, accounts and cards traded, and where do banks see it?	04 05 08 09
Communications and legal	How do we speak about unverified claims, and what does the new law require?	06 10 12

01 Executive summary
What happened in 2026 and what leaders should decide first

02 Context
Why Azerbaijan attracts espionage, hacktivism and fraud at once

03 National exposure
How 250 leading organisations score with the Atlas method

04 Dark web
What criminals post about Azerbaijan once spam is removed

05 Sectors
Which sectors are named and what response each needs

06 Hacktivism
What was claimed, what was confirmed, how to prepare

07 Threat actors
Who the actors are, how they connect, what reporting says

08 Fraud economy
How identities and accounts are turned into money

09 Banking
Where banks' visible exposure sits

10 Regulation
What changed and what is due by 1 July 2027

11 Outlook
What to plan for and what would change the plan

12 Action plan
Who does what in 90 days

CHAPTER 02

Azerbaijan's digital and geopolitical context

02

THIS CHAPTER ANSWERS

Why does Azerbaijan attract espionage, hacktivism and fraud at the same time, and which features of the country shape the evidence in the rest of this report?

91%

internet penetration, with 12.4 million cellular connections

2.1 A connected, mobile-first population 10

2.2 Energy, transit and the espionage interest 10

2.3 Politically framed hacktivist claims 10

2.4 Centralised digital government 11

2.5 A changing national cyber authority 11

CHAPTER 02

Azerbaijan's digital and geopolitical context

IN SHORT

Three features shape Azerbaijan's threat picture: an energy and transit role that attracts state espionage; politically framed hacktivist claims, some of uncertain origin; and a highly digitised, centralised public-service model that concentrates citizen data. Plan for all three at once: patch edge systems, prepare DDoS statements and protect identity data.

2.1 A connected, mobile-first population

Azerbaijan had about 10.5 million inhabitants and 9.51 million internet users in October 2026, a penetration of 90.8%. It had 12.4 million cellular connections (118% of the population) and 8.44 million social-media user identities [S14]. Telegram is the dominant channel in the criminal data we hold for Azerbaijan, and Russian is its dominant language (Chapter 4). That combination matters. Most Azerbaijan-relevant underground trading happens in Russian-language Telegram communities that also serve Russia, Ukraine, Kazakhstan and Uzbekistan. Azerbaijan often appears as one country among many on a seller's price list, not as a target of choice.

2.2 Energy, transit and the espionage interest

Azerbaijan is an oil and gas exporter, a supplier to Europe through the Southern Gas Corridor and a link in east-west transit routes across the Caspian. Bitdefender noted that the South Caucasus had not previously been linked to the FamousSparrow activity cluster in public reporting; its case rests on one victim [S12]. For state-linked collectors, Azerbaijani energy companies hold commercially and politically valuable information about supply, pricing and partners. That interest is independent of criminal market activity and requires different evidence: incident telemetry and vendor research, not forum posts.

2.3 Politically framed hacktivist claims

In 2026, actors invoking regional and international political issues claimed cyber activity against Azerbaijani targets. In our 2026 data we observed:

- a group described in press reporting as **pro-Iranian** (313 Team) claiming attacks on government websites, citing what it described as a ban on the hijab in schools and universities;
- **pro-Palestinian** framing (Python Squad) justifying claims against two transport companies and an entertainment company by reference to Azerbaijan's relations with Israel;
- a **self-styled Armenian-nationalist** channel ("Armenian code") claiming attacks on Azerbaijani companies, universities, insurers, logistics firms and an industrial control system;

- a **pro-India**-framed channel ("F ~ INTELLIGENCE") claiming DDoS against a state portal, a bank site and a state security body's site in March-April under the tag #opazarbeijaan, citing what it called Azerbaijan's support for Pakistan;
- Russian-language channels commenting on Azerbaijan-Russia relations, which make up a large share of keyword hits but are not crime.

An Azerbaijani official attributed the February 2025 attack on Azerbaijani media to APT29 at a parliamentary hearing in May 2025, describing it as a Russian-linked group. The official also linked the timing to the closure of the Russian House in Baku [S13]. We report that as an official attribution, not an independently confirmed one.

2.4 Centralised digital government

Azerbaijan runs national e-government, e-ID, e-visa and one-stop public-service platforms. Centralised platforms also concentrate high-value identity data and create single points that attract both data-theft claims and DDoS. Among 2026 underground offers we observed claims naming state service platforms, a state security body and a "state register of individuals" (Chapters 4-5). None is verified, but the targeting pattern follows the architecture.

2.5 A changing national cyber authority

On 2 June 2026, a presidential decree established the **National Cybersecurity Agency** as a public legal entity [S15]. The decree creates it as the legal successor to the Electronic Security Service, which was subordinate to the Ministry of Digital Development and Transport [S22]. The ministry announced it in the same terms [S16]. Separately, the State Service for Special Communication and Information Security remains the voice on attacks against state infrastructure, as its October statement shows [S10]. Chapter 10 sets out what changed for organisations.

Official figures show continuing pressure on state systems. The State Service for Special Communication and Information Security counted 274 cyberattack indicators against state agencies in January-March 2026 [S35] and 518 in January-July 2026 [S36], compared with 573 in January-July 2025 [S54]. That is a 10% lower same-period count, though these figures measure detected indicators on state systems rather than national attack incidence.

On 19 November a deputy minister of digital development reported more than 134,000 botnet infections detected, over 2,000 sites with malicious content and more than 300 defacement and DDoS cases in 2026 [S37]. The same statement reported detailed investigations into the activity of 10 APT groups [S37][S56]. In June the same official reported 160,000 botnet infections prevented in six months [S50]. The two botnet figures use different wording and should not be compared as a trend.

KEY TAKEAWAYS

01

Energy and transit make Azerbaijan an espionage target independent of criminal markets.

02

Hacktivist claims in 2026 cited religious, regional and foreign-policy themes, from several directions at once.

03

Most 2026 data claims against state bodies name bodies that hold citizen data, including central state service platforms.

CHAPTER 03

National exposure: 250 leading organisations

03

THIS CHAPTER ANSWERS

How exposed are the country's 250 leading public and private organisations when they are assessed with Brandefense Atlas, and which signals should defenders act on first?

80 of 250

organisations had a credential listed for sale on the day of the check

3.1 Universe card 14
3.2 Exposure signals by sector 15
3.3 Devices and credentials 17
3.4 Current credential listings 18
3.5 Lookalike domains, exposed documents and mentions 19
3.6 Email and web hygiene 19
3.7 Two homepages serving gambling spam 20

CHAPTER 03

National exposure: 250 leading organisations

IN SHORT

We assessed 250 leading Azerbaijani organisations using Brandefense Atlas exposure ratings. Three in four have infected devices associated with their domains, nine in ten have historical credential records, and almost one in three had a credential listed for sale when we checked. Email and web hygiene is uneven: two thirds enforce DMARC, but we observed DNSSEC delegation (DS) records for only 12 of 250 domains. Triage current listings first, then employee devices.

3.1 Universe card

Item	Definition
Population	250 organisations: 68 government bodies, 35 banking and finance, 26 retail and holding groups, 23 universities, 18 energy and utilities, 16 media and entertainment, 14 telecom, 14 manufacturing and industry, 11 hospitality and tourism, 10 transport, 8 insurance, 7 healthcare. 136 state-owned, 103 private, 11 foreign or joint
Selection	Purposive: state bodies and national portals, licensed banks and payment infrastructure, state-owned enterprises, market leaders. Selected for size or systemic role, not ranked by revenue; no published Azerbaijani top-250 ranking was used
Unit	One primary domain per organisation. All 250 resolve in DNS (19 November 2026). For the 155 domains that answered our request, the homepage title matched the organisation. The 95 that did not answer our web checks (mostly government sites) were provisionally assigned by the domain name matching the organisation's official name or acronym; their ownership is not independently confirmed. 13 candidates were dropped because the domain belonged to another party
Measurements	Infected devices and employee devices, breach-database, stealer-log and combolist records, dark-web chat and forum mentions, lookalike domains, exposed documents and current credential-market listings, using the same data Atlas uses; plus public DNS, TLS and HTTP header checks
Date	Counts read 19 November 2026. Device, credential and listing counts are all records held on that date, regardless of capture date (cumulative, not 2026-only). Mention counts cover 19 November 2025-18 November 2026; lookalike counts cover the last 30 days

Item	Definition
Not deduplicated	Across sources, across organisations or across people. One person can appear in several sources; one device can hold logins for several organisations
Not representative	Results describe this list. They are not national prevalence rates

3.2 Exposure signals by sector

Atlas rates each organisation from 0 (no risk observed) to 100. This report publishes only the national headline for the 250 organisations: 48 out of 100. By sector, it shows how many organisations carry each signal.

How to read Atlas ratings.

Term	Meaning
Rating	0 (no risk observed) to 100 per organisation; a higher value means more exposure
National headline	One Atlas figure for all 250 organisations: 48 out of 100
Current listing	A credential tied to the domain on sale at the time of the check; validate the account first

Credentials and infected devices are common in every sector; current listings vary by sector

Share of organisations in each sector with the signal. Current credential listings are shown in coral.

	Infected devices	Employee devices	Credential records	Current listing	Listing history	Lookalikes (30 days)	Exposed documents
Insurance (8)	88%	62%	75%	75%	62%	50%	0%
Retail and holdings (26)	73%	50%	92%	54%	50%	65%	12%
Media and entertainment (16)	81%	50%	100%	50%	50%	62%	12%
Telecom (14)	79%	64%	86%	50%	43%	79%	29%
Banking and finance (35)	89%	77%	97%	31%	26%	86%	17%
Education (23)	96%	96%	96%	30%	26%	91%	22%
Transport and logistics (10)	100%	90%	100%	30%	30%	50%	10%
Energy and utilities (18)	61%	50%	89%	28%	17%	61%	11%
Government (68)	72%	54%	85%	25%	25%	88%	16%
Hospitality and tourism (11)	36%	27%	64%	9%	9%	64%	9%
Manufacturing and industry (14)	64%	50%	79%	7%	7%	50%	21%
Healthcare (7)	57%	57%	86%	0%	0%	71%	14%

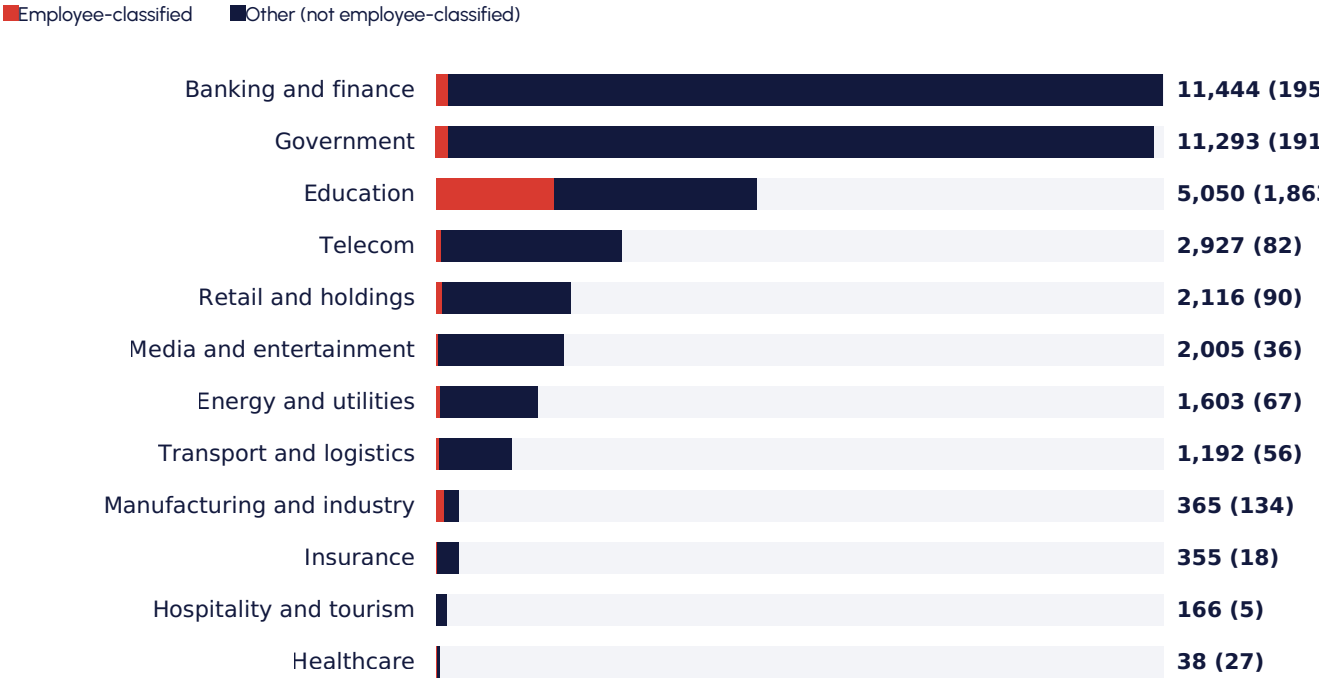
Source: Brandefense Atlas ratings and Blackhole associations for 250 organisations, read 19 November 2026 [S3][S4]. Records are cumulative, not 2026-only.

Sector	Orgs	Orgs with a current credential listing
Insurance	8	6
Retail and holdings	26	14
Media and entertainment	16	8
Telecom	14	7
Banking and finance	35	11
Education	23	7
Transport and logistics	10	3
Energy and utilities	18	5
Government	68	17
Hospitality and tourism	11	1
Manufacturing and industry	14	1
Healthcare	7	0
All 250	**250**	**80**

Reading the table. Infected-device and credential associations appear in every sector (§3.3). Current listings vary more: on the day of the check, 6 of 8 insurers had one and none of the 7 healthcare organisations did. Treat a sector's listing count as a triage queue for identity teams, not as a measure of its security.

3.3 Devices and credentials

Banking and government carry the most infected-device associations, almost all outside the employee classification



Source: Brandefense Atlas ratings and Blackhole associations for 250 organisations, read 19 November 2026 [S3][S4]. Records are cumulative, not 2026-only.

Sector	Orgs with infected devices	Devices (employee)	Credential records	Share held by two largest orgs
Banking and finance	31 of 35	11,444 (195)	15,739	32%
Government	49 of 68	11,293 (191)	8,772	22%
Education	22 of 23	5,050 (1,863)	81,719	48%
Telecom	11 of 14	2,927 (82)	19,310	55%
Retail and holdings	19 of 26	2,116 (90)	9,229	71%
Media and entertainment	13 of 16	2,005 (36)	2,742	35%
Energy and utilities	11 of 18	1,603 (67)	7,940	60%
Transport and logistics	10 of 10	1,192 (56)	2,976	71%
Manufacturing and industry	9 of 14	365 (134)	16,978	93%
Insurance	7 of 8	355 (18)	1,385	67%

Sector	Orgs with infected devices	Devices (employee)	Credential records	Share held by two largest orgs
Hospitality and tourism	4 of 11	166 (5)	349	69%
Healthcare	4 of 7	38 (27)	892	77%
All	**190 of 250**	**38,554 (2,764)**	**168,031**	**23%**

Credential records split into 37,737 breach-database records, 52,041 stealer-log lines and 78,253 combolist entries. The infected devices hold 1.75 million captured credentials in total, for all services, not only the organisation's own.

What this means.

- **Banking and government carry the device load, mostly outside the employee classification.** 11,249 of 11,444 bank-associated devices are not employee-classified in this dataset. Their stealer logs include a login to the bank's site, so they are most plausibly customers' own computers, though ownership is not established. These associations are a fraud and account-hijacking signal and do not by themselves establish an intrusion into the bank. The 195 employee-classified devices are the intrusion-relevant subset; both groups require validation.
- **Universities hold the employee-device problem.** Education has 1,863 employee-classified devices, two thirds of the national total in our list, and the largest credential count. University staff and students share domains, so "employee" here may include students; the risk is credential reuse into research, finance and government systems that the same people access.
- **Concentration varies.** In manufacturing, two organisations hold 93% of credential records; in government the two largest hold 22%. A sector total is therefore a poor guide to a typical organisation.
- **The median organisation is modest.** The median organisation has 11 infected devices and 117 credential records. The heaviest single organisations carry thousands of devices or tens of thousands of credential records.

3.4 Current credential listings

80 of 250 organisations had at least one credential tied to their domain listed on a monitored credential market at the time of the check. Of those 80, 72 also have a listing history, and no organisation has a history without a current listing.

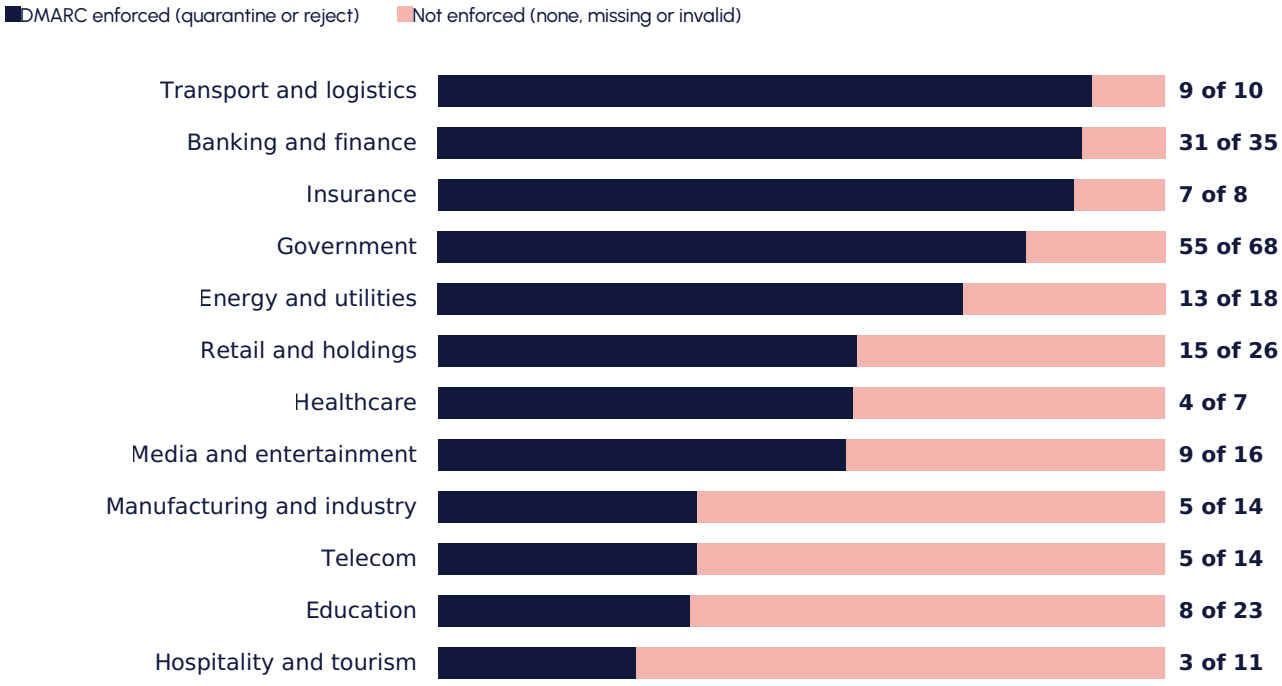
For a defender, a current listing is the most direct market signal that a login tied to the domain is on offer. Whether that login still works is exactly what validation must establish. It should be read precisely. The listing does not say how many accounts, whose accounts, or whether the account is active, protected by multi-factor authentication, or already reset. The decision it supports is "validate the account now", not "declare a breach".

3.5 Lookalike domains, exposed documents and mentions

- **Lookalikes:** 188 organisations had at least one newly observed lookalike domain in the last 30 days. For the 156 organisations with a distinctive brand root, counts are usable for triage. For the other 94 the Atlas lookalike signal could not be assessed reliably (Appendix A.4). Lookalikes are candidates, not confirmed phishing sites.
- **Exposed documents:** 39 organisations have at least one exposed document that references their domain (102 in total).
- **Mentions:** 77 organisations were mentioned in dark-chat sources in the last 365 days and 18 in dark-web (onion) sources. News sites dominate the largest counts because Telegram news channels link to them; one news site alone has 95,811 dark-chat mentions. Mention counts measure visibility, not hostility.

3.6 Email and web hygiene

Banking and government mostly enforce DMARC; universities, hospitality and manufacturing mostly do not



Source: Brandefense public DNS, TLS and homepage checks of 250 domains, 19 November 2026 [S5].

Results from our public DNS, TLS and homepage checks [S5]:

Control	Result (of 250 unless stated)	Reading
DMARC reject	92	Spoofed mail from the domain should be refused

Control	Result (of 250 unless stated)	Reading
DMARC quarantine	72	Spoofed mail should go to spam
DMARC p=none, missing or invalid	86 (33 none, 51 missing, 2 invalid)	No enforcement; spoofing the domain is easier
SPF ending -all / ~all / ?all / redirect / none	131 / 58 / 1 / 43 / 17	17 domains publish no SPF policy; 43 delegate to another domain's policy by redirect
DKIM record found	169	Not finding a record is not proof of no DKIM
DS record observed (DNSSEC delegation)	12	No DS record observed for 238 domains; a DS record alone does not prove a valid chain of trust
TLS certificate invalid	13 of 202 checked	Expired, mismatched or untrusted certificates
HSTS on homepage	64 of 155 reachable	Many sites do not force HTTPS for returning visitors
Mail provider	63 Microsoft 365, 11 Google, 15 no MX	The rest run their own or regional mail

Web checks were unavailable for 95 sites, mostly government sites. Their DNS checks are complete.

Banking leads, hospitality and manufacturing lag. 31 of 35 banking and payment organisations enforce DMARC, as do 55 of 68 government bodies. Universities (8 of 23), hospitality (3 of 11) and manufacturing (5 of 14) enforce least. On the passive hygiene index (Appendix A.5; 0–100, higher is weaker), tourism (58) and manufacturing (56) have the weakest index values and transport (25) and banking (32) the strongest.

3.7 Two homepages serving gambling spam

The primary domains of two industrial organisations on our list serve online-gambling spam on their homepage. That is consistent with either unauthorised changes to a content-management system or a lapsed domain registration taken over by a spam operator. Both are fixable and both damage trust in the organisation's name; we include them because they are the kind of exposure an external scan finds immediately and an internal programme can miss. Both owners should check content-management integrity and domain-registration status.

KEY TAKEAWAYS

01

Infected-device and credential associations are widespread in the list; they call for validation, not alarm.

02

80 of 250 organisations had a credential listed for sale when checked; each listing is the first item to triage.

03

One in three domains does not enforce DMARC and only 12 of 250 publish DNSSEC delegation.

CHAPTER 04

What we see on the dark web

04

THIS CHAPTER ANSWERS

What do criminals actually post about Azerbaijan once bot spam is removed, and which offers matter to defenders?

6,172-6,901

cleaned posts remain from 49,097 tagged posts

4.1 Universe card 22
4.2 Platforms, languages and volume 23
4.3 Crime families after cleaning 25
4.4 Four notable offers advertise Azerbaijani population data 26
4.5 Government-themed offers and recirculated material 28
4.6 Case studies 31
4.7 What the forums add 36

CHAPTER 04

What we see on the dark web

IN SHORT

Most Azerbaijan-tagged underground traffic is bulk advertising in Russian-language Telegram chats. After cleaning, a few thousand posts remain, and the Azerbaijan-specific ones are dominated by bank-account trading, payment cards, citizen data and identity documents. Forums play a small role; leak sites play almost none. Read cleaned counts only, and triage each claim by provenance before comment.

4.1 Universe card

Item	Definition
Source	Brandefense Blackhole: Telegram channels and groups, a set of cybercrime forums, paste sites and Discord, collected continuously
Country definition	A country tag ("this post is about, targets or mentions Azerbaijan"), cross-checked with keyword sets in four languages
Window	Post time 1 January–18 November 2026 (November partial). Collection time is never used
Tagged set	49,097 posts counted; 49,096 distinct
Keyword sets	Country and city terms in four languages plus major organisation names; counts are near-complete, and a lower bound from July (§4.2)
Combined corpus	85,591 distinct posts, of which 84,361 carry the tag or an Azerbaijani term
Cleaning	Spam, very short posts, stress-test logs, repeated template posts and news mirrors removed (Appendix A.2)
Not established	That a tagged post targets Azerbaijan, that a claim is true, or that two posts concern the same file

4.2 Platforms, languages and volume

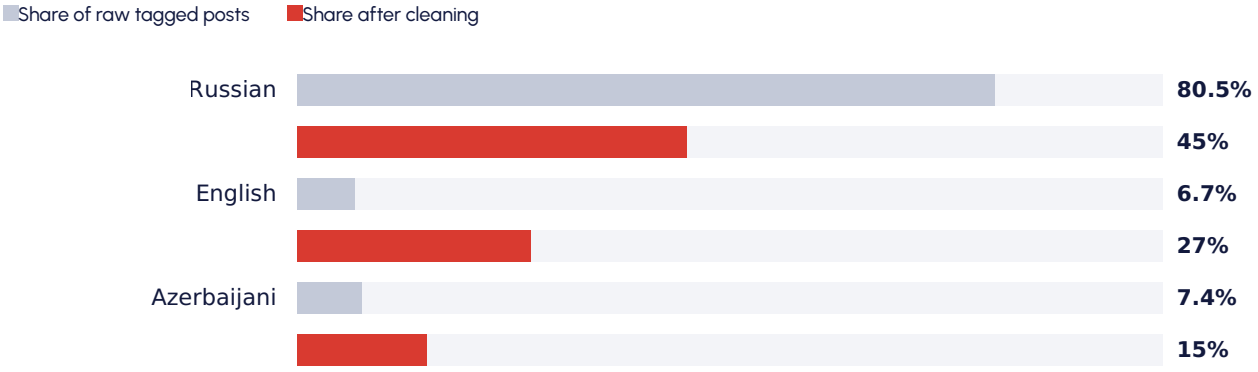
Two months of bot templates inflate the raw count; cleaned volume stays between 336 and 1,380 posts in every complete month



Source: Brandefense Blackhole, posts tagged Azerbaijan, post dates 1 January–18 November 2026, November partial [S1]. Cleaned counts are an upper bound.

Measure	Value
Telegram share of tagged posts	99.86% (49,026)
Forum posts	60 (plus 144 forum posts matching "Azerbaijan")
Paste, Discord, onion sites	6, 5, 0
Russian / Azerbaijani / English / Turkish	80.5% / 7.4% / 6.7% / 3.7% of raw posts
After cleaning: Russian / English / Azerbaijani	45% / 27% / 15%
Raw posts per month	19,598 in February and 14,392 in March; 747–3,154 in other months

Russian dominates the raw tag; among crime-relevant posts, English and Azerbaijani carry more weight



Telegram carries 99.86% of tagged posts. Source: Brandefense Blackhole, posts tagged Azerbaijan, post dates 1 January–18 November 2026, November partial [S1]. Cleaned counts are an upper bound.

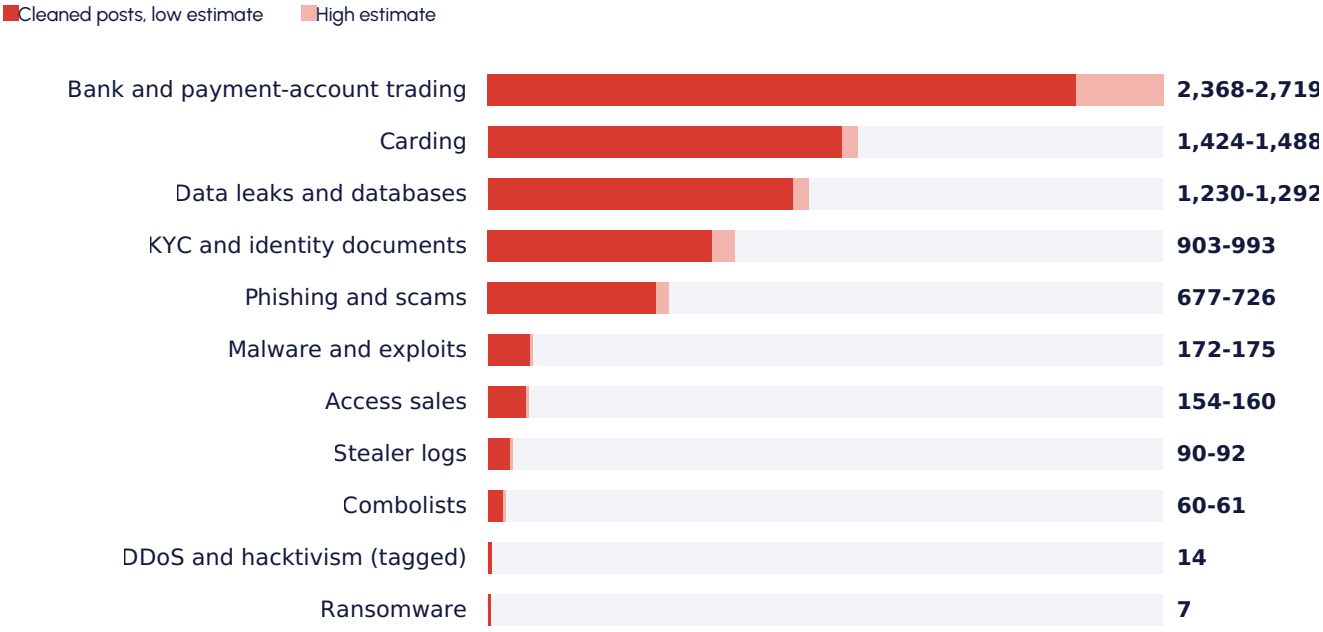
The February–March spike is not an attack wave. 69% of the year's tagged posts fall in two months and are dominated by one family of bot templates. These are multi-country price lists for "personal bank-account access" posted to hundreds of Russian-language chats. Georgia and Armenia show the same spike. After template removal, volume is 336–1,380 cleaned posts in each complete month (January–October); the partial November window holds 218–224.

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

Collection appears lower from July onwards. Türkiye's tagged volume, which has no comparable bot spike, falls from 528,914 in May to 107,910 in July. From July every compared country is below its January–May average. We do not read declines from July as threat trends.

4.3 Crime families after cleaning

Bank-account trading leads the cleaned corpus; cards, data leaks and identity services follow



Source: Brandefense Blackhole, posts tagged Azerbaijan, post dates 1 January-18 November 2026, November partial [S1]. Cleaned counts are an upper bound.

Family	Cleaned posts (low-high)	What it contains
Bank and payment-account trading	2,368-2,719	Offers to buy, rent or sell bank and wallet accounts, often with Azerbaijan as one entry on a multi-country list
Carding	1,424-1,488	Card-checker outputs, card-shop updates, buyers seeking Azerbaijani cards
Data leaks and databases	1,230-1,292	Citizen, student and customer databases; call-centre lead lists; lookup bots
KYC (know-your-customer) and identity documents	903-993	Verification services, document templates, SIM registration
Phishing and scams	677-726	Scam pages, SMS confirmation services, "traffic" for scams
Malware and exploits	172-175	Tool sales and exploit discussion, mostly global
Access sales	154-160	Remote access, panels, "hacked accounts/systems Azerbaijan" requests
Stealer logs	90-92	Log sales and buyers

Family	Cleaned posts (low-high)	What it contains
Combolists	60-61	Country-labelled credential lists
DDoS and hacktivism (tagged)	14	Small within the tag; see Chapter 6 for keyword-based collection

Families overlap and must not be added. In an informal one-reviewer spot check of 30 cleaned posts, 18 of 30 were crime posts that genuinely concern Azerbaijan; the other 12 were multi-country lists, cargo chats and banking questions. That small sample is not a corpus-wide estimate, so treat cleaned counts as an upper bound.

Prices quoted. In cleaned posts, the median quoted price was 2,500 USD for access offers (few values, wide spread) and 65 USD for KYC and document services. Bank-account offers had a median of 60 USD and carding posts 15 USD per card (Chapter 8). These are asking prices, not completed sales.

4.4 Four notable offers advertise Azerbaijani population data

Four offers stand out because they claim large Azerbaijani population datasets. None was independently verified, and we did not obtain any file.

Date	Claimed dataset	Claimed fields	Claimed volume	Venue	Post
28-30 Jan	Student records	Name, surname, birth date, address	817,241 rows (30 Jan offer); similar titles without a count on another forum, 28-30 Jan	Two leak forums, one via a leak-monitoring bot	B01
9 Aug	Citizen records	ID, name, birth year, city, phone	"1 million"	Turkish-language Telegram channel, sale via Signal	B02
15 Aug	"State register of individuals"	Name, address, birth year	4,584,191 rows, 2,000 USD	Lead-trading Telegram channel	B03
29 Oct	"All citizen info" attributed to a breach of a state service platform	"Full PII"	Not stated	Telegram; a separate poster invoking the brand used in the January offer	B04

What this tells defenders. A large population file does not reveal which system it came from. The advertised field sets differ. The student file lists name, surname, birth date and address, and the "1 million" file lists ID, name, birth year, city and phone. The "state register" lists name, address and birth year; the state-platform claim lists no fields. Any of them could derive from older sources, aggregation or a new breach; the posts do not settle it.

What they do establish is a market in Azerbaijani identity data that fraud operations can use for impersonation, account recovery and social-engineering scripts. Organisations that verify customers by name, birth date or year, address or phone should assume those fields are not secret.

The four posts as they appeared, redacted:

Evidence card B01 — 30 Jan 2026

xploitleaks | Leak forum | Forum | English

ORIGINAL

Azerbaijan Student Data
DATABASE SIZE --> 817241 Row
DATABASE CONTENT --> Name, Surname, Birth Date, Address
Sample [image link removed]
FOR CONTACT --> [contact removed]

Held
The offer, fields and row count; three earlier relays of similarly titled listings by another persona (28-30 Jan).

Not established
File identity across venues, origin, age, any sale.

Evidence card B02 — 9 Aug 2026

X Ticaret | Telegram channel | Telegram | Turkish

ORIGINAL

AZERBAYCAN DATASI
1 Milyon Azerbaycan Datası
ID, Adı Soyadı, Doğum Yılı, Şehir ve Telefon bilgileri
Signal Kanalında [link removed]

TRANSLATION

AZERBAIJAN DATA
1 million Azerbaijan records
ID, name and surname, year of birth, city and phone details
On the Signal channel [link removed]

Held
The offer and the claimed fields.

Not established
Volume, origin, authenticity.

Evidence card B03 — 15 Aug 2026

Lead-trading poster | Lead-trading Telegram channel | Telegram | English, apparently machine-translated from Russian

ORIGINAL

Database name: State Register of Individuals of the Republic of Azerbaijan [...]
Year (period) of data: Current cross-section (2026).
fio (text) [...]
address (text) - The official address of registration / permanent residence.
birth_ear (text) - The exact year of the citizen's birth.
Number of records: 4,584,191 rows (unique individuals).
Price: 2000$

Note. The field name "fio" is the Russian abbreviation for full name; the poster's English renders it as "full photos", a sign of machine translation.

Held
Offer, claimed fields (full name, registered address, birth year), count and price.

Not established
Any link to a state register; recency.

Evidence card B04 — 29 Oct 2026

Poster invoking xploitleaks | Telegram group | Telegram | English

ORIGINAL

[state service platform] breached by Xploitleaks
-All citizen info of Azerbaijan
-Full PII
Dm for price

Held
The claim and the brand association.

Not established
Any intrusion at the platform; that the January seller made this post.

Smaller identity and customer-data offers. Beyond the four population-scale offers, the blind audit (Appendix A.8) found narrower offers that point the same way. None was verified, and we obtained no file.

Date	Observed offer	Our reading
9 Jan (re-posted Sep, Nov)	400,000 "casino player" leads from 2024, with a sample, for 350 USD on a breach forum	Marketing-lead data; if genuine, could support gambling and loan-fraud targeting
18 Jan; resale 11 Feb	A ZIP of 468 Azerbaijani ID-card images on a Telegram fraud channel, later offered on a forum; "1,000+ more" promised in March	If genuine, document images could support KYC fraud (§8.3)
Jan-Apr	Lookup results and "query panel" offers returning ID-card series, personal code, address and workplace	The data source behind the lookups is unknown
14 Feb	Records of grade 5-9 pupils attributed to an education provider	Children's data; unverified
21 Feb	1,465,516 Azerbaijani email "leads", with a sample, on a breach forum	If genuine, could serve as a phishing distribution list; origin unknown
24 Jul	5,000 Azerbaijani passport records "current as of 12 May 2026" on a Turkish-language channel	Unverified; if genuine, passport data could support travel and KYC fraud

4.5 Government-themed offers and recirculated material

Date	Observed offer	Our reading	Post
19 Feb	A small set of "cloud" credential lines for a state service platform, relayed by a leak-monitor bot from a forum's automated uploader	Consistent with stealer-log lines from users' own devices (an inference; origin not established); no evidence of a portal breach	B05
6 Mar	Re-post of a 2013-era ministry leak title on a Turkish-language forum, with a dead link (B06); separate 2013-era re-posts on the same forum named a state security body and a 458,000-record health SQL file (no card shown)	Reposts claiming 2013-era material; do not report as a 2026 breach	B06
21 Mar	A forum reply asking for a re-upload of a 1.4 GB ministry leak (summarised in B06; reply not shown as a separate card)	Same theme; demand for old material	None

Date	Observed offer	Our reading	Post
18 Jul	A database said to come from a state security body offered for sale ("only two buyers"), relayed by a hacktivist-branded channel	Unverified; no sample assessed; the body named makes the claim likely to attract attention	B07
Undated (reported 2026)	A vendor blog reports that a government case-management system was offered for sale [S32]	Single public source; not observed in our data; no seller, price or sample published	None
18 Oct	A 400 GB "Azerbaijan DB" torrent dump advertised on a breach forum, with no description of its contents	Unverified; no source system named; no sample assessed	B22
17 Nov	The xploitleaks brand writes that it buys "active sessions" from Azerbaijani government entities, with escrow	Demand for access, not evidence of a breach	B21

What this tells defenders. Government-themed claims cluster around bodies that hold citizen data or carry symbolic value. One row is a repost that itself dates the material to 2013, and another is a request to re-upload old material. The state-platform credential case is most consistent with user-side malware. The state-security, case-management and 400 GB claims are unverified, and the case-management item rests on a single vendor report that our data does not corroborate.

The request for active government sessions is a demand signal: someone is seeking to buy access, which makes session and token monitoring on government systems more urgent. A government response team should be able to separate these quickly: provenance, age and sample comparison first, public comment second.

Evidence card B05 — 19 Feb 2026

X FORUMS (bot) | Leak-monitor bot relaying a forum uploader | Telegram | English

ORIGINAL

"Source": "[forum removed]",
"Content": "[state service platform domain] auth [file label removed] By X FORUMS",
"Type": "Data leak"

Held
A relayed title for a small credential file referencing a state service platform login page.

Not established
Any portal breach; the lines are consistent with stealer logs from users' devices.

Evidence card B07 — 18 Jul 2026

0cx00iq (relayed) | Hacktivist-branded channel relaying a breach forum | Telegram | English

ORIGINAL

Azerbaijan [state security body] database
Now for sale
If you are not serious, do not try to contact.
Offer your price and we will negotiate for your price
The data may only be sold to two people!
[handle removed]

Note. The poster named a state security body by its acronym.

Held
The sale claim and the venue.

Not established
Any sample, content or origin.

Evidence card B06 — 6 Mar 2026

arcturus (quoted) | Turkish-language forum | Forum | Turkish

ORIGINAL

AZERBAYCAN [bakanlık] LEAK 2013
arcturus Nickli Üyeden Alıntı
İNDİR [link removed]
Link çalışmıyor

TRANSLATION

AZERBAIJAN [ministry] LEAK 2013
Quoted from the member named arcturus
DOWNLOAD [link removed]
The link is not working

Held
A re-posted title the poster dates to 2013, a dead link, and a later request for a re-upload of a "1.4 GB" leak (21 Mar).

Not established
Any 2026 incident.

Evidence card B21 — 17 Nov 2026

xploitleaks | Breach forum | Forum | English

ORIGINAL

I buy Azerbaijani active sessions from gov entities. PM me if you have poc and ready to trade with escrow!
Thread: Buying AZERBAIJAN - I buy databases and active sessions

Held
A request to buy active sessions in government entities, with escrow.

Not established
That any session was sold or any system accessed.

Evidence card B22 — 18 Oct 2026

iq313 | Breach forum | Forum | English

ORIGINAL

400GB TORENT OTHER TYPE DUMP
Thread: DATABASE - AZERBAIJAN DB
[link removed]

Held
A thread titled "Database Azerbaijan DB" advertising a 400 GB torrent.

Not established
Contents, source system, age or any sample.

4.6 Case studies

Each case follows the same structure: claim, chronology, what we can establish, alternatives, limits and a proportionate response.

CASE A

A

Similar student-data listings appear across venues

Evidence card B01 | 30 Jan 2026 | Leak forum | Education

Claim unverified

CLAIM	A seller brand offers "Azerbaijan Student Data", 817,241 rows with name, surname, birth date and address, pointing buyers to its Telegram shop.
CHRONOLOGY	A leak-monitoring bot relayed listings titled "Azerbaijan student database" and "Azerbaijan citizen data" from one leak forum on 28, 29 and 30 January, posted by a persona we record as menpolisem. On 30 January the seller brand xploitleaks posted the 817,241-row offer on a second forum.
WHAT WE CAN ESTABLISH	That matching-themed listings appeared on two venues within three days, under two different names. The posts do not establish that the files are identical, that either poster obtained the data first, or that any sale took place.
ALTERNATIVES	One seller using two names; one reseller copying another's listing; two unrelated datasets with similar titles.
LIMITS	No sample was assessed. Age is unknown.

RESPONSE	Education authorities and universities should check whether the claimed fields match any internal export and review recent bulk-export logs. Regardless of origin, apply the identity-verification advice in §4.4.

Bottom line

Treat name, birth date and address as public for verification; check exports before anyone speaks of a breach.

CASE B

B ■ A separate poster invokes the same brand for a government claim

Claim unverified

Evidence card B04 | 29 Oct 2026 | Telegram group | Government

CLAIM	On 29 October a Telegram poster wrote that a state service platform had been "breached by xploitleaks", offering "all citizen info" for a price on request.
WHAT WE CAN ESTABLISH	That a Telegram poster attributed a much larger government claim to the brand that advertised student data in January. This does not establish that the January seller made the October claim; brand reuse supports at most a persona association, not a common operator or a real breach.
ALTERNATIVES	Promotional exaggeration; relabelled older data; a genuine incident.
RESPONSE	For the platform operator, an inexpensive first step is to compare any sample with known export schemas and with the January student file. For banks and telecoms, the claim is a reason to rehearse customer-impersonation scenarios, not to reset credentials.

Bottom line

A brand name is not proof of a breach: compare any sample with known schemas before comment.

CASE C

C ■ A "state register" priced like a lead list

Claim unverified

Evidence card B03 | 15 Aug 2026 | Lead-trading Telegram channel | Government, banking, telecom

CLAIM	A lead-trading channel advertised a "State Register of Individuals of the Republic of Azerbaijan, current cross-section 2026" with 4,584,191 rows of name, address and birth year for 2,000 USD.
WHAT WE CAN ESTABLISH	The offer, the fields, the price and the venue. The venue mainly trades marketing and call-centre leads.

READING	One possibility is an aggregated or older dataset rebranded as a national register; price and venue do not establish the file's origin, and a fresh exfiltration cannot be excluded. Its fields overlap with, but are not identical to, those of the student file (Case A).
RESPONSE	As for Case A. Call-centre fraud against bank and telecom customers is the most plausible use.

Bottom line

Price and venue point to call-centre use; the file's origin is unknown.

D

CASE D

An infostealer demand signal

Evidence card B08 | 4 Aug 2026 | Russian-language drop-services chat | All sectors

Demand observed (one post)

CLAIM	On 4 August a buyer in a Russian-language "drop" services chat posted: "BUYING INFOSTEALER BOTNETS FOR AZERBAIJAN AND CAUCASUS REGION".
WHAT WE CAN ESTABLISH	Demand for infected-device access with Azerbaijani targeting, expressed in a venue that also trades bank accounts.
WHY IT MATTERS	The post shows buyer demand for Azerbaijan-related infostealer access, the same class of exposure measured across the 250 organisations in Chapter 3. Infostealer logs are the raw material for both account hijacking and corporate intrusion.
RESPONSE	Treat employee-device associations as the priority subset of the 38,554 devices; validate active sessions and tokens, not just passwords.

Bottom line

The post shows demand for Azerbaijan-related infostealer access; after current listings, validate employee devices and their sessions before the wider device set.

CASE E

E A gambling-related site in an automated dump bot

Evidence card B09 | 20 Oct 2026 | Automated dump bot | Gambling-related site

Bot announcement only

CLAIM	On 20 October a "dump" bot reported 130 lines extracted from the domain of a gambling-related site.
WHAT WE CAN ESTABLISH	That the bot announced it. Automated dump bots often run SQL-injection tooling against public sites and publish small extracts to advertise paid services.
RESPONSE	For any organisation named by such a bot, the first step is a web-application log review for injection attempts on the announced date, not a breach announcement.

Bottom line

Review web logs for the announced date; a bot post is not a breach notice.

Evidence card B08 — 4 Aug 2026

Anonymous buyer | Russian-language drop-services chat | Telegram | English

ORIGINAL

BUYING INFOSTEALER BOTNETS FOR AZERBAIJAN AND CAUCASUS REGION!!!

Held
Demand for infected-device access with regional targeting.

Not established
Whether a sale took place.

Evidence card B09 — 20 Oct 2026

Dump bot | Automated dump bot | Telegram | English

ORIGINAL

Dump completed
Target: [gambling-related site domain]
Lines: 130
Time: 10.03s
For Private Data and access : [handle removed]

Held
The bot's announcement.

Not established
What the lines contain.

CASE F

F Passenger data attributed to an Azerbaijani transport company offered for sale

Evidence card B20 | 11 Nov 2026 | Breach forum | Transport

Claim unverified

CLAIM	On 11 November a seller on a breach forum offered "800K Passengers' Data" and information on 10,000 passengers with upcoming trips, attributed to an Azerbaijani transport company, for 2,000 USD with samples.

WHAT WE CAN ESTABLISH	The offer, the claimed fields (names, document and contact details, customer account data, and trip and route details), the price and the advertised samples. A public monitoring account reportedly flagged it the same day as alleged [S31]. Neither the company nor the authorities had confirmed a breach by our cut-off, and we did not obtain the samples. Our exposure data for the transport sector (Chapter 3) is a separate signal; it neither confirms nor rules out this sale.
ALTERNATIVES	Recycled or aggregated older data; data taken from a third-party booking, travel-agency or partner system rather than the company; a genuine compromise of a reservation system.
RESPONSE	If the offered data is genuine, expect phishing and passenger impersonation that quote real bookings, because upcoming-trip data would make them credible. Monitor customer accounts for hijacking, and review partner, agency and booking-system access and API credentials. Prepare a customer notice in case a sample is verified.

Bottom line

If genuine, upcoming-trip data would make booking-themed phishing credible: watch customer accounts and partner systems while the claim is checked.

Evidence card B20 — 11 Nov 2026

databreach000 | Breach forum | Forum | English

ORIGINAL

SELLING [Azerbaijani transport company] Database [domain removed] Passengers' upcoming [trip] [...]
800K Passengers' Data + 10K Passengers upcoming [trip] information [...]
Each data block contains: 1. Passengers: firstName, lastName, type, gender [...]; document details [...]; email; phone details [...]; [...] 2. Tickets [...] 3. Routes [...]
Samples: [sample links removed]
Price : 2,000 $
Contact TG : [contact removed]

Note. The thread title names the company and its domain; both are redacted here.

Held
The offer, the claimed fields, the price and advertised samples; a public monitor reportedly flagged it as alleged.

Not established
Any sample, the source system, or a breach of the company's own systems.

4.7 What the forums add

Forums contributed only 60 tagged posts in the year, but they carry the most specific claims (Case A and the re-posts of government-themed material). Most forum hits are global phone-number and crypto-lead lists naming Azerbaijan among 100 or more countries. Forum buyers also posted requests. In August a forum user offered "a high price" for a ready-made "lookup" solution covering Azerbaijan and other former Soviet states. In March a forum user living in Azerbaijan asked others for Azerbaijani data shared in the past. Demand for Azerbaijani lookup and identity data is itself a finding.

KEY TAKEAWAYS

01

Raw volume is dominated by bot templates; read only cleaned counts, and treat them as an upper bound.

02

Four population-data offers matter for fraud whatever their origin (§4.4).

03

Government-themed claims mix 2013-era reposts, user-side stealer lines and unverified sales; triage provenance before comment.

CHAPTER 05

Targeting examples by sector

05

THIS CHAPTER ANSWERS

Which Azerbaijani sectors are named in criminal and political posts, and what kind of response does each one need?

9

sectors with observed activity, from government to retail

CHAPTER 05

Targeting examples by sector

IN SHORT

The posts below show how criminal and political actors talk about Azerbaijani organisations. Most are offers of access, accounts or data with Azerbaijan as one market among several; a minority name a specific organisation. Post examples are claims; rows also cite separately attributed official reports (§8.5). Verify each claim with the named operator before escalating, and start with the sector's First response.

Victims are described by role under the policy in Appendix A.9. Examples are drawn from the cleaned corpus and the keyword sets; official reports are marked with §8.5. The final row combines examples from the retail and holdings and the media and entertainment sectors in §3.1.

Government

DDoS claim | data claim | stealer lines | PII exposure | phishing | supply-chain warning

EXAMPLE OF OBSERVED ACTIVITY (ANONYMISED)

313 Team target lists naming national portals and ministries (Oct); claims against a state security body (Jul) and a state service platform (Oct); #opazarbeijaan DDoS claims (Mar-Apr); a buyer seeking government sessions (Nov); a vendor-reported sale of a government case-management system; state-platform credential lines (Feb); e-visa applicant lists from a visa agent (Apr-Aug); mass phishing of state mailboxes (Government CERT, Apr; §8.5); official warning on supply-chain attacks via trusted contractors (Jun; [S57])

WHAT IT MEANS

Availability and citizen-data integrity are the two exposures, and staff mailboxes and contractor links are entry routes; the e-visa lists are a process risk in third-party agents, not a portal breach

FIRST RESPONSE

Pre-agree status statements; monitor sessions, tokens and contractor access on government systems

Banking

Carding | cash-out | credential | account trading | phishing | business-account intrusion

EXAMPLE OF OBSERVED ACTIVITY (ANONYMISED)

Card-checker outputs printing, in clear text, cards from 17 Azerbaijani issuers; "I will dump Georgian/ Azerbaijani POS terminals" (Jun); cash-out offers listing Azerbaijan at a 30% cut (Aug); a combolist line containing a bank employee's mailbox (Oct); Russian-language chats on opening accounts at an Azerbaijani bank remotely; police-reported loan-page phishing and business-account intrusion (Feb-Aug; §8.5)

WHAT IT MEANS

Posts are dominated by fraud tooling; the intrusion-relevant exposure is in the device data (167 employee-classified devices at issuers, Chapter 9) plus one employee mailbox in a combolist

FIRST RESPONSE

Triage current listings, then employee devices; alert on BIN checker declines

Energy and industry

APT intrusion | DDoS claim | OT claim

EXAMPLE OF OBSERVED ACTIVITY (ANONYMISED)

Espionage intrusion into an oil and gas company (vendor research, Dec 2025-Feb 2026); a mining company and a defence-sector company on an "Armenian code" DDoS list (Apr); water-reservoir and water-supply control claims (Feb) and a heating-control claim (Mar) in Baku

WHAT IT MEANS

The material risk is espionage via edge servers; DDoS and OT (operational technology) claims need verification before escalation

FIRST RESPONSE

Re-test Exchange and edge servers; verify OT claims with the operator

Telecom

SIM fraud services | lead data | DDoS testing

EXAMPLE OF OBSERVED ACTIVITY (ANONYMISED)

SIM registration, "number rental" and SMS-reception services listing Azerbaijani numbers; phone-number lead lists naming Azerbaijan; stresser-bot test logs against hosting ranges (Mar)

WHAT IT MEANS

SIM-swap and number-rental services connect directly to bank account-recovery fraud

FIRST RESPONSE

Tighten SIM-swap and number-port checks

Transport

Data sale claim | DDoS claims

EXAMPLE OF OBSERVED ACTIVITY (ANONYMISED)

Passenger data attributed to an Azerbaijani transport company offered for sale (Nov, unverified; Case F); Armenian code DDoS claims against a transport operator, an airport site and a port (Feb); Python Squad claims against two transport companies (Mar), with availability-check links; DDoS claims against an airport site (DieNet relay, Mar; Armenian code, Apr), three logistics firms and a transport company (Armenian code, Apr)

WHAT IT MEANS

Passenger and booking data is the material exposure; public-facing booking systems are the likely DDoS target

FIRST RESPONSE

Watch customer accounts and partner systems; review partner and booking-system credentials

Education

Data claims | credential exposure

EXAMPLE OF OBSERVED ACTIVITY (ANONYMISED)

817,241-row student database offer (Jan); Armenian code DDoS claims against several universities (Feb); "sensitive files of an Azerbaijani institute" leaked by a forum persona (Feb); highest employee-device count of any sector (Chapter 3)

WHAT IT MEANS

Universities are a credential reservoir for people who also work in government and industry

FIRST RESPONSE

Enforce MFA and reset staff passwords found in stealer logs

Healthcare

Recirculated data

EXAMPLE OF OBSERVED ACTIVITY (ANONYMISED)

2013-era "458K health data" SQL re-posted (Mar)

WHAT IT MEANS

Old data, but health identifiers do not expire

FIRST RESPONSE

Compare the 2013 schema with current systems before any notice

Insurance

Data sale claim | DDoS claim

EXAMPLE OF OBSERVED ACTIVITY (ANONYMISED)

A Telegram seller advertising a "final database" it says leaked from an insurer in 2025 (Mar); whether it relates to the 2025 extortion listing is unknown; Armenian code DDoS list against three insurers (Mar)

WHAT IT MEANS

If the offer is genuine, leaked insurance, medical and vehicle records keep circulating; plan for long-tail fraud

FIRST RESPONSE

Add fraud checks on policy and claims changes

Retail, media and entertainment examples

DDoS | defacement

EXAMPLE OF OBSERVED ACTIVITY (ANONYMISED)

DieNet DDoS claims against a news site, a payment-terminal provider and a travel company (Mar); 22 .az sites reported defaced in a day in a relayed notice attributed to the National Cybersecurity Agency (Sep); an entertainment company claimed by Python Squad (Mar)

WHAT IT MEANS

Low-cost attacks on smaller web estates; reputational more than operational

FIRST RESPONSE

Patch the CMS and monitor for defacement

Reading across sectors. Organisation-specific claims fall into two groups. Politically motivated actors name symbolic targets (state portals, transport, defence and mining companies) and claim disruption. Financially motivated actors rarely name an organisation; they name Azerbaijan as a market for accounts, cards, SIMs and data. The second group is less visible and may create cumulative fraud risk; this report does not measure harm.

Contractor and supplier access to state systems. In June an official of the State Service for Special Communication and Information Security warned that attackers also reach state information systems through the networks of trusted contractors and service providers [S57]. State bodies and critical operators should inventory contractor accounts and network connections, restrict them to required systems and monitor third-party sessions alongside staff accounts.

KEY TAKEAWAYS

01

Political actors name symbolic targets and claim disruption; criminal sellers name Azerbaijan as a market.

02

For banks and telecoms, fraud tooling dominates the posts; intrusion-relevant exposure sits in employee-device data (Chapter 9).

03

Energy faces espionage through edge systems; DDoS and OT claims there need verification first.

CHAPTER 06

Hacktivism and DDoS

06

THIS CHAPTER ANSWERS

Who claimed attacks on Azerbaijan in 2026, what did the authorities confirm, and how should an organisation prepare for the next claim?

>100 vs 1,825

state domains targeted (official) vs sites the attacker claimed offline

6.1 Timeline 45

6.2 The 313 Team campaign: claim against measurement 46

6.3 Other claims in their own words 49

6.4 Lessons for defenders 51

CHAPTER 06

Hacktivism and DDoS

IN SHORT

Hacktivist claims against Azerbaijan in 2026 came from four directions: pro-Iranian, pro-Palestinian, self-styled Armenian-nationalist and, in March-April, a channel with pro-India framing; mostly DDoS and defacement. The most prominent was 313 Team's claimed campaign of 13-16 October, which coincided with an officially reported cyberattack on more than 100 state domains. Pre-agree who confirms service status, and contract upstream mitigation before the next claim.

6.1 Timeline

2 Feb 2026	**Armenian code** Claims tampering with a Baku water-reservoir control panel (2 Feb) and a water-supply SCADA system (5 Feb); unverified
10 Feb 2026	**Armenian code** DDoS claims against a transport operator, an airport site and a port
15 Feb 2026	**Seniman1337** Defacement of one .az site (defacement-feed relay)
18 Feb 2026	**Armenian code** DDoS claims against a state portal, a leasing firm and an investment firm
19 Feb 2026	**Armenian code** DDoS list against several universities
5 Mar 2026	**Armenian code** Claims a Baku heating-control system forced into failure
7 Mar 2026	**DieNet** Relayed claims of DDoS on a news site, a payment-terminal provider, a travel company and an airport site, with probe results
9 Mar 2026	**Armenian code** DDoS list against three insurers
17 Mar 2026	**Python Squad / Team Python** Two transport companies and an entertainment company claimed with check links
29 Mar 2026	**F ~ INTELLIGENCE** #opazarbeijaan DDoS claims from 29 Mar to 5 Apr: a capital-markets firm, a state portal, a bank investment site and a state security body's site
2 Apr 2026	**Armenian code** DDoS list against three logistics firms and a transport company

8 Apr 2026	**Armenian code** DDoS claims against an airport site, a hotel-booking service and a state agency's site
21 Apr 2026	**Armenian code** DDoS list: a mining company, a holding group, a travel agency and a defence-sector company
30 Apr 2026	**Armenian code** DDoS claims against three commercial banks (30 Apr–1 May) and a statement against Azerbaijan's economy and banks
25 Sep 2026	**Local security channel** Relays an agency monitoring notice: 22 .az websites defaced in one day, 19 on one hosting network, linked to the persona Xscyth3
13 Oct 2026	**313 Team** Announces action, citing what it called a hijab ban in schools; claims 47 IP ranges, >2.5 Tbps, 1,825 sites offline
14 Oct 2026	**State Service for Special Communication and Information Security** More than 100 state domains targeted from about 22:00 on 13 Oct; measures taken to limit impact
14 Oct 2026	**313 Team** Extends by 24 hours; 54 IP ranges, ">1,800 sites"
16 Oct 2026	**313 Team** Further 48-hour extension ("four consecutive days")
16 Oct 2026	**National Cybersecurity Agency** DDoS on 13–15 Oct against government, media and diplomatic-mission resources; commercial service Litterbox (Catbox) identified

Dark markers are actor posts, outlined markers are relays by third parties, coral markers are official statements. Dates are post dates in UTC; Baku time is UTC+4, so a post late on 13 October UTC falls on 14 October in Baku. Times and full wording are in the evidence cards and §6.2.

6.2 The 313 Team campaign: claim against measurement

Claim. The group announced at 21:41 Baku time on 13 October that it would "completely destroy" Azerbaijan's government digital infrastructure. It cited what it described as a ban on the hijab in schools and universities, and the size of the Shia community. Azernews noted that the claim of a general ban had not been substantiated [S49]. Within three hours it claimed 47 IP ranges attacked at more than 2.5 Tbps and 1,825 government websites offline, and published availability-check links for national portals and ministries. It extended the campaign twice. OC Media described the group as pro-Iranian and believed to operate from Iraq [S20].

Evidence card B10 — 13 Oct 2026

313 Team | Actor channel | Telegram

Arabic, with the group's own English

ORIGINAL

لقد تلقينا شكاوى عديدة ضد حكومة جمهورية أذربيجان بشأن حظر ارتداء الطالبات للحجاب في المدارس والجامعات. [...] فإننا سنتخذ إجراءً حازماً ضد الدولة: إذ سنقوم بتدمير بنيتها التحتية الرقمية الحكومية بالكامل.

TRANSLATION

We have received numerous complaints against the government of the Republic of Azerbaijan regarding the ban on female students wearing the hijab in schools and universities. [...] we will take firm action against the state: we will completely destroy its government digital infrastructure.

Held
The announcement and its stated motive (17:41 UTC, 21:41 Baku time).

Not established
Any capability; this post is intent only.

Evidence card B11 — 13 Oct 2026

313 Team | Actor channel | Telegram

Arabic, with the group's own English

ORIGINAL

نفذت المقاومة الاسلامية السيبرانية في العراق - فريق 313 هجوم سيبراني ضخم ومتطور استهدف خلاله 47 نطاق ip اساسي تابع للبنية التحتية الالكترونية الحكومية لجمهورية اذربيجان بلغت شده الهجوم اكثر من 2.5 تيرابايت بالثانية [...]

TRANSLATION

[...] targeting 47 key IP ranges belonging to the Republic of Azerbaijan's government digital infrastructure. With an intensity exceeding 2.5 terabits per second [...] This attack is 100% powered by [second DDoS-for-hire service] & Litterbox [links removed]

Held
The claimed scale and the two services the group credits.

Not established
Traffic volume and outage count; compare the official statements in §6.2.

Official account. The State Service for Special Communication and Information Security said that malicious activity against more than 100 government domains began at about 22:00 on 13 October and disrupted the online resources of several agencies. It said technical measures were taken to limit the impact. It described the attacker as a foreign hacker group and did not name a country [S10][S11]. Local media initially named several ministries and a state agency as affected; the official statement did not confirm a list. A theory linking the attack to Türkiye circulated on social media; JAMnews found no evidence establishing it [S17].

What we can establish. The timing of the claim and the official start time match within minutes. The official statement counts domains targeted (more than 100) and reports disruption to several agencies; the actor counts websites it says were offline (1,825). These are different measures, and neither was independently verified, so we do not compute a ratio. No data theft was claimed or reported in the sources reviewed for this campaign.

Point	313 Team's claim	Official account	Press reporting
Start	Announcement at 21:41 Baku time on 13 Oct; attack claim at 00:25 on 14 Oct	Activity from about 22:00 on 13 Oct [S10]	Same timing reported [S20]
Scope	47, then 54 government IP ranges	More than 100 state domains [S10]	Authorities' figure repeated [S20]

Point	313 Team's claim	Official account	Press reporting
Effect	1,825, then ">1,800" sites offline; "complete paralysis"	Disruption to several agencies; measures taken to limit the impact [S10]	Several ministry sites unreachable when reporters checked [S20]
Volume	More than 2.5 Tbps	Not stated	Not measured
Tooling	Credits Litterbox and a second DDoS-for-hire service	Commercial service Litterbox (Catbox), sold on Telegram [S23]	Not stated
Duration	24 h, then +24 h and +48 h (four days)	Attacks on 13-15 Oct [S23]	Not stated
Attribution	Own claim	"Foreign hacker group"; the agency notes the group's claim [S10][S23]	Pro-Iranian, believed to operate from Iraq [S20]; no evidence for a Türkiye theory [S17]

Later official account. On 16 October the National Cybersecurity Agency said DDoS attacks were carried out on 13-15 October against the information resources of government bodies, media organisations, Azerbaijan's diplomatic missions abroad and other organisations. The agency identified a commercial DDoS service called Litterbox (also known as Catbox), offered through Telegram and paid in cryptocurrency, as the service used.

It said the service can generate traffic over GRE, ICMP, UDP and TCP and route it through bots in selected countries; it did not specify which capabilities were used in these attacks. The agency noted that the hacktivist group 313 Team had taken responsibility; it gave no traffic volumes or outage counts [S23]. Litterbox is one of the two services 313 Team itself credited.

What it means. A DDoS campaign against state and other resources took place, and the authorities said they acted to limit its impact. The method and the commercial tooling are officially described; 313 Team's responsibility is stated as the group's own claim, and its traffic and outage figures remain unverified.

The group's claims were published hours before the first official statement we found. The episode shows that rented DDoS capacity, sold on Telegram for cryptocurrency, was used against state resources; the operator behind the attacks remains officially unresolved beyond the group's own claim. Five days earlier the national cybersecurity body had warned about attacks exploiting outdated database software and default credentials [S17]. JAMnews used the former name, Electronic Security Service; the National Cybersecurity Agency had succeeded it in June (§2.5). No link to the October attack was reported.

Evidence card B17 14 Oct 2026

313 Team | Actor channel | Telegram | Arabic, with the group's own English

ORIGINAL

[...] قررت المقاومة الاسلامية السيبرانية في العراق - فريق 313 تمديد الهجوم السيبراني لمدة 24 ساعة إضافية. وقد قمنا بتكثيف العملية عبر استهداف 7 عناوين IP رئيسية جديدة [...] ليصل بذلك إجمالي نطاقات عناوين IP المستهدفة إلى 54 نطاقاً.

TRANSLATION

[...] the Islamic Cyber Resistance in Iraq - 313 Team has decided to extend the cyberattack by an additional 24 hours. We have intensified the operation by targeting 7 new key IP addresses [...] bringing the total of targeted IP ranges to 54.

Held
The extension claim (21:17 UTC).

Not established
The claimed "more than 1,800" sites offline.

6.3 Other claims in their own words

The other 2026 claimants posted far less, and none of their claims was confirmed by an operator or an authority. Their profiles, with what public reporting says about each, are in §7.3.

Evidence card B12 — 17 Mar 2026

Python Squad | Actor channel | Telegram | Azerbaijani, with the group's own English

ORIGINAL

Python Squad olaraq, [əyləncə şirkəti]-ın rəqəmsal infrastrukturuna qarşı hədəflənmiş kiber əməliyyat həyata keçirmiş və nəticəsində onun rəqəmsal infrastrukturunda tam dayanma yaranmışdır. [...] Bu haker əməliyyatlarının səbəbi kimi Azərbaycan hakimiyyətinin İsrailə hərtərəfli yardımları [...]

TRANSLATION

Python Squad has carried out a targeted cyber operation against [entertainment company], resulting in a total shutdown of its digital infrastructure. [...] The reason for these hacking operations is the Azerbaijani authorities' comprehensive support for Israel [...]

Held
The claim, its motive and an availability-check link [removed].

Not established
Duration and real effect; an availability-check link can at most record a momentary probe result.

Evidence card B15 — 17 Mar 2026

Team Python | Actor channel | Telegram | English and Azerbaijani, as posted

ORIGINAL

We, Team Python, take responsibility for the attack on [transport company] due to their support for Israel.
Biz, Python Komandası, İsrailə verdiyi dəstəyə görə [nəqliyyat şirkəti]-nə edilən hücumun məsuliyyətini öz üzərimizə götürürük.

Held
The claim, posted in the same minute as the other transport-company and entertainment-company claims (B12).

Not established
Any outage beyond the group's own check link.

Evidence card B14 — 7 Mar 2026

DieNet (relayed) | Relay channel of an automated tracking bot | Telegram | English

ORIGINAL

DieNet network is currently targeting [news site] and it may be down for you at the moment
Check-Host
[3 probe nodes]: Connection timed out
This is an automated message from [bot removed],
Real-time DieNet attacks tracking

Held
A relayed claim with a probe result for one moment in time; three similar relays the same evening, one naming an airport site.

Not established
Sustained outage; which service carried the traffic.

Evidence card B16 — 21 Apr 2026

Armenian code | Actor channel | Telegram | English, as posted

ORIGINAL

[...] we strike at the economies of those who encroach on sacred things. Azerbaijan suffers from our cyberattacks on their industry, tourism, and other strategic sectors.
[mining company] [check link removed]
[holding group] [check link removed]
[travel agency] [check link removed]
[defence-sector company] [check link removed]

Held
The target list and four availability-check links.

Not established
Effect on any target.

A fourth direction appeared in March and April. A Telegram channel calling itself "F ~ INTELLIGENCE" posted availability-check links for a capital-markets firm, a state portal, a bank investment site and a state security body's site under the tag #opazarbeijaan. It framed the campaign as retaliation for Azerbaijan's support for Pakistan. We found no public reporting that corroborates these claims or identifies the operators; we record them as claims.

Evidence card B23 5 Apr 2026

F ~ INTELLIGENCE | Actor channel | Telegram | English, as posted

ORIGINAL

[state security body, in leetspeak].
w3bsite: [state site address]
St4tus: D0wn, n0t R3sponding.
L0cked Sinc3: F3w H0urs.
Durati0n: [...]
R3ason: Supp0rting [Pakistan, insulting term].
St4tus Ch3ck: [check link removed]
J0ining L1nk: [link removed]

Note. Leetspeak as posted.

Held
The claim, the stated motive and an availability-check link.

Not established
Any outage beyond a momentary probe; the operators' identity.

Not counted as hacktivism: the 15 November link redirects. The presidential press service said the President's social-media accounts were under cyberattack on 15 November. Links in old posts redirected to third-party videos for several hours. The press service did not state a method or actor [S34]. The same day, old short links on many prominent accounts worldwide redirected in the same way. Bitly said an issue had let malicious actors reuse some old, inactive links [S34]. No official source had linked the two by our cut-off. We do not count the episode as hacktivism because no source we found named an actor. The defensive lesson is to review and replace old short links on official accounts.

6.4 Lessons for defenders

1. **Pre-agree the public line.** A hacktivist's numbers and an authority's numbers rarely measure the same thing. Decide in advance who confirms status, within what time and through which channel.
2. **Protect portals at the upstream.** Volumetric attacks at the claimed scale are absorbed upstream or not at all. Contract mitigation for citizen-facing portals before an event.
3. **Watch the issues actors cite.** In 2026, claimants cited a school dress-code issue, Azerbaijan's foreign relations and regional disputes in their announcements (§6.2–6.3). Treat new references of this kind in actor channels as a planning signal for DDoS readiness.
4. **Do not over-read OT claims.** Verify with the operator and physical readings before escalation; treat a public claim as reconnaissance of interest.

KEY TAKEAWAYS

01

The October campaign was real by the authorities' account; the attacker's numbers were not confirmed.

02

A commercial DDoS service sold on Telegram was officially identified in the October attacks, and NETSCOUT assessed in 2025 that DieNet likely used rented infrastructure; upstream mitigation is the control either way.

03

Smaller claimants post availability-check links, which can at most record a moment of unreachability, not an outage.

CHAPTER 07

Threat actors

07

THIS CHAPTER ANSWERS

Who is behind the activity, how are the actors connected, and what does public reporting say about each of them?

8

actor profiles; public reporting checked for each, found for six

7.1 How the actors connect 54
7.2 State-linked espionage 56
7.3 Hacktivist and DDoS actors 58
7.4 Ransomware and extortion 64
7.5 Criminal personas seen in Blackhole 65
7.6 Unattributed intrusion campaigns 66

CHAPTER 07

Threat actors

IN SHORT

Four actor types matter for Azerbaijan. Two intrusions are publicly attributed to state-linked groups: a vendor named one (entry through a vulnerable Exchange server), an official the other (entry route not published). The Freshdesk phishing campaign was not attributed; other reported cases name only a persona, a group or a suspect (§7.3, §7.6, §8.5). Hacktivists claim disruption, and a criminal market trades Azerbaijani identity and payment data. Ransomware groups are the least visible. Patch edge servers first, and verify every hacktivist claim before comment.

Each profile separates **observed behaviour**, **the actor's own claim**, **what remains unresolved** and **what it means for organisations**. Confidence applies to a specific proposition, not to the actor as a whole.

7.1 How the actors connect

The map links actors only where we hold evidence, and each line says what kind: the actor's own post, a third-party relay, an official statement or public reporting. A line is an association, not proof of a common operator. Wolves of Turan appears on the map only as a comparator named in public reporting on Armenian code [S29] and is outside the eight profiles.

Own post Relay Official statement Public reporting Our observation

Second DDoS-for-hire service (credited by the group)

own post
credited ↑

313 Team

own post
credited ↓

Litterbox / Catbox (DDoS)

official
named as the service used (APA, citing the agency) ↑

National Cybersecurity Agency

DieNet

relay
claims relayed by tracking bots ↓

Relay channels

Armenian code

public reporting
one team behind both? ↓

Wolves of Turan (reported comparator, outside the 8 profiles)

menpolisem

observation
similar listings, 3 days ↑

xploitleaks

own post
invokes the brand ↑

state-platform claim poster

NO EVIDENCED LINK TO OTHER ACTORS

Python Squad / Team Python

F ~ INTELLIGENCE

7.2 State-linked espionage

FamousSparrow

overlaps Earth Estries

Espionage (China-linked per Bitdefender) | China-linked (vendor attribution)

IN AZERBAIJAN, DEC 2025 - FEB 2026

Dec 2025

Web shell on an oil and gas company's Exchange server

Jan 2026

Second wave: Terndoor attempted via loader

Feb 2026

Third wave: modified Deed RAT, new C2

TARGETED SECTOR

Energy (oil and gas)

SEEN IN PUBLIC REPORTING

[S12] Bitdefender (13 May 2026): moderate-to-high confidence attribution; the region had not previously been linked to this cluster in public reporting (one victim)

[S55] Government CERT (15 May 2026): checked the published indicators across AzStateNet, reported no evidence of FamousSparrow activity there, and applied preventive blocks

OUR ASSESSMENT

The most consequential documented intrusion of the year. Entry and re-entry through an internet-facing Exchange server still exploitable through ProxyNotShell (CVE-2022-41040, CVE-2022-41082).

CONFIDENCE

Moderate-to-high (vendor)

The intrusion entered and re-entered through the same Exchange server after remediation attempts. Web-shell activity was first seen on 25 December 2025, and Deed RAT appeared in the first wave. The second wave attempted a Terndoor deployment through a loader, and the third used a modified Deed RAT with new command-and-control infrastructure [S12]. Selected techniques that Bitdefender names are shown below, mapped to current MITRE ATT&CK IDs and tactics (Bitdefender's original table used older ATT&CK labels).

TECHNIQUES NAMED IN THE VENDOR RESEARCH, BY TACTIC

Initial access	Persistence	Defence evasion	Defense impairment	Execution	Lateral movement	Stealth
T1190 Exploit public-facing application (ProxyNotShell on Exchange: CVE-2022-41040, CVE-2022-41082)	T1505.003 Web shell T1543.003 Windows service	T1574.001 DLL: DLL side-loading	T1685 Disable or modify tools (API hooking)	T1059.001 PowerShell	T1021.001 Remote desktop T1021.002 SMB / admin shares	T1014 Rootkit: attempted kernel-driver service

Techniques from Bitdefender's report of 13 May 2026 [S12], displayed with current MITRE ATT&CK v20.1 IDs and tactics (checked 23 November 2026): T1574.001 for DLL side-loading, T1685 under Defense Impairment (TA0112) for disabling or modifying defensive tools, and T1014 under Stealth for rootkit activity. Bitdefender's original table used older pre-v17 labels for those three rows. [S12]

Patch reference. ProxyNotShell is two Microsoft Exchange Server flaws: CVE-2022-41040 (server-side request forgery) and CVE-2022-41082 (remote code execution) [S51]. NVD lists Exchange Server 2013, 2016 and 2019 as affected and records that CISA lists both as known exploited [S51]. Microsoft's advisories give the security updates that fix them [S52]. Verify that neither can still be exploited, including where a mitigation rule was used instead of the patch. Bitdefender's report publishes indicators for this intrusion [S12]; load them into mail-server and EDR hunts.

On 15 May 2026 the Government CERT stated that it had checked the published indicators across the AzStateNet government network and found no evidence of FamousSparrow activity there [S55]. It applied preventive blocks on those indicators and advised state institutions to screen outbound connections against them [S55].

Unresolved. The victim's identity, the data taken and whether other Azerbaijani energy firms were affected. **Meaning.** A 2022 vulnerability on an internet-facing mail server was enough for repeated access by a group Bitdefender links to a state from December 2025 into 2026. For energy, transit and government organisations, the decisive controls are edge-system patch verification, web-shell detection on mail servers and alerting on remote-desktop use with domain-admin credentials from internal hosts. Nothing in this case appeared in the 2026 leak-site and forum data we searched.

APT29

Midnight Blizzard

Espionage (Russia-linked per official statement) · Russia (official Azerbaijani attribution)

IN AZERBAIJAN (2025, PRIOR REPORTING)

Feb 2025

Attack on Azerbaijani media outlets, attributed in May 2025

TARGETED SECTOR

Media platforms

SEEN IN PUBLIC REPORTING

[S13] Trend News Agency (2 May 2025): a parliamentary commission chair stated that forensic analysis matched the attack to APT29, with two to three years of access

OUR ASSESSMENT

Official attribution, not independently confirmed. Long dwell times favour identity and email telemetry over perimeter alerts.

CONFIDENCE
As stated by an official

Unresolved. No independent technical report on the case was available to us; we present the attribution as stated by an official, not as independently confirmed. (The landing page for an earlier Brandefense report dated the attack to February 2024 [S9]; its cited source and the official statement date it to February 2025 [S13].) **Meaning.** If the official account is accurate, media organisations face espionage and influence operations with long dwell times, which identity and email-system telemetry detect better than perimeter alerts.

Coverage boundary for state-linked activity. On 19 November a deputy minister of digital development reported that authorities had examined the activity of 10 APT groups in 2026, without naming the groups or targets [S37] [S56]. This report profiles only the two state-linked groups named in public vendor or official attributions. The other official investigations cannot be characterised from the public detail available.

7.3 Hacktivist and DDoS actors

313 Team

Islamic Cyber Resistance in Iraq

Hacktivist (DDoS) | Pro-Iranian (per OC Media, Unit 42); reported to operate from Iraq

IN AZERBAIJAN, 2026

13 Oct
Announces action, citing what it called a hijab ban in schools (B10)

13 Oct
Claims 47 IP ranges, >2.5 Tbps, 1,825 sites offline (B11)

14 Oct
Extends by 24 h; 54 ranges (B17)

16 Oct
Extends by 48 h; "four consecutive days"

CLAIMED TARGETS

Government portals, ministries and other state institutions

IN THEIR WORDS

"we will completely destroy its government digital infrastructure" B10

SEEN IN PUBLIC REPORTING

[S20] OC Media: claimed the October attack; authorities counted more than 100 state domains

[S27] Security Affairs: claimed a 24-hour DDoS on a social-media platform in April 2026; the platform confirmed a DDoS attack

[S26] Graphika: claimed disruption of a global e-commerce platform in April 2026 and used media coverage to bolster credibility

[S28] Unit 42: described as an active pro-Iranian hacktivist cell, with claims against Kuwaiti government and defence websites

OUR ASSESSMENT

A repeat claimant. Its October claim coincided with an officially reported attack that used a commercial DDoS service; the group's own role and capacity remain unverified, and its figures were not confirmed.

CONFIDENCE
High that it claimed the campaign; role and capacity unverified

DieNet

DieNet v2

Hacktivist DDoS brand | Pro-Palestinian (per the Center for Internet Security); NETSCOUT describes its attacks as ideologically driven

IN AZERBAIJAN, 2026

7 Mar
Four Azerbaijani sites, including an airport site, named in automated tracking relays (B14)

CLAIMED TARGETS

A news site, a payment-terminal provider, a travel company, an airport site

RELAY WORDING

"it may be down for you at the moment" B14

SEEN IN PUBLIC REPORTING

[S24] NETSCOUT: appeared on Telegram in March 2025; over 60 claims in two months; many appeared to have no impact

[S24] NETSCOUT: found no owned botnet and assessed that DieNet likely used rented DDoS infrastructure shared with other groups (2025 observations)

[S25] CIS: many claimed attacks hit minor web pages and likely caused no significant outage

OUR ASSESSMENT

An opportunistic brand whose Azerbaijani claims were one evening of relayed probe results. Treat as noise unless an availability monitor agrees.

CONFIDENCE
Claims observed; impact unverified

Python Squad

Team Python

Hacktivist (DDoS claims) | Pro-Palestinian framing tied to Azerbaijan-Israel relations

IN AZERBAIJAN, 2026

17 Mar
Two transport companies and an entertainment company claimed in one minute (B12, B15)

CLAIMED TARGETS

Transport and entertainment booking sites

IN THEIR WORDS

"resulting in a total shutdown of its digital infrastructure" B12

SEEN IN PUBLIC REPORTING

No reputable public reporting found on this group; its own channel is the only source

OUR ASSESSMENT

A low-profile channel posting in Azerbaijani and English; no reputable public reporting was found on this group beyond its own channel. Claims arrived together with availability-check links, which can at most record a moment of unreachability.

CONFIDENCE
Low; single-source claims

Armenian code

Self-styled Armenian-nationalist channel (DDoS, OT claims) | Presents as Armenian-nationalist

IN AZERBAIJAN, 2026

2-5 Feb
Claims tampering with a Baku water-reservoir panel and a water-supply SCADA system

10 Feb
DDoS claims: a transport operator, an airport site, a port

CLAIMED TARGETS

Universities, insurers, logistics, airport, transport, tourism, industry, defence, banks, a state portal, water and heating OT

IN THEIR WORDS

"Azerbaijan suffers from our cyberattacks on their industry, tourism" B16

18 Feb
DDoS claims: a state portal, two finance firms

19 Feb
DDoS list against several universities

5 Mar
Claims a Baku heating-control system was forced into failure (B13)

9 Mar
DDoS list against three insurers

2 Apr
DDoS list: three logistics firms, a transport company

8 Apr
DDoS: an airport site, hotel booking, a state agency's site

21 Apr
DDoS list: a mining company, a holding group, a travel agency, a defence-sector company (B16)

30 Apr-1 May
DDoS claims against three banks; "crushing the banks of Turkey and Azerbaijan" (B19)

SEEN IN PUBLIC REPORTING

[S29] JAMnews (16 Apr 2026): an Armenian security expert assesses that Armenian Code and its supposed rival Wolves of Turan are run by one team, citing a shared administrator and identical proof links

[S29] JAMnews: language markers suggest Russian-speaking operators; the expert sees a manufactured "cyber war" ahead of Armenia's June 2026 elections

OUR ASSESSMENT

One published expert analysis assesses that the channel and its supposed rival may be run by one team. Treat the nationalist label as unverified and check each claim, including any OT claim, with the operator.

CONFIDENCE
Medium that the label is unreliable (one expert analysis)

F ~ INTELLIGENCE

#opazarbeijaan

Hacktivist (DDoS claims) | Pro-India framing; cites what it called Azerbaijan's support for Pakistan

IN AZERBAIJAN, 2026

29 Mar
Capital-markets firm site with check link

30 Mar
A state portal

31 Mar
Bank investment site; claims the site was geo-blocked after 12 hours

5 Apr
A state security body's site (B23)

CLAIMED TARGETS

State portal, a state security body, finance

IN THEIR WORDS

"St4tus: D0wn, n0t R3sponding" B23

SEEN IN PUBLIC REPORTING

No public reporting found that corroborates these claims or names the operators

OUR ASSESSMENT

A short campaign from a direction not seen elsewhere in our 2026 data, framed in terms of India-Pakistan tensions; no public reporting was found that corroborates these claims or names the operators. Check links record at most a moment of unreachability.

CONFIDENCE
Claims observed; impact unverified

Evidence card B13 5 Mar 2026

Armenian code | Actor channel | Telegram | English, as posted

ORIGINAL

A remote heating control system in Baku was hacked. As a result of the breach, the radiators were set to the maximum value, but the system itself was forced to operate in cooling mode. Result: both boilers were brought to an emergency condition.

Held
The claim.

Not established
Any of it; no operator confirmation.

Evidence card B19 1 May 2026

Armenian code | Actor channel | Telegram | English, as posted

ORIGINAL

[...] we are crushing the banks of Turkey and Azerbaijan.
[Turkish bank] [check link removed]
[Azerbaijani bank] [check link removed]

Held
The statement and two availability-check links, one of them for an Azerbaijani bank.

Not established
Any effect on the bank.

The September defacement wave, reported in a relayed notice that attributes it to **Xscyth3**, is the largest other 2026 hacktivist-style case in our data. A defacement feed also relayed a single defacement by Seniman1337 (15 February). A local channel relayed a monitoring notice attributed to the National Cybersecurity Agency (MKA in Azerbaijani). It reported 22 .az sites defaced in a day, 19 of them on one hosting network; the notice named the persona but no motive. Its recommendations (audits, CMS and plugin updates, password changes, MFA and log review) are general hygiene advice; how the sites were entered is not established (B18).

Evidence card B18 25 Sep 2026

Local security channel | Local relay of a notice attributed to the National Cybersecurity Agency | Telegram | Azerbaijani

ORIGINAL

".AZ" DOMENLƏRİNƏ KÜTLƏVİ KİBERHÜCUM
MKA-nın monitorinqi zamanı eyni gündə 22 ".az" domenində Web Defacement hadisəsi aşkarlanıb. Hücumların "Xscyth3" adlı kiberdələduzla əlaqəli olduğu bildirilir. 22 domenin 19-u [hosting network removed] şəbəkəsində yerləşib [...]

TRANSLATION

MASS CYBERATTACK ON ".AZ" DOMAINS
During monitoring by MKA (National Cybersecurity Agency), web defacement was detected on 22 ".az" domains on the same day. The attacks are reported to be linked to a cybercriminal called "Xscyth3". 19 of the 22 domains were hosted on [hosting network removed] [...]

Note. MKA is the Azerbaijani acronym of the National Cybersecurity Agency (Milli Kibertəhlükəsizlik Agentliyi); we hold only the local channel's relay of the notice. The notice recommended audits, CMS and plugin updates, password changes, MFA and log review.

Held
The relayed notice and its recommendations.

Not established
The method; the attribution to Xscyth3 is the notice's own.

7.4 Ransomware and extortion

No accepted Azerbaijani ransomware listing in 2026, against five in Georgia, two in Armenia and none in Kazakhstan

Azerbaijan

0

Accepted listings, 1 Jan-18 Nov 2026

2025	All time
1	1

Groups in 2026

None listed

Georgia

5

Accepted listings, 1 Jan-18 Nov 2026

2025	All time
4	17

Groups in 2026

RansomHouse, Krybit, Thegentlemen, Nightspire, INC Ransom

Armenia

2

Accepted listings, 1 Jan-18 Nov 2026

2025	All time
0	2

Groups in 2026

APT73

Kazakhstan

0

Accepted listings, 1 Jan-18 Nov 2026

2025	All time
0	2

Groups in 2026

None listed

Source: Brandefense Ransompedia accepted listings, all dates, to 18 November 2026 [S6]; ransomware.live as a cross-check [S7].

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

The single Azerbaijani listing (2025) is an extortion claim against an insurer. On 6 March 2026 a Telegram seller advertised, for 600 Telegram Stars, a "final database" of insurance, medical, vehicle and internal records. It said the data leaked from an insurer in 2025. Whether it relates to the 2025 listing is unknown; we did not obtain the files.

Relay labels we rejected. Two further 2026 claims labelled Azerbaijan appeared only in third-party relays in Blackhole. A DeadLock claim (26 July) names an IT and recruitment firm whose own description places it in the United Kingdom, so the label is doubtful. An INC Ransom relay (22 August) was wrongly labelled Azerbaijan; Ransompedia records the company as Spanish, so it is excluded. A public tracker lists one Azerbaijani victim in 2026 (the same DeadLock claim) and two in 2025 [S6][S7].

What this means. Very few public extortion claims name Azerbaijani organisations. That is a measurement of what extortion groups chose to publish, not proof that no Azerbaijani organisation was attacked; negotiated, unpublished and pre-publication incidents are invisible here. It does suggest what should drive ransomware

readiness in Azerbaijan. One driver is the region's group mix (The Gentlemen, INC Ransom, Krybit and others in Georgia, and APT73 in Armenia). The other is the device and credential findings in Chapter 3, the usual entry routes.

7.5 Criminal personas seen in Blackhole

xploitleaks

Data-seller brand | Financial

IN AZERBAIJAN, 2026

30 Jan
Offers 817,241 Azerbaijani student records (B01)

29 Oct
Invoked by a separate poster in a state service platform "all citizen info" claim (B04)

17 Nov
Posts that it buys active sessions in government entities (B21)

CLAIMED TARGETS

Population and student data

IN THEIR WORDS

"Azerbaijan Student Data [...] 817241 Row" B01

SEEN IN PUBLIC REPORTING

[S30] Dark Web Informer (13 Jan 2026): the same handle claimed a large Iranian chat-platform database, sold exclusively through Telegram; unverified

OUR ASSESSMENT

A regional data-seller brand that markets large population files and, in November, sought paid access to government systems. Brand reuse by another poster shows the name carries value; it does not establish a common operator.

CONFIDENCE
High that offers were made; authenticity unverified

Other personas and brands, aliases only; no contacts, links or real identities.

Persona or brand	Observed role in 2026	Own claim	Unresolved
xploitleaks	Seller brand; student data (Jan) and government-session buyer post (Nov); brand invoked by a separate poster in a state service platform claim (Oct)	Own claim: 817,241 student rows (Jan). Claim invoking the brand (separate poster, Oct): "all citizen info"	Whether one operator; data origin
menpolisem	Leak-forum poster of student and citizen data titles (Jan)	Data leak	Relationship to xploitleaks
Simon111	Leak-forum poster: "sensitive files" of an Azerbaijani institute (Feb)	Data leak	Content and origin
0cx00iq	Breach-forum seller of a database attributed to a state security body (Jul)	Sale to "two buyers only"	Any verification
ComboPoster	Cracking-forum poster of an "Azerbaijan combolist" (Apr)	Combolist	Size, age
X FORUMS (bot)	Automated uploader of small credential files, including .az domains	None	Not a person; a distribution bot
databreach000	Breach-forum seller of passenger data attributed to an Azerbaijani transport company (Nov)	800K passengers, 10K upcoming trips	Origin; any verification (Case F)
iq313	Breach-forum poster of a 400 GB "Azerbaijan DB" torrent (Oct)	Dump	Contents, origin
An Azerbaijani-flagged carding channel	408 distinct Azerbaijan-associated cards in clear text in checker outputs, mostly Jan-Feb	Live cards	Operator; card source

7.6 Unattributed intrusion campaigns

In June the National Cybersecurity Agency disclosed a large phishing campaign run through the legitimate Freshdesk support platform, Report.az reported [S33]. According to that report, it used the names of transport, oil and gas, trade and business-development organisations. It also used official mailboxes that attackers had earlier gained access to. An adversary-in-the-middle (AiTM) page, which relays a real login, captured passwords and one-time MFA codes in real time. The agency did not attribute the campaign. For energy and transport organisations it is the most direct documented route from email to account hijacking.

KEY TAKEAWAYS

01

FamousSparrow is the most consequential documented intrusion; the APT29 case rests on an official attribution.

02

A commercial DDoS service was officially identified in the October attacks; one expert assesses a nationalist brand as a possible false flag.

03

Data-seller brands are reused by others; a brand name is not proof of a common operator or a breach.

CHAPTER 08

The fraud economy

08

THIS CHAPTER ANSWERS

How do criminals turn Azerbaijani identities and accounts into money, and what does it cost them?

60 USD

median asking price for a bank or wallet account

8.1 Bank and payment-account trading 69

8.2 Card material in posts: a narrow view 69

8.3 Identity, KYC and SIM services 69

8.4 Prices in context 70

8.5 What police and cyber authorities reported 70

CHAPTER 08

The fraud economy

IN SHORT

Bank and payment-account trading is the largest category in our cleaned Blackhole corpus; carding and identity-document offers are also prominent, alongside SIM and cash-out services. Prices are low and Azerbaijan is usually one market among many on Russian-language price lists. Confirm payment instructions out of band, and assume identity data is known to criminals.

8.1 Bank and payment-account trading

Bank-account trading is the largest cleaned crime family (2,368-2,719 posts). Typical posts buy or sell access to bank and wallet accounts, recruit "drops" who open accounts for others, or ask for "drops in Armenia, Georgia, Azerbaijan, Kazakhstan". Azerbaijani wallets and payment services appear alongside banks; one post offered to buy a wallet account for 15 AZN. The risk these offers create for banks is not a hack of the bank but mule accounts: accounts opened or rented under real identities that could later carry fraud proceeds. The posts show the offers, not that such accounts were opened or used at any assessed bank.

8.2 Card material in posts: a narrow view

SCOPE OF THE CARD FIGURES

The card figures in this report cover only payment cards that appeared in clear text inside the dark-web posts we collected for this report. Brandefense detects stolen cards through many other methods, which this report does not cover. These figures are not a measure of card theft or fraud loss in Azerbaijan.

Within that narrow scope, 657 distinct Azerbaijan-associated cards appeared in clear text in collected posts: 529 attributed to one of 17 named Azerbaijani banks and the other 128 labelled only as Azerbaijani, without an issuer. Most of them appeared in card-checker output in January and February; one Azerbaijani-flagged channel accounts for 408 of them. We stored no card numbers, expiry dates, security codes or names (Appendix A.6) [S8]. The useful signal for issuers is the checker pattern itself: batches of cards tested with small authorisations against merchant gateways (Chapter 9).

8.3 Identity, KYC and SIM services

KYC and document posts (903-993 cleaned) offer to pass verification at exchanges and casinos, register companies with nominee directors, provide document templates and "verification for money", and recruit people from Azerbaijan for paid verification. Telephony services list Azerbaijani numbers for rent and SMS reception. Combined with the population datasets in §4.4, these services lower the cost of opening accounts in someone else's name.

8.4 Prices in context

Product (cleaned posts)	Median asking price	Spread
Card (per card)	15 USD	10-40 USD
Bank or wallet account	60 USD	60-90 USD (often local-currency quotes)
KYC or document service	65 USD	30-190 USD
Access offer	2,500 USD	Wide, few values
"State register" dataset	2,000 USD	Single offer
Small DDoS job	3-50 AZN (about 2-30 USD)	Few values

Prices are asking prices from a minority of posts that quote one; they do not measure market value or completed sales. Spread is the middle half of the quoted prices (25th to 75th percentile), so it is not the full range. Some individual quotes fall outside it, such as the 15 AZN (about 9 USD) wallet bid in §8.1. The DDoS quotes come from a local services chat. AZN amounts are converted at about 1.70 AZN per USD.

8.5 What police and cyber authorities reported

The posts show offers. The reports below describe attempted attacks and reported fraud cases; all were published in 2026. The blind audit in Appendix A.8 found them; none appeared in our Blackhole data.

Date	Reported by	What happened
Feb, May, Aug	Interior Ministry cybercrime department	Fake bank and lender "low-interest loan" pages collected card details, including security and one-time codes. In the February case the ministry reported about 500 victims and, citing the suspects' initial statements, about 400,000 AZN [S40]. The ministry reported detentions in separate, similar loan-page scams in May [S38] and August [S39]
6 Feb	Electronic Security Service	The service investigated an attempted attack on government and bank organisations using files hidden with steganography; opening them could download the Remcos remote-access tool [S41]
27 Feb	Electronic Security Service	Emails from a group called Narketing163 imitated known brands and were sent to state and private institutions; part of the malicious code was spread through a .az resource, which the service identified, preventing further spread [S42]

Date	Reported by	What happened
8 Apr	Government CERT (State Service for Special Communication and Information Security)	A mass phishing campaign targeted government email addresses on the Az-StateNet network, using fake criminal-investigation notices and demands for payment [S43]
10 Apr	Electronic Security Service	Acting on a tip from Hungary's national cybersecurity centre, the service found malicious files on a local organisation's server that was being used against foreign systems [S44]
22 Jul	Interior Ministry	A suspect used software he had developed to obtain companies' business-banking credentials, then sent login-approval requests that were approved without their source being checked; losses exceeded 100,000 AZN [S45]
10 Aug	State Security Service, as reported by APA	Foreign-run networks sent "urgent" WhatsApp messages to civil servants and company staff from fake accounts carrying their managers' photos, then referred them to fake law-enforcement accounts that instructed transfers to foreign accounts [S46]
18 Aug	National Cybersecurity Agency	Attempts against organisations' Microsoft 365 and other email accounts, from foreign addresses and from VPN or proxy traffic exiting in Azerbaijan [S47]
14 Sep	National Cybersecurity Agency	TikTok accounts advertised fake payment sites offering cheap mobile packages to harvest card details [S48]

What this tells defenders. The police cases that state amounts describe fake loan pages and stolen credentials combined with unchecked login approvals, not the database sales that dominate dark-web headlines. Manager impersonation over messaging apps, reported without a loss figure, targets the same weak point: payment instructions that are not confirmed through a second channel. The controls are both procedural and technical: out-of-band confirmation of payment instructions, number-matching MFA, protection and monitoring of business-banking credentials, and customer warnings about loan advertising.

KEY TAKEAWAYS

01

Account trading, not card theft, is the largest fraud signal in the posts we collected; police cases with amounts describe fake loan pages and unchecked approval prompts.

02

Card figures cover only cards seen in clear text in collected posts (§8.2).

03

KYC, SIM and population-data services together lower the cost of opening accounts in someone else's name.

CHAPTER 09

Banking and finance deep dive

09

THIS CHAPTER ANSWERS

Where does the visible exposure of Azerbaijani banks sit: in the bank, at its staff, or at its customers?

5 of 22

card-issuing banks with a current credential listing, the first item to triage

CHAPTER 09

Banking and finance deep dive

IN SHORT

Most visible exposure sits on the customer side: 7,520 non-employee device associations (most plausibly customers' devices), card-checker activity and account-trading chats. The bank- and staff-side signals are current listings at 5 of 22 issuers and 167 employee-classified devices. Three issuers carry most of the card and customer-device signals. Triage each current credential listing first (validate the account and record a disposition). Then validate employee devices, and monitor checker declines on your BIN ranges (a BIN is the issuer's card-number prefix).

This chapter covers the 22 card-issuing banks among the 35 banking-and-finance organisations in Chapter 3; the other 13 are not card-issuing banks. That is why 7,520 non-employee devices here differs from 11,249 there, 167 employee devices from 195, and 5 of the sector's 11 current listings sit at issuers. Aggregates only; individual banks are not named.

5 of 22

issuers with a current credential listing (5 of the sector's 11 current listings; the other 6 sit at organisations that do not issue cards)

11 of 35

banking and finance organisations with a current credential listing

21 of 22

issuers with non-employee device associations (7,520 in total; ownership and current infection unverified)

19 of 22

issuers with employee-classified devices (167 in total)

31 of 35

banking and finance organisations enforcing DMARC

17 of 22

card-issuing banks on our list with cards in clear text in collected posts (529 of the 657 cards name one of them; narrow scope, §8.2)

The top three issuers account for 90% of the attributed cards and 75% of the non-employee device associations.

What it means for banks.

1. **Current listings come first.** 5 of 22 issuers had one on the day of the check; apply the first decision in §1 (disposition within 5 working days).

2. **Employee exposure is small but real.** 167 employee-classified devices across 19 banks, plus one employee mailbox in a combolist, are the intrusion-relevant subset. After current listings, these deserve priority validation over the much larger non-employee total.
3. **Non-employee device associations are the larger exposure.** 7,520 device associations across 21 of 22 issuers are not employee-classified, and most plausibly they are customers' devices. Ownership, current infection and whether any stored session or password still works are unverified and require validation. Fraud teams should use device and session risk signals at login and at payee changes, not only password checks.
4. **Card checking is a detectable precursor.** Checker bots test cards with small authorisations or card-add attempts on merchant gateways. Issuers can detect clusters of declined low-value attempts from foreign gateways on their BIN ranges, identify the cards involved, check their authorisation and fraud signals, and reissue the cards confirmed at risk under issuer policy.
5. **Mule accounts are the downstream risk.** Account-trading posts target banks with remote onboarding; they do not show that accounts were opened or used at the assessed banks. Onboarding controls should assume that name, birth date and address are known to criminals (§4.4).

KEY TAKEAWAYS

01

Current credential listings at 5 of 22 issuers come first, then the 167 employee-classified devices; the 7,520 non-employee ones also need validation.

02

Banking and finance organisations enforce DMARC widely (31 of 35).

03

Card-checker declines on your BIN ranges are a detectable precursor.

CHAPTER 10

Regulatory and national response

10

THIS CHAPTER ANSWERS

What changed in Azerbaijan's cyber governance in 2026, and what must an organisation have in place before the new fines apply?

1 Jul 2027

Article 371-2 fines enter into force

CHAPTER 10

Regulatory and national response

IN SHORT

2026 reshaped Azerbaijan's cyber governance: a National Cybersecurity Agency, new duties in the information law, and new administrative fines effective 1 July 2027. Several rules are still being drafted. Use the applicability table to confirm which regime applies to you, and name your incident reporter now.

Measure	What we could verify	Status and caution
National Cybersecurity Agency	Established by presidential decree on 2 June 2026 as a public legal entity on the basis of, and legal successor to, the Electronic Security Service, subordinate to the Ministry of Digital Development and Transport [S15][S22]	Its regulation and control cover cybersecurity and personal-data protection. For critical information infrastructure and state-body infrastructure its role is information exchange only, and its preventive measures exclude them. Its charter adds the national computer incident response centre, threat and incident analysis, a personal-data system register and audits, and measures against online gambling through telecom services and access to foreign betting operators [S22]
Cybersecurity amendments to the information law	A new chapter added to the Law on Information, Informatization and Protection of Information (10 August 2026, per legal commentary) [S18]	Specific rules for government bodies and critical public infrastructure were still being prepared in November 2026, according to the Deputy Speaker [S19]
Administrative offence Article 371-2	Law signed 14 July 2026, published 2 September 2026; Article 371-2 **enters into force on 1 July 2027** [S21]. Breaches of 371-2.1 (duties listed below) carry 500-1,000 AZN for officials and 1,000-2,000 AZN for legal entities. 371-2.2 covers operating an incident-response centre or SOC without registry entry: 1,000-1,500 and 1,500-2,500 AZN [S21]	Excludes critical information infrastructure; state bodies, including the Central Bank; intelligence and counter-intelligence bodies; supervised financial-market entities; protected or strategic facilities; and incident-response centres and SOCs set up by the designated body or the Central Bank [S21]. Legal commentary [S18] gives only the 371-2.2 fine band
Incident notification	Article 371-2.1.2 penalises information-infrastructure subjects that do not report cyber threats, attacks or incidents immediately to the designated body [S21]	Penalty enforceable from 1 July 2027; reporting channel and format to be set by implementing rules
Personal data protection	The 2010 law remains in force as far as we could verify; a replacement was in drafting	Adoption not confirmed

Article 371-2.1 applies to incident-response centres, SOCs and information-infrastructure subjects, including internet and hosting providers and internet-resource owners, that:

- fail to follow the designated body's instructions;
- do not report cyber threats, attacks or incidents immediately;
- miss the designated body's deadlines (24 hours on cybersecurity status or proactive research, five working days for digital-investigation requests);
- lack continuous monitoring and initial response;
- breach cybersecurity requirements for public-importance infrastructure, or obstruct forensic research.

The law does not name the designated body; it refers to a body designated by the relevant executive authority [S21]. Article 371-2.1.5 speaks of infrastructure performing functions of public importance, a different term from the critical information infrastructure excluded in the exclusion note following Article 371-2.

Does Article 371-2 apply to you? The table reads the exclusions in the law [S21] for four common cases.

Organisation	371-2 applies?	Action now
Licensed bank, insurer, payment provider or other supervised financial-market entity	Excluded	Follow your financial-market supervisor's requirements (the law describes these entities as supervised but does not name the supervisor); ask counsel about other cyber duties
Critical-infrastructure operator	Excluded if designated as critical information infrastructure	Confirm your designation in writing; rules for such infrastructure were still being prepared [S19]
State body	Excluded	Track the state-body rules being prepared [S19]; name an incident reporter now
Any other organisation, including providers and internet-resource owners (many of the 250)	Applies, unless an exclusion covers you	Name an incident reporter; build monitoring and initial response before 1 July 2027

What CISOs should do now. Map whether your organisation is an information-infrastructure subject, an internet-resource owner or a provider under the new chapter, or falls under an exclusion. Name the person who would report an incident to the designated body. Build the monitoring and response capability that 371-2.1 expects before 1 July 2027. Keep a dated record of the controls you implement, because implementing rules are still arriving. This section is not legal advice.

KEY TAKEAWAYS

01

A National Cybersecurity Agency now succeeds the Electronic Security Service.

02

Fines for failing to report incidents or follow instructions apply from 1 July 2027, with important exclusions.

03

Map your status under the new chapter now; implementing rules are still arriving.

CHAPTER 11

Outlook

11

THIS CHAPTER ANSWERS

What should Azerbaijani organisations plan for next, and what evidence would change that plan?

5

key judgements, each with a signal to watch

11.1 Key judgements 81

11.2 What would change the assessment 82

11.3 Conditional scenarios 82

CHAPTER 11

Outlook

IN SHORT

Plan for the same evidence types, not a new threat. These are identity exposure that stays invisible until it is used, politically motivated DDoS, and espionage. Espionage reached energy through edge systems (one documented case) and media (one official attribution, entry route not published). We have no comparable time series to say whether any of them is growing. Change the plan when the evidence below changes, not on a calendar.

11.1 Key judgements

Judgement	Confidence	Basis and limit
Identity exposure (devices, stealer logs, credential listings) is the most widespread measurable risk to Azerbaijan's leading organisations	High for the 250-organisation list	190 with devices, 222 with credential records, 80 with current listings; not national prevalence
Accepted Azerbaijani leak-site listings are rare relative to neighbours	High for observed listings	0 accepted Azerbaijani listings in 2026 vs 5 in Georgia; unpublished incidents invisible
If actor channels cite new political or religious themes about Azerbaijan, plan for hacktivist DDoS claims	Medium (planning assumption)	Four distinct hacktivist actor sets (313 Team, Python Squad, Armenian code and F ~ INTELLIGENCE; §6.1-6.3) cited such themes in 2026; signal: target lists in actor channels
If known edge vulnerabilities remain exploitable, plan for state-linked espionage attempts against energy and media organisations	Medium (planning assumption)	One detailed 2026 vendor case (energy) and one official 2025 attribution (media); small sample; signal: vendor advisories and scanning
Plan for further citizen-data offers using government names	Medium (planning assumption)	Four large offers and several re-posts in 2026; authenticity unverified; signal: new offers in monitored channels

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

11.2 What would change the assessment

Current interpretation	Evidence that would change it	Decision affected
Accepted Azerbaijani leak-site listings were rare in this collection	Accepted leak-site listings naming Azerbaijani organisations, or a disclosed extortion incident	Raise ransomware readiness priority; run the restore test in §12.1 first
Citizen-data offers are unverified	A sample matched to a specific system's schema, or an official confirmation	Trigger notification and customer-protection actions for that dataset
Hacktivist figures exceed what authorities confirm	Official confirmation of sustained outage of critical services, or of attacker identity beyond the group's claim	Revisit upstream mitigation capacity and service-continuity plans
Current listings mean "validate", not "breached"	Validation shows active accounts without MFA among listed credentials	Escalate to incident response and enforce MFA for the affected population
Espionage evidence is one vendor case and one official attribution	Further vendor or official reports of Azerbaijani energy, transport or government intrusions	Fund edge-system and identity telemetry ahead of other projects

11.3 Conditional scenarios

- **If** actor channels cite new political or religious themes about Azerbaijan, **then** plan for hacktivist DDoS claims against government and transport portals (a planning assumption, not a measured interval); **signal:** target lists in actor channels. **Decision:** activate the pre-agreed communication line and upstream mitigation.
- **If** a new critical edge vulnerability is disclosed, **then** plan for state-linked and criminal exploitation attempts at energy, government and telecom organisations; **signal:** vendor advisories and scanning activity. **Decision:** patch-and-verify within your patch deadline for internet-facing systems, then hunt for web shells.
- **If** card-checker activity on your BIN ranges rises and investigation confirms that specific cards are being tested, **then** plan for card-not-present fraud attempts on those cards; **signal:** clustered low-value declines from foreign gateways. **Decision:** investigate the attempts, check authorisation and fraud signals, and reissue the cards confirmed at risk.

KEY TAKEAWAYS

01

Plan for evidence types, not a new threat: identity exposure, political DDoS, espionage through edge systems and long-lived access.

02

Each judgement has a signal; change the plan when the signal changes.

03

No comparable time series exists yet to say whether any of these is growing.

CHAPTER 12

Action plan

12

THIS CHAPTER ANSWERS

What should each team do in the next 90 days, and how will the board know it was done?

20

actions with an owner and completion evidence

12.1 30/60/90 days 84

12.2 By role 87

12.3 How Brandefense can help 88

CHAPTER 12

Action plan

IN SHORT

Start by confirming you receive listing and device alerts, then act on the evidence that is specific to you: current credential listings, employee-device associations and internet-facing edge systems. Then close the phishing, payment-approval, email and web gaps, and rehearse hacktivist and identity-fraud scenarios. The board knows the work is done from each row's completion evidence and the scorecard below; report both by day 90.

12.1 30/60/90 days

This is a sequence, not a waiting period. A current material threat should enter your incident process immediately.

1Days 1-30		
Confirm that you receive credential-listing and infected-device alerts for your primary domains; if not, arrange them, and record the listing-validation and employee-device rows as blocked until alerts arrive	OWNER CISO and threat intelligence	COMPLETION EVIDENCE Alert source named; first alert received
For every current credential listing tied to your domains, validate the account and its MFA status within 5 working days	OWNER Identity team	COMPLETION EVIDENCE Each listing has a disposition: reset, already remediated, or not ours, with a date
Validate employee-classified device associations; revoke sessions and tokens where active	OWNER Identity and endpoint teams	COMPLETION EVIDENCE Device list reconciled with asset inventory; revocations logged
Confirm every internet-facing mail and edge server is patched, including CVE-2022-41040 and CVE-2022-41082 on Exchange	OWNER Infrastructure	COMPLETION EVIDENCE External re-test passes; web-shell hunt on mail servers completed

Name the spokesperson and channel for service-status statements during DDoS, and the person who reports incidents to the designated body (§10)

OWNER
Communications, CISO and legal

COMPLETION EVIDENCE
A one-page playbook naming both, approved

Review Microsoft 365 and other mail sign-ins from foreign addresses and VPN or proxy ranges; block legacy authentication (§8.5)

OWNER
Messaging and SOC

COMPLETION EVIDENCE
Sign-in review recorded; legacy authentication disabled

2Days 31-60

Where DMARC is p=none, missing or invalid, inventory senders and stage enforcement

OWNER
Messaging

COMPLETION EVIDENCE
Aligned senders; p=quarantine with a rollback route

Contract or test upstream DDoS mitigation for citizen- and customer-facing portals

OWNER
Infrastructure and procurement

COMPLETION EVIDENCE
Mitigation test record

Test account-recovery and payee-change processes against an attacker who knows name, birth date and address; warn customers about fake loan and card-payment pages (§8.5)

OWNER
Fraud and customer operations

COMPLETION EVIDENCE
Weaknesses recorded and fixed, retest passed; customer warning issued

Monitor session and token anomalies on government systems

OWNER
SOC

COMPLETION EVIDENCE
Alert live and tested

Move privileged and remote users first, then others, to phishing-resistant MFA (FIDO2 security keys, passkeys or certificate-based sign-in) against the adversary-in-the-middle route (§7.6). Use number matching only as an interim step for push and approval prompts (§8.5); CISA calls it an interim mitigation, weaker than phishing-resistant MFA [S53]. Alert on adversary-in-the-middle-style sign-ins from any lure, and revoke the session when one is suspected

OWNER
Identity team and SOC

COMPLETION EVIDENCE
Phishing-resistant coverage recorded per user group; an authorised test AiTM sign-in is detected and its session revoked

Require out-of-band confirmation for payment-instruction and payee changes, including requests that cite a manager (§8.5)

OWNER
Finance and fraud

COMPLETION EVIDENCE
Procedure signed off; one simulated request caught

Reject any business-banking login approval you did not initiate, and register approval devices with your bank (§8.5)

OWNER
Finance and treasury

COMPLETION EVIDENCE
Procedure signed off

Banks: alert on new approval-device enrolment and unusual approval sources for business customers (§8.5)

OWNER
Digital-banking fraud team

COMPLETION EVIDENCE
Alert live and tested

Alert on clustered card-checker declines on your BIN ranges

OWNER
Fraud

COMPLETION EVIDENCE
Alert live; first review recorded

Run a timed restore test of one crown-jewel system

OWNER
Infrastructure

COMPLETION EVIDENCE
Restore time recorded against the recovery time objective (RTO: the longest outage your business-continuity plan allows)

3Days 61-90

Sign DNS for primary domains where your registrar supports it; fix invalid TLS certificates and add HSTS

OWNER
Network and web teams

COMPLETION EVIDENCE
DNSSEC validation succeeds from an external resolver; certificate checks pass

Check homepage content integrity and domain-registration status

OWNER
Web team

COMPLETION EVIDENCE
No unauthorised content on primary sites

Run a tabletop combining a hacktivist DDoS with a simultaneous data-leak claim

OWNER
CISO, communications, legal

COMPLETION EVIDENCE
Decision log and timings

Report the scorecard against targets (below)

OWNER	COMPLETION EVIDENCE
CISO to board	Board paper with remaining gaps and owners

Scorecard targets. These are suggested defaults; set your own where policy differs.

Measure	Target
Current listings with a disposition within 5 working days	100% by day 90
Employee-classified devices reconciled with the asset inventory	100% by day 90
Internet-facing mail and edge servers passing an external retest	100% by day 90
Primary domains with DMARC at quarantine or reject	100%, or a dated plan, by day 90
Privileged and remote users on phishing-resistant MFA (number matching does not count)	100%, or a dated plan, by day 90
Payee and payment-instruction changes confirmed out of band	100% by day 90
Restore test within RTO	Passed, or a dated fix, by day 90
Credential-listing and infected-device monitoring for primary domains, internal or through a provider	In place by day 30

12.2 By role

Role	First decision
Board	Ask for the current-listing and employee-device numbers for your organisation and for the date by which each is validated, and confirm the monitoring that produces them
CISO	Put listing and device monitoring in place first, then prioritise edge-system exploitability checks and identity validation
SOC	Add detections for web shells on mail servers, RDP from internal hosts with domain-admin credentials, AiTM sign-in patterns (for example, a sign-in from an unexpected hosting network right after a legitimate MFA prompt, then the same session reused from a new IP address or device) and mass token use from new devices

Role	First decision
Fraud	Use device and session risk at login and payee changes; monitor clustered card-checker declines on your BINs; warn customers about fake loan and card-payment pages (§8.5)
Communications	Prepare status statements for DDoS and for unverified leak claims, separating claim, verified fact and action

KEY TAKEAWAYS

01

Confirm monitoring, then validate current listings and employee devices in the first 30 days.

02

Stage DMARC enforcement, start phishing-resistant MFA for privileged and remote users and lock down payment changes by day 60; report the scorecard, including DMARC and MFA, by day 90.

03

Rehearse a combined hacktivist and data-leak scenario; DNS signing and TLS fixes follow by day 90.

12.3 How Brandefense can help

Brandefense combines Cyber Threat Intelligence, Digital Risk Protection and External Attack Surface Management. The analysis in this report used the same data and scoring that the platform applies to monitored organisations: infected-device and credential associations, current credential-market listings, lookalike domains, exposed documents and dark-web mentions. It does not promise that every claim can be verified or that a historical record remains usable.

Bring your domains, brands and security priorities to a 30-45 minute demo with Sales and Presales. The team can show how platform monitoring relates external signals to the assets you manage. A Brandefense team member or a partner in your region will follow up.

Request a demo

APPENDICES

Appendices

A–D

THIS CHAPTER ANSWERS

Appendix A. Method · Appendix B. Evidence register · Appendix C. Sources · Appendix D. Glossary

57
sources

Appendix A. Method 90
Appendix B. Evidence register 94
Appendix C. Sources 96
Appendix D. Glossary 100

Appendix A. Method

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

A.1 Window, sources and priority

The research window is 1 January-18 November 2026 by the date a post was published, not the date it was collected. Own data comes first: Brandefense Blackhole (dark-web and messaging posts, infected-device and credential associations, card material in posts), Ransompedia (ransomware leak-site listings) and Brandefense Atlas exposure ratings. External sources give context and are cited after reading the supporting passage (or, where an original post was unavailable, the dated repost or press report noted in Appendix C). Data were extracted on 19 November 2026. Sources S1-S6 and S8 are Brandefense's own data and have no public address. External entries in Appendix C give the source address (or the site root where the full path would name an unconfirmed victim) and the verification date.

A.2 Blackhole posts

Item	Value
Posts with the Azerbaijan country tag	49,097, all retrieved
Keyword sets	Country, city and organisation terms in Azerbaijani, Russian, English and Turkish spellings
Keyword counts	Near-complete; a lower bound from July
Posts after cleaning	6,172-6,901, depending on how strictly repeated templates are removed

Cleaning removed spam, very short posts, automated stress-test logs, repeated template posts and news mirrors. In an informal one-reviewer check of 30 random cleaned posts, 18 of 30 were relevant crime posts concerning Azerbaijan. Because that sample is too small for a corpus-wide rate, cleaned counts remain an upper bound for criminal activity.

Two collection limits shape every trend in this report. Categories are not compared across the year. Collection appears lower from July onwards: Türkiye's tagged volume, which has no comparable bot spike, falls from 528,914 in May to 107,910 in July. From July every compared country is below its January-May average, so we do not read declines from July as threat trends.

A.3 The 250 organisations

Selection, verification and limits are in §3.1. For each primary domain we read the exposure signals that Atlas uses for its ratings. They are infected devices, employee devices, credential records, dark-chat and dark-web mentions, new lookalike domains, documents that reference the domain, and current and past credential-market listings. Data were read on 19 November 2026.

A.4 Atlas ratings

Each organisation received an Atlas exposure rating from these signals. This report publishes only the national headline for the 250 organisations (48 out of 100). Treat a current credential-market listing as a reason to validate accounts, not as proof of a breach.

For 94 organisations with very short or hyphenated brand names, lookalike-domain counts return unrelated domains, so that signal could not be assessed reliably for them. The chart data also hold a separate 2026 lookalike measure, assessed for 150 organisations; it is not the Atlas 30-day lookalike signal (156 assessable).

A.5 DNS, TLS and web checks

We made public DNS queries for mail, SPF, DMARC, DKIM, DNSSEC and CAA records, plus a TLS and homepage check per domain. Missing, invalid and monitoring-only (p=none) DMARC policies count as no enforcement. No scanning went beyond these passive checks.

The passive hygiene index is an Odin analytical composite of these email, DNS, TLS and header checks, on a scale of 0-100. A higher value means weaker hygiene; it is a model, not an Atlas rating.

A.6 Card material in posts

Scope: only payment cards that appeared in clear text in the dark-web posts collected for this report. Brandefense detects stolen cards through many other methods, which are outside this report. These figures do not measure card theft or fraud loss.

We stored no card numbers, expiry dates, security codes or names; only issuer-level counts were kept. Generator output was excluded.

A.7 Ransomware

We used Ransompedia accepted listings for Azerbaijan, Georgia, Armenia and Kazakhstan, all dates, dated by publication. Rejected and duplicate listings are excluded. A public tracker and relayed Blackhole posts are used only as cross-checks.

A.8 Incident coverage

Before release we ran a per-organisation incident sweep. For all 250 organisations we searched the full Blackhole corpus (posts 1 January–18 November 2026) for their domains, names, short names and Azerbaijani and Russian aliases. We read every relevant forum or market hit and every post describing a specific data-leak, access or exploit event.

We also searched public reporting for the priority organisations and the country in English, Azerbaijani, Russian and Turkish, covering national press, CERT notices, vendor research and public monitoring accounts, on 20 November 2026. Twenty-three entries were reviewed. Azerbaijan incidents in the window are reflected in Chapters 2 and 4–8. Most remaining entries concerned other countries or were false matches. One unverified file listing on a public tracker could not be tied to any source and remains open, and one entry is official statistics used in Chapter 2.

Blind audit (20 November 2026). After the sweep we ran an independent "what did we miss" check. Two auditors worked without access to this report. One read the Blackhole corpus, including a fresh pull for 18–20 November, together with Ransompedia and Atlas exposure data. The other searched only open sources in English, Azerbaijani, Russian and Turkish. Of the 14 high-materiality items they listed, 8 were already covered; of 30 medium items, 8 were covered and 5 partly covered.

The following missing items were added: officially reported fraud and phishing cases (§8.5), narrower identity offers (§4.4), and further hacktivist claims (§6.1). Four items were withheld because they rest on official pages we could not retrieve. They are a card-phishing campaign using a national payment brand, a phishing-kit attempt against a holding, a database-server intrusion warning and postal-brand SMS phishing. Item-level counts are kept in an internal audit register. One ransomware-feed entry labelled Azerbaijan proved to concern a Spanish company. The 18–20 November pull added no new incident.

Remaining coverage limits. Our view is still partial:

- Tor ransomware leak sites are covered only through Ransompedia.
- Closed and invite-only forums, private Telegram groups and sales arranged in direct messages are outside our collection.
- Posts deleted before collection are missing.
- Machine translation can miss Azerbaijani slang.
- Some official websites could not be retrieved for checking.
- Incidents that organisations handle without disclosure stay invisible.

That an incident is absent from this report does not mean it did not happen.

A.9 Confidence and boundaries

High confidence applies to a reproducible measurement, not to a criminal's underlying assertion. Medium indicates an interpretation with a clear supporting line and stated limits. "Unverified" means not independently established; it is neither proof of fabrication nor proof of a breach. Victim organisations are described by role; a state body is named only where an official statement confirms the incident. Actor aliases are printed; links, contacts, indicators and personal data are withheld. Full provenance is held in an internal evidence register.

Appendix B. Evidence register

Every post quoted in this report appears as a redacted post card in the chapter shown. Excerpts are short; omissions are marked […]; identifiers, contacts, links and victim organisations are replaced with labels in brackets, under the policy in A.9. Translations are ours unless the post carried the actor's own English. Posting dates are not intrusion dates. Post identifiers, links and full text are held in an internal evidence register.

Card	Posted	Venue	Alias as shown	Language	Shown in
B01	2026-01-30	Leak forum	xploitleaks	English	§4.4
B02	2026-08-09	Telegram channel	X Ticaret	Turkish	§4.4
B03	2026-08-15	Lead-trading Telegram channel	Lead-trading poster	English, apparently machine-translated from Russian	§4.4
B04	2026-10-29	Telegram group	Poster invoking xploitleaks	English	§4.4
B05	2026-02-19	Leak-monitor bot relaying a forum uploader	X FORUMS (bot)	English	§4.5
B06	2026-03-06	Turkish-language forum	arcturus (quoted)	Turkish	§4.5
B07	2026-07-18	Hacktivist-branded channel relaying a breach forum	0cx00iq (relayed)	English	§4.5
B08	2026-08-04	Russian-language drop-services chat	Anonymous buyer	English	§4.6
B09	2026-10-20	Automated dump bot	Dump bot	English	§4.6
B10	2026-10-13	Actor channel	313 Team	Arabic, with the group's own English	§6.2
B11	2026-10-13	Actor channel	313 Team	Arabic, with the group's own English	§6.2
B12	2026-03-17	Actor channel	Python Squad	Azerbaijani, with the group's own English	§6.3
B13	2026-03-05	Actor channel	Armenian code	English, as posted	§7.3

Card	Posted	Venue	Alias as shown	Language	Shown in
B14	2026-03-07	Relay channel of an automated tracking bot	DieNet (relayed)	English	§6.3
B15	2026-03-17	Actor channel	Team Python	English and Azerbaijani, as posted	§6.3
B16	2026-04-21	Actor channel	Armenian code	English, as posted	§6.3
B17	2026-10-14	Actor channel	313 Team	Arabic, with the group's own English	§6.2
B18	2026-09-25	Local relay of a notice attributed to the National Cybersecurity Agency	Local security channel	Azerbaijani	§7.3
B19	2026-05-01	Actor channel	Armenian code	English, as posted	§7.3
B20	2026-11-11	Breach forum	databreach000	English	§4.6
B21	2026-11-17	Breach forum	xploitleaks	English	§4.5
B22	2026-10-18	Breach forum	iq313	English	§4.5
B23	2026-04-05	Actor channel	F ~ INTELLIGENCE	English, as posted	§6.3

Appendix C. Sources

S1: Brandefense Blackhole post corpus, Azerbaijan country tag and keyword sets, post dates 1 January–18 November 2026, extracted 19 November 2026.

S2: Brandefense Blackhole posts of the 313 Team channel, 13–16 October 2026.

S3: Brandefense Blackhole infected-device, breach-database, stealer-log and combolist associations for 250 domains, read 19 November 2026.

S4: Brandefense Atlas domain-scoring method applied to the 250 domains, 19 November 2026, including credential-market listings, lookalike domains, exposed documents and mention statistics.

S5: Brandefense public DNS, TLS and homepage checks of the 250 domains, 19 November 2026.

S6: Brandefense Ransompedia, accepted listings for Azerbaijan, Georgia, Armenia and Kazakhstan, all dates, extracted 19 November 2026.

S7: ransomware.live, country victims for AZ, GE, AM, KZ, accessed 19 November 2026 (cross-check only). https://www.ransomware.live/ (article URL withheld). Verified on 21 November 2026.

S8: Brandefense Blackhole extraction of Azerbaijan-associated cards seen in clear text in collected posts, 19 November 2026.

S9: Brandefense, Azerbaijan Cybersecurity Threat Landscape Report 2024–25, published 3 June 2025. https://brandefense.io/reports/azerbaijan-threat-landscape-report-2/. Verified on 23 November 2026. (landing page)

S10: APA, "Intensive cyberattacks targeting state information infrastructure reported in Azerbaijan", 14 October 2026 (since retitled), citing the State Service for Special Communication and Information Security. https://en.apa.az/ict/intensive-cyberattacks-targeting-state-information-infrastructure-reported-in-azerbaijan-529891. Verified on 21 November 2026.

S11: Azernews, "Cyberattacks target more than 100 government domains in Azerbaijan", 14 October 2026. https://www.azernews.az/nation/265520.html. Verified on 21 November 2026.

S12: Bitdefender, "FamousSparrow APT Targets Azerbaijani Oil and Gas Industry", 13 May 2026. https://www.bitdefender.com/en-gb/blog/businessinsights/famoussparrow-apt-targets-azerbaijani-oil-gas-industry. Verified on 21 November 2026.

S13: Trend News Agency, "Russian-linked APT29 behind recent cyberattacks on Azerbaijani media - official", 2 May 2025. https://www.trend.az/azerbaijan/politics/4038980.html. Verified on 21 November 2026.

S14: DataReportal (Kepios), Digital 2027: Azerbaijan, 5 November 2026 (data for October 2026). https://datareportal.com/reports/digital-2027-azerbaijan. Verified on 21 November 2026.

S15: APA, "Azerbaijan establishes National Cybersecurity Agency - DECREE", 2 June 2026. https://en.apa.az/official-news/azerbaijan-establishes-national-cybersecurity-agency-decree-509614. Verified on 21 November 2026.

S16: Ministry of Digital Development and Transport, "National Cybersecurity Agency established on the basis of the Electronic Security Service", 2 June 2026. https://mincom.gov.az/en/media-en/news/national-cybersecurity-agency-established-on-the-basis-of-the-electronic-security-service. Verified on 21 November 2026.

S17: JAMnews, "Azerbaijani government websites hit by cyberattack allegedly originating in Turkey", 14 October 2026. https://jam-news.net/azerbaijani-government-websites-hit-by-cyberattack-allegedly-originating-in-turkey/. Verified on 21 November 2026.

S18: Caspian Legal Center, "Liability in the Field of Cybersecurity: Amendments to the Code of Administrative Offences", 18 September 2026. https://www.caspianlegalcenter.az/news/more/cybersecurity-azerbaijan-penalties. Verified on 21 November 2026.

S19: APA, "Azerbaijan to introduce new cybersecurity rules for government institutions", 19 November 2026. https://en.apa.az/ict/azerbaijan-to-introduce-new-cybersecurity-rules-for-government-institutions-537090. Verified on 21 November 2026.

S20: OC Media, "Pro-Iran hackers claim responsibility for cyberattack on Azerbaijan, citing hijab ban", October 2026 (no exact date shown). https://oc-media.org/breaking-pro-iran-hackers-claim-responsibility-for-cyberattack-on-azerbaijan-citing-hijab-ban/. Verified on 21 November 2026.

S21: Law of the Republic of Azerbaijan amending the Code of Administrative Offences (Article 371-2), signed 14 July 2026, published 2 September 2026 (newspaper print 3 September). Official text as printed in the Azərbaycan newspaper: https://www.azerbaijan-news.az/az/posts/detail/azerbaycan-respublikasinin-inzibati-xetalar-mecellesinde-deyisiklik-edilmesi-haqqinda-1788397403/400592. Verified on 21 November 2026. The president.az copy was not reachable on 21 November 2026.

S22: President of the Republic of Azerbaijan, decree of 2 June 2026 establishing the National Cybersecurity Agency, and the agency's charter approved by the same decree. https://president.az/az/articles/view/72657 and https://president.az/az/articles/view/72658. Verified on 21 November 2026.

S23: APA, "Azərbaycan informasiya resurslarına qarşı DDoS hücumlarında kommersiya xidmətindən istifadə edilib" (Commercial service used in DDoS attacks on Azerbaijani information resources), 16 October 2026, citing the National Cybersecurity Agency. https://apa.az/ict/azerbaycan-informasiya-resurslarina-qarsi-ddos-hucumlarinda-kommersiya-xidmetinden-istifade-edilib-1005789. Verified on 21 November 2026.

S24: NETSCOUT ASERT, "Profiling DieNet: A New Hacktivist Threat", 5 May 2025 (data as of 28 April 2025). https://www.netscout.com/blog/asert/profiling-dienet-new-hacktivist-threat. Verified on 21 November 2026.

S25: Center for Internet Security, "Hacktivist Group DieNet Claims DDoS Attacks Against U.S. CNI", 16 April 2025. https://www.cisecurity.org/insights/blog/hacktivist-group-dienet-claims-ddos-attacks-against-u-s-c-n-i. Verified on 21 November 2026.

S26: Graphika, report on 313 Team's claimed disruption of a global e-commerce platform and its use of media attention (title names the platform), 30 April 2026. https://www.graphika.com/ (article URL withheld). Verified on 21 November 2026.

S27: Security Affairs, report on a 24-hour DDoS attack on a social-media platform claimed by a pro-Iran group (title names the platform), 21 April 2026. https://securityaffairs.com/191059/security/bluesky-hit-by-24-hour-ddos-attack-as-pro-iran-group-claims-responsibility.html. Verified on 21 November 2026.

S28: Palo Alto Networks Unit 42, "Threat Brief: Escalation of Cyber Risk Related to Iran", updated 17 April 2026. https://unit42.paloaltonetworks.com/iranian-cyberattacks-2026/. Verified on 21 November 2026.

S29: JAMnews, "Hybrid attacks on Armenia by two supposedly rival hacking groups", 16 April 2026. https://jam-news.net/hybrid-attacks-on-armenia-by-two-supposedly-rival-hacking-groups/. Verified on 21 November 2026.

S30: Dark Web Informer, post on an alleged breach of an Iranian chat platform offered by the xploitleaks handle (title names the platform), 13 January 2026. https://darkwebinformer.com/ (article URL withheld). Not reachable on 21 November 2026; the claim was checked in a dated repost.

S31: VECERT Analyzer, "Preventive alert" on an alleged offer of passenger data (post names the company), X, 11 November 2026. https://x.com/ (article URL withheld). Not reachable on 21 November 2026 (X refused automated access); the same alleged sale was reported as a claim by Siber Güvenlik Haber the same day.

S32: BeamSec, "3 APT Intrusions, 2 Database Leaks, and 1 New Cyber Department: Inside Azerbaijan's 2026 Threat Landscape", 9 September 2026. https://beamsec.com/3-apt-intrusions-2-database-leaks-and-1-new-cyber-department-inside-azerbaijans-2026-threat-landscape/. Verified on 21 November 2026.

S33: Report.az, "Azerbaijan's cybersecurity authority warns of large-scale Freshdesk phishing operation", 17 June 2026, citing the National Cybersecurity Agency. https://report.az/en/ict/azerbaijan-s-cybersecurity-authority-warns-of-large-scale-freshdesk-phishing-operation. Not reachable on 21 November 2026; worded as attributed reporting.

S34: JAMnews, report on the 15 November social-media link incident (title withheld), 17 November 2026. https://jam-news.net/?p=238581. Verified on 21 November 2026.

S35: Report.az, "Azerbaijan records 274 cyber attack indicators in early 2026", 7 April 2026, citing the State Service for Special Communication and Information Security. https://report.az/en/ict/azerbaijan-records-274-cyber-attack-indicators-in-early-2026. Not reachable on 21 November 2026; worded as attributed reporting.

S36: Report.az, "Azerbaijan records 518 cyberattack indicators in seven months", 10 August 2026, citing the same service. https://report.az/en/ict/azerbaijan-records-518-cyberattack-indicators-in-seven-months. Not reachable on 21 November 2026; worded as attributed reporting.

S37: Trend, "В Азербайджане выявлено более 134 тысяч случаев заражения ботнетами - Самеддин Асадов", 19 November 2026. https://ru.trend.az/azerbaijan/society/4248212.html. Verified on 21 November 2026. Also reported by Media.az the same day (https://media.az/politika/sameddin-asadov-rasskazal-o-masshtabah-kiberugroz-v-azerbajdzhane; not reachable on 21 November 2026).

S38: Operativ Məlumat Mərkəzi (operativmm.az), "Cyber-fraudsters detained in Azerbaijan for banking scams", 1 May 2026, citing the Interior Ministry. https://operativmm.az/en/post/cyber-fraudsters-detained-in-azerbaijan-for-banking-scams/71389. Verified on 23 November 2026.

S39: Operativ Məlumat Mərkəzi (operativmm.az), "Azerbaijani police arrest individual for cyber fraud scheme", 21 August 2026, citing the Interior Ministry. https://operativmm.az/en/post/azerbaijani-police-arrest-individual-for-cyber-fraud-scheme/77014. Verified on 23 November 2026.

S40: Operativ Məlumat Mərkəzi (operativmm.az), "Cyberpolice dismantle hacker network in Azerbaijan", 3 February 2026, citing the Interior Ministry. https://operativmm.az/en/post/cyberpolice-dismantle-hacker-network-in-azerbaijan/66761. Verified on 23 November 2026.

S41: ABC.az, "Attack on banking sector investigated", 6 February 2026, citing the Electronic Security Service. https://abc.az/en/news/195749/attack-on-banking-sector-investigated. Verified on 21 November 2026.

S42: Trend, "Azerbaijani authorities thwart cyberattack attempt", 27 February 2026, citing the Electronic Security Service. https://www.trend.az/azerbaijan/society/4158466.html. Verified on 21 November 2026.

S43: Government CERT (cert.gov.az), "Mass phishing attacks were conducted on behalf of government institutions", 8 April 2026. https://cert.gov.az/en/news/mass-phishing-attacks-were-conducted-on-behalf-of-government-institutions-9427. Verified on 21 November 2026.

S44: AzerNews, "Azerbaijan identifies cyber attack with Hungary's assistance", 10 April 2026. https://www.azernews.az/nation/256851.html. Verified on 21 November 2026.

S45: Trend, Interior Ministry statement on business-account intrusions, 22 July 2026 (first cited from Baku TV). https://az.trend.az/azerbaijan/society/4209083.html. Verified on 21 November 2026. The Baku TV item was not reachable on 21 November 2026.

S46: APA, "State Security Service: Illegal activities of international cybercriminal networks against Azerbaijan being prevented", 10 August 2026. https://en.apa.az/incident/state-security-service-illegal-activities-of-international-cybercriminal-networks-against-azerbaijan-being-prevented-519772. Verified on 21 November 2026.

S47: APA, "NCA: Cyberattack attempts recorded against user accounts of some organizations in Azerbaijan", 18 August 2026. https://en.apa.az/ict/nca-cyberattack-attempts-recorded-against-user-accounts-of-some-organizations-in-azerbaijan-520797. Verified on 21 November 2026.

S48: Caliber.Az, "Azerbaijan detects TikTok accounts impersonating payment systems", 14 September 2026. https://caliber.az/en/post/azerbaijan-detects-tiktok-accounts-impersonating-payment-systems. Verified on 21 November 2026.

S49: Azernews, "Iran-linked group claims responsibility for large-scale cyberattacks on Azerbaijani government websites", 15 October 2026. https://www.azernews.az/events/265618.html. Verified on 21 November 2026.

S50: Trend, "Azerbaijan blocks hundreds of major cyberattacks, official says", 4 June 2026. https://www.trend.az/azerbaijan/society/4194332.html. Verified on 21 November 2026.

S51: NIST National Vulnerability Database, CVE-2022-41040 and CVE-2022-41082. https://nvd.nist.gov/vuln/detail/CVE-2022-41040 and https://nvd.nist.gov/vuln/detail/CVE-2022-41082. Verified on 21 November 2026.

S52: Microsoft Security Response Center, security update guides for CVE-2022-41040 and CVE-2022-41082. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41040 and https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41082. Listed as the vendor references in NVD on 21 November 2026.

S53: CISA, "Implementing Number Matching in MFA Applications" (fact sheet), October 2022. https://www.cisa.gov/sites/default/files/publications/fact-sheet-implement-number-matching-in-mfa-applications-508c.pdf. Verified on 21 November 2026.

S54: State Service for Special Communication and Information Security, "XRITDX blocked over 1 million malicious emails in 7 months", 11 August 2025. https://scis.gov.az/en/news/view/287/xritdx-blocked-over-1-million-malicious-emails-in-7-months. Verified on 23 November 2026.

S55: Government CERT (cert.gov.az), "Azerbaijan Government CERT investigates cyberattack activities targeting Azerbaijan's energy sector by China-linked APT group", 15 May 2026. https://www.cert.gov.az/en/news/azerbaijan-government-cert-investigates-cyberattack-activities-azerbaijans-energy-sector-by-china-linked-apt-group-9702. Verified on 23 November 2026.

S56: Report.az, "Azərbaycanda bu il qeydə alınmış kiberhücumların sayı açıqlanıb", 19 November 2026, citing Deputy Minister Sameddin Asadov. https://report.az/amp/ikt/azerbaycanda-bu-il-qeyde-alinmis-kiberhucumlarin-sayi-aciqlanib. Verified on 23 November 2026.

S57: Report.az, "Azerbaijani official warns of supply-chain cyberattacks on state bodies", 4 June 2026, citing the State Service for Special Communication and Information Security. https://api.report.az/en/ict/azerbaijani-official-warns-of-supply-chain-cyberattacks-on-state-bodies. Verified on 23 November 2026.

Appendix D. Glossary

- **Blackhole:** Brandefense's cybercrime data source covering posts, infected devices, credentials and card material.
- **Ransompedia:** Brandefense's ransomware database; listings record criminal claims.
- **Atlas:** Brandefense's external exposure scoring; scores run from 0 (nothing observed) to 100.
- **Infected device:** a device whose stealer log contains a login to the organisation's domain; "employee" is a classification from usage, not verified employment.
- **Credential-market listing:** a credential tied to the domain offered on a monitored market at the time of the check.
- **Combolist:** a list of login and password pairs assembled from various sources; age and validity vary.
- **Stealer log:** data captured by information-stealing malware from a device.
- **Checker bot:** a bot that tests stolen cards against payment gateways and prints the result.
- **Post card:** a redacted reproduction of one dark-web post, with venue, date, alias, language and what it does and does not establish.
- **Relay:** a third-party channel or bot that reposts another actor's claim; a relay is weaker evidence than the actor's own post.
- **DMARC / SPF / DKIM:** email-authentication standards; DMARC tells receivers what to do with mail that fails.
- **DNSSEC:** signatures that let resolvers verify DNS answers.
- **TLP:CLEAR:** may be shared without restriction; other legal duties still apply.
- **AiTM (adversary-in-the-middle):** a phishing page that relays a real login and captures passwords, one-time codes and the session cookie, so the attacker can sign in without the second factor again.
- **BIN:** the issuer's card-number prefix (bank identification number).
- **C2:** command and control, the infrastructure an attacker uses to direct malware.
- **DS record:** the record in the parent zone that links a domain to its DNSSEC keys.
- **EDR:** endpoint detection and response, security software that records and flags activity on devices.
- **Drops and mule accounts:** people, and accounts opened in their names, used to receive and move fraud proceeds.
- **Headline score:** the national Atlas figure for all 250 organisations (48 out of 100).
- **HSTS:** a web header telling browsers to use HTTPS only.
- **KYC:** "know your customer" identity checks at banks, exchanges and other services.
- **Legacy authentication:** older mail sign-in protocols that cannot enforce MFA.
- **Lookup bot:** a Telegram bot that returns personal data for a name, number or ID.
- **MFA (multi-factor authentication):** a sign-in that needs a second factor beyond the password.

- **Number matching:** the user types a number shown on the sign-in screen into the authenticator app; it stops blind approvals but not an AiTM relay.
- **OT / SCADA:** operational technology and the supervisory control systems that run physical processes.
- **p=none:** a DMARC policy that only monitors and does not ask receivers to reject or quarantine.
- **Passive hygiene index:** an Odin analytical composite of email, DNS, TLS and header checks; 0-100, higher means weaker.
- **Phishing-resistant MFA:** sign-in tied to the real site (FIDO2 security keys, passkeys or certificates), so a relay page cannot reuse it.
- **RAT:** remote-access trojan, malware that gives an attacker remote control of a device.
- **RDP:** Remote Desktop Protocol, used to control a Windows computer over the network.
- **Stresser:** a DDoS-for-hire service, often sold as a "stress test".
- **Telegram Stars:** Telegram's in-app currency, used by some sellers as payment.

About this report

Prepared by Odin by Brandefense. Version 1.0 was completed on 19 November 2026. Version 1.1 (20 November 2026) redesigned the layout, added post and actor cards with public reporting, and narrowed the card section. Version 1.2 (21 November 2026, revised 23 November 2026) closes five independent review rounds. It describes victims generically, recounts the SPF results and gives an address (or site root where victim names are withheld) and verification date for each external source. It also adds a guide to Atlas ratings, decision targets and a legal applicability table.

Research cutoff: 18 November 2026 (primary data window); a blind audit on 20 November 2026 added officially reported and press-reported items (Appendix A.8). The report prioritises Brandefense's own data, keeps criminal claims separate from independently established incidents and does not claim a complete census of cybercrime affecting Azerbaijan. Recommendations describe what organisations could do; they do not state that any organisation has or has not done them. An Azerbaijani-language edition of version 1.2 accompanies this report.

© 2026 Brandefense. All rights reserved.

ABOUT BRANDEFENSE

Attackers See You First. We make sure you do.

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

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

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

GARTNER PEER INSIGHTS
4.7 / 5

COVERAGE
3 pillars
CTI, DRPS, EASM

MONITORING
24 / 7
Open, deep and dark web

REQUEST A DEMO

Request A Demo. See what attackers see.

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

Request a demo →

AWARDS

Recognised Around The World. Technology and trust.

Selected awards recognising Brandefense technology and innovation.



Top InfoSec Innovator

2026



Deloitte Technology Fast 500 EMEA

2024



Global InfoSec Awards

2025



Cybersecurity Excellence Awards

2025

See Brandefense In Action.

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

Request a demo →

BRANDEFENSE

See what attackers see. Before they act.

UNITED STATES

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

TÜRKIYE

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

BRANDEFENSE.IO