COUNTRY REPORT · BRANDEFENSE COUNTRY REPORT · QATAR 2026 · TLP:CLEAR · 77 MIN READ

Brandefense Qatar Cyber Threat Landscape Report 2026

Identity exposure, data claims and a hacktivist burst in a connected energy and aviation hub

BY	PUBLISHED	READING TIME	EDITION	RESEARCH WINDOW
Odin by Brandefense	21 November 2026	77 min read	Version 1.0 · Public Research Edition · TLP:CLEAR	1 January-20 November 2026

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

7,867-8,175
cleaned posts remain from 55,241 tagged posts

31,836
DDoS attacks on Qatar measured by NETSCOUT in January-June 2026

9 of 9
card-issuing banks on our list with a current credential listing, the first item to triage

CONTENTS

01	Executive summary		Report map
02	Qatar's digital and strategic context	03	National exposure: 250 leading organisations
04	What we see on the dark web	05	Targeting examples by sector
06	Hacktivism and DDoS	07	Threat actors
08	The fraud economy	09	Banking and finance deep dive
10	Regulatory and national response	11	Outlook
12	Action plan	A	Appendix A. Method
B	Appendix B. Evidence register	C	Appendix C. Sources
D	Appendix D. Glossary		About this report

CHAPTER 1

Executive summary

THIS CHAPTER ANSWERS

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

4

decisions for leaders, each tied to evidence in the chapters

INSIDE THIS CHAPTER

Four decisions for leaders | The year in numbers

IN SHORT

For the 250 selected organisations, one primary domain each (68 linked provisionally), the main measured exposure is identity: infected-device and credential associations, and credentials listed for sale. The most visible activity was a March burst of hacktivist DDoS claims that no authority confirmed as an outage. Vendors documented espionage attempts against government and energy, and Citizen Lab found Al Jazeera devices targeted and infected with spyware. Act in this order: validate every credential-listing alert; harden mail and attachment handling; then pre-agree DDoS statements and reporting roles.

This report combines three of Brandefense's own data sources with verified public reporting. **Brandefense Blackhole** supplied 55,241 posts tagged as concerning Qatar and further posts mentioning Qatar or Qatari organisations, 74,809 distinct posts in all. 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 Qatar and four Gulf comparators. **Atlas** exposure ratings were computed for the 250 organisations, through one primary domain each; for 68 of these domains, ownership is not independently confirmed. These are separate populations and are never added together.

1. Identity exposure is the most widespread measured risk. 182 of the 250 organisations have infected devices associated with their domains (115,683 in total), and 213 have historical credential records (420,122 records). These counts are all records held on 21 November 2026, whatever their capture date: they are cumulative, not 2026-only. They can involve staff, students, patients or customers. These are association counts: whether any login or session is still usable, and who it belongs to, requires validation. [S1][S3]

2. Credentials listed for sale are the first signal to triage. 73 of 250 organisations had a credential linked to their domain listed for sale when checked, on credential markets that Brandefense monitors. The 250-organisation Atlas headline is 46 out of 100; a higher value means more exposure signals were observed, and a low value does not mean strong controls. All nine card-issuing banks on our list had such a listing. A listing tells a defender to look for an active account; it does not say how many accounts or whose. [S4]

3. A burst of hacktivist DDoS claims followed the regional escalation; no outage was confirmed. Between 28 February and 25 March four groups claimed DDoS against government portals, ministries, a public-service billing and payment portal, a financial regulator and an energy-sector site. We found no statement from a Qatari authority or a named organisation confirming an outage. NETSCOUT measured 31,836 DDoS attacks on Qatar in January-June and classed most targets as wired telecom carriers; its data does not show whether the sites the groups named were hit. [S2][S29][S32]

4. Espionage attempts were documented, and a broadcaster's devices were confirmed infected with spyware. Check Point reported that China-nexus Camaro Dragon tried to deploy PlugX against Qatari targets within a day of the escalation, using lures about the escalation. It assessed a second campaign, with low confidence, as China-aligned; its weekly summary said the campaigns targeted government and energy-related entities. Neither appeared in the leak-site and forum data we searched. Separately, Citizen Lab reported in October 2026 that at least 45 Al Jazeera devices were targeted with Candiru spyware in 2024 and 2025, and that devices were infected (§7.2). [S26][S27][S47][S48]

5. Data claims named energy, banking, security and education bodies; none was confirmed. Two posters claimed the same energy-sector company in February and March (Case A). Sellers offered personnel data of a government security body (Case B) and customer records attributed to a large bank (Case C). Ransompedia holds nine 2026 listings for Qatar, naming eight organisations, mostly contractors, consultancies and infrastructure suppliers. [S1][S6]

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 on evidence of usable stolen authentication material, session abuse or unauthorised access, whether or not multi-factor authentication (MFA) is enabled. Record MFA status as one factor in the investigation. 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. **Close the attachment route that espionage used.** The 2026 campaigns were built around archives and shortcut files that a user had to open, then legitimate programs loading malicious libraries. Block archive and shortcut attachments from outside, and alert on signed binaries loading DLLs from user folders (§7.2).
3. **Prepare for hacktivist claims that outrun the facts.** Agree in advance who confirms service status publicly during a DDoS burst, and pre-arrange upstream mitigation for citizen-facing portals and payment pages. In March, claims circulated for weeks without any official statement on outages.
4. **Name one person for every reporting clock.** Privacy guidance sets 72 hours for a serious personal-data breach. The national standard and the 2026 risk frameworks also set reporting duties whose deadlines we could not confirm; obtain written clarification from NCSA. Name the reporter and a deputy now (§10.3).

The year in numbers

9

Ransompedia accepted ransomware listings for Qatar dated 1 Jan-20 Nov 2026, naming 8 organisations (24 all-time)

WHAT IT IS NOT

Not a count of confirmed intrusions; unlisted and unpublished cases are invisible

55,241

Blackhole posts tagged as concerning Qatar, 1 Jan-20 Nov 2026

WHAT IT IS NOT

Not a count of attacks; 78% fall in October and are mostly automated Turkish-language recruitment posts

7,867-8,175

tagged posts left once spam and automated posts are set aside

WHAT IT IS NOT

Not unique incidents; many are multi-country lists or concern other countries, so the range is an upper bound

31,836

DDoS attacks on Qatar measured by NETSCOUT, January-June 2026

WHAT IT IS NOT

Not hacktivist attacks specifically; most targets classed as telecom carriers

250

leading public and private organisations assessed with Atlas ratings, one primary domain each (68 linked provisionally)

WHAT IT IS NOT

Not a random sample; not a national prevalence estimate

115,683

infected devices associated with those 250 domains (4,191 classified as employee devices); cumulative, all records held on 21 Nov 2026

WHAT IT IS NOT

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

420,122

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

73 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

110

distinct Qatar-associated payment cards seen in clear text in collected dark-web posts (85 attributed to a named Qatari bank, 25 labelled only as Qatari)

WHAT IT IS NOT

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

50%

of the 250 organisations enforcing DMARC (124)

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?

GO TO 1 3 12

CISO and security leads

Which exposures are ours, which actors matter, and which controls come first?

GO TO 3 6 7 9 10 12

SOC and threat intelligence

What did the actors post, how are they connected, and which techniques did espionage use?

GO TO 4 6 7 8 12 App. A-B

Fraud and customer protection

How are Qatari identities, accounts and cards traded, and where do banks see it?

GO TO 4 5 8 9

Communications and legal

How do we speak about unverified claims, and which reporting clocks apply?

GO TO 6 10 12

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

02 **Context**
Which features of Qatar shape the threats

03 **National exposure**
How exposed 250 leading organisations are, measured with Atlas ratings

04 **Dark web**
What criminals post about Qatar once spam is removed

05 **Sectors**
Which sectors are named and what response each needs

06 **Hacktivism**
What was claimed, what was measured, 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**
Which reporting clocks apply and what to do now

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

12 **Action plan**
Who does what in 90 days

CHAPTER 2

Qatar's digital and strategic context

THIS CHAPTER ANSWERS

Which features of Qatar shape the cyber threats in this report, and why did 2026 look different from earlier years?

98.1%

internet penetration in October 2026, with 4.71 million cellular connections

INSIDE THIS CHAPTER

2.1 Connected and mobile-first
2.2 Energy, aviation and finance attract espionage
2.3 A digitised, centralised service model
2.4 The March 2026 escalation and the hacktivist burst
2.5 A national cyber authority with new 2026 frameworks

IN SHORT

Four features shape Qatar's threat picture. Connectivity is near-universal; a global energy and aviation role attracts espionage; services are highly digitised and centralised; and in 2026 a regional military escalation brought a burst of hacktivist claims. Each needs a different control. Assign owners to identity monitoring, attachment controls, upstream mitigation and service-status communications.

2.1 Connected and mobile-first

Qatar had about 3.19 million inhabitants and 3.13 million internet users in October 2026, a penetration of 98.1%. It had 4.71 million cellular connections (148% of the population) and 3.29 million social-media user identities [S9]. In August the Communications Regulatory Authority reported a score of 98.4 out of 100 in the ITU ICT Development Index 2026, sixth of 159 economies, with 99% 5G and 100% fibre population coverage [S10].

That level of connectivity matters for defenders in two ways. Almost every resident and visitor can be reached by SMS, messaging and email lures. And the device population that information-stealing malware can infect is large relative to the population, which is why identity exposure dominates Chapter 3.

2.2 Energy, aviation and finance attract espionage

Qatar was the second-largest liquefied natural gas (LNG) exporter in 2024, with nearly 20% of global LNG exports, according to the US Energy Information Administration [S11]. Hamad International Airport handled 54.3 million passengers in 2025 [S12]. Banks, insurers and the Qatar Financial Centre serve a regional market.

Organisations in these sectors hold information that espionage operators value: contracts, pricing, partners and travel. The documented 2026 espionage activity in our sources fits that pattern. Check Point described two campaigns against Qatari targets in early March; its weekly summary said the campaigns targeted government and energy-related entities (Chapter 7) [S26][S27]. In October 2026 Citizen Lab reported that at least 45 Al Jazeera devices were targeted with Candiru spyware in 2024 and 2025, and that devices were infected [S48][S47].

2.3 A digitised, centralised service model

Government, payments and identity run through a small number of national platforms. Qatar Central Bank operates the Fawran instant-payment system, launched in 2024, and the QPAY e-commerce gateway [S13]. Two global cloud providers run regions in Doha [S42], and QCB has issued a Cloud Computing Regulation for the entities it licenses (Chapter 10) [S23].

Central platforms are efficient, and they also concentrate value. Fraudsters imitate them because residents trust them. In 2026 the Ministry of Interior, the General Tax Authority and the National Cyber Security Agency each warned the public about messages impersonating government bodies (Chapter 8) [S35][S36][S45].

2.4 The March 2026 escalation and the hacktivist burst

From 28 February 2026 a military escalation in the region was followed, in vendor reporting, by a surge of hacktivist DDoS claims across the Gulf [S29][S30]. Intel 471 placed Qatar among the ten most claimed-against locations in the first week [S30]. NETSCOUT recorded 31,836 DDoS attacks on Qatar in January-June 2026 [S32], and StormWall reported that DDoS attacks on Qatar rose 75% year on year in the first quarter [S31].

We describe the escalation only as context for the security data. This report takes no position on the conflict, on any government involved or on Qatar's foreign relations. Claims by hacktivists are reported as their claims (Chapter 6).

2.5 A national cyber authority with new 2026 frameworks

The National Cyber Security Agency (NCSA), established in 2021, sets the national strategy and standards and acts as the personal-data privacy regulator [S14][S21]. In October 2026 it launched national and enterprise risk management frameworks [S18]. Its public advisory feed is busy: we counted more than 160 security advisories on its site between January and 20 November 2026, 65 of which mention active exploitation or a zero-day [S43]. Chapter 10 sets out what changed for organisations.

KEY TAKEAWAYS

01

Near-universal connectivity makes identity theft and impersonation the default criminal route.

02

Energy, aviation and government attract espionage that does not show up in criminal markets.

03

The March escalation brought a burst of hacktivist claims; treat it as a planning signal, not a trend line.

CHAPTER 3

National exposure: 250 leading organisations

THIS CHAPTER ANSWERS

How exposed are the country's 250 leading public and private organisations when measured with Brandefense Atlas ratings, and which signal should they triage first?

73 of 250

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

INSIDE THIS CHAPTER

3.1 Universe card | 3.2 Atlas headline and listings by sector | 3.3 Devices and credentials | 3.4 Current credential listings: the first signal to triage | 3.5 Lookalike domains, exposed documents and mentions | 3.6 Email and web hygiene

IN SHORT

We assessed 250 leading Qatari organisations, one primary domain each, using Brandefense Atlas exposure ratings; for 68 the domain's ownership is not independently confirmed. Seven in ten have infected devices associated with their domains, more than eight in ten have historical credential records, and almost three in ten had a credential listed for sale when we checked. Email and web hygiene is uneven: half enforce DMARC, and we observed DNSSEC delegation records for only 6 of 250 domains. Triage current listings first, then employee devices.

3.1 Universe card

Item	Definition
Population	250 organisations: 52 government bodies, 30 banking and finance, 29 retail and holding groups, 24 media, sports and culture, 23 education and research, 19 energy and utilities, 18 manufacturing and industry, 14 transport and logistics, 12 hospitality and tourism, 11 healthcare, 9 insurance, 9 telecom. 128 state-owned, 117 private, 5 foreign or joint
Selection	Purposive: state bodies and national portals, licensed banks and market infrastructure, state-owned enterprises, listed companies and market leaders. Selected for size or systemic role, not ranked by revenue; no published Qatari top-250 ranking was used
Unit	One primary domain per organisation. All 250 resolve in DNS (21 November 2026). For the 182 domains whose homepage could be checked, it matched the organisation. For the other 68 the link to the organisation is provisional: ownership is not independently confirmed, and their results are attributed with that caveat
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	Device, credential and listing counts read 21 November 2026; they 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 19 October–18 November 2026
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 Atlas headline and listings by sector

Atlas rates each organisation from 0 (no risk observed) to 100 from signals including infected devices, employee devices, third-party breach records, dark-chat mentions, dark-web mentions, lookalike domains, exposed documents and data sales.

How to read Atlas ratings.

Term	Meaning
Headline	Atlas's summary score for the country (all 250 organisations); it is not an average
Current listing	A credential tied to the domain on sale at the time of the check

Credentials and infected devices are common in most sectors

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
Media, sports and culture (24)	88%	71%	92%	50%	46%	75%	46%
Healthcare (11)	73%	64%	82%	45%	9%	27%	45%
Telecom (9)	89%	89%	89%	44%	22%	67%	56%
Transport and logistics (14)	86%	64%	86%	43%	36%	57%	50%
Banking and finance (30)	60%	30%	70%	40%	23%	60%	40%
Energy and utilities (19)	58%	58%	84%	32%	16%	53%	37%
Education and research (23)	91%	87%	100%	26%	13%	65%	39%
Government (52)	92%	73%	94%	25%	19%	83%	42%
Retail and holdings (29)	69%	66%	90%	24%	3%	48%	48%
Insurance (9)	44%	33%	67%	11%	11%	56%	22%
Manufacturing and industry (18)	39%	33%	67%	6%	6%	39%	33%
Hospitality and tourism (12)	33%	8%	75%	0%	0%	17%	25%

Source: Brandefense Blackhole associations and Atlas ratings for 250 organisations, read 21 November 2026 [S3][S4]. Records are cumulative, not 2026-only.

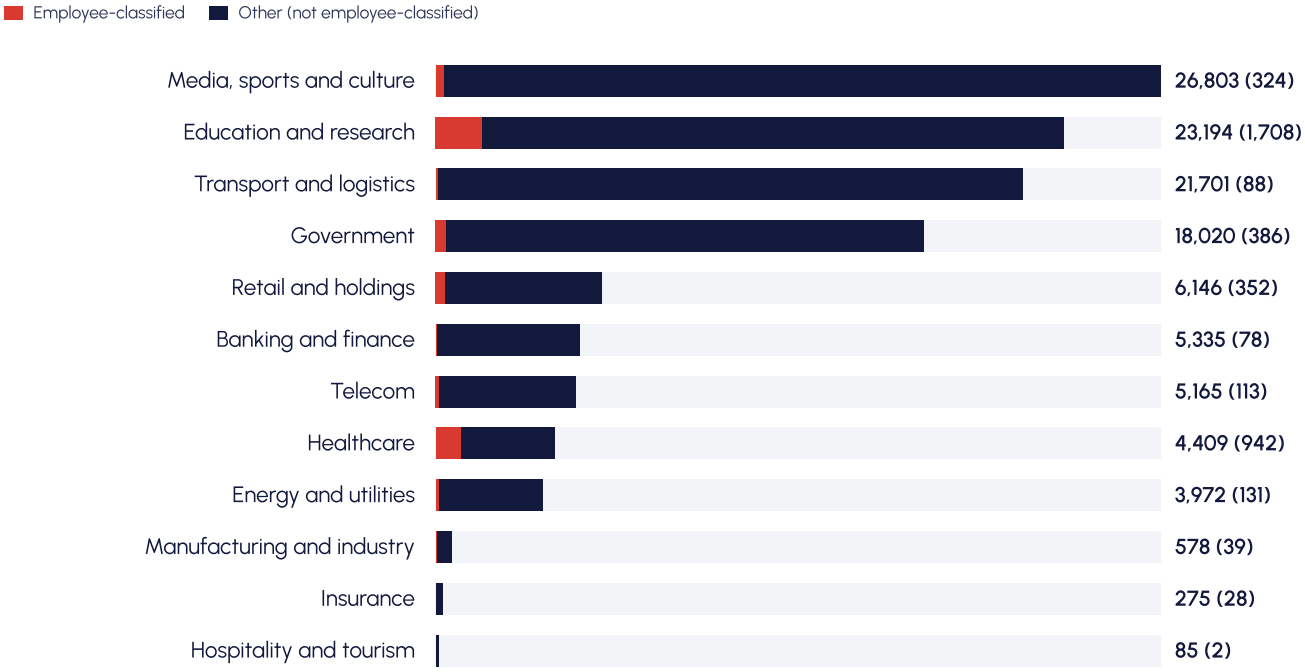
Sector	Orgs	Orgs with a current credential listing
Government	52	13
Banking and finance	30	12
Retail and holdings	29	7
Media, sports and culture	24	12
Education and research	23	6
Energy and utilities	19	6
Manufacturing and industry	18	1

Sector	Orgs	Orgs with a current credential listing
Transport and logistics	14	6
Hospitality and tourism	12	0
Healthcare	11	5
Insurance	9	1
Telecom	9	4
All 250	250	73

Reading the table. Counts describe this list, not each sector nationally. The national Atlas headline for all 250 organisations is 46 out of 100. A higher headline means more exposure signals were observed; a low headline means few signals were observed, not that controls are strong (see §3.6).

3.3 Devices and credentials

Media, education and transport carry the most infected-device associations; education and healthcare hold most employee-classified devices



Source: Brandefense Blackhole associations and Atlas ratings for 250 organisations, read 21 November 2026 [S3][S4]. Records are cumulative, not 2026-only.

Sector	Orgs with infected devices	Devices (employee)	Credential records	Share of credential records held by the two largest organisati
Media, sports and culture	21 of 24	26,803 (324)	36,274	
Education and research	21 of 23	23,194 (1,708)	192,723	

Sector	Orgs with infected devices	Devices (employee)	Credential records	Share of credential records held by the two largest organisati
Transport and logistics	12 of 14	21,701 (88)	22,321	
Governme nt	48 of 52	18,020 (386)	25,502	
Retail and holdings	20 of 29	6,146 (352)	24,271	
Banking and finance	18 of 30	5,335 (78)	15,049	
Telecom	8 of 9	5,165 (113)	10,165	
Healthcare	8 of 11	4,409 (942)	74,475	
Energy and utilities	11 of 19	3,972 (131)	10,002	
Manufactu ring and industry	7 of 18	578 (39)	7,391	
Insurance	4 of 9	275 (28)	1,149	
Hospitality and tourism	4 of 12	85 (2)	800	
All	**182 of 250**	**115,683 (4,191)**	**420,122**	

Credential records split into 116,273 breach-database records, 118,099 stealer-log lines and 185,750 combolist entries. The infected devices hold about 1.98 million captured credentials in total, for all services, not only the organisation's own.

What this means.

- **Most device associations sit outside the employee classification.** 111,492 of the 115,683 devices are not employee-classified. Their stealer logs include a login to the organisation's site, so they are most plausibly customers' or visitors' own computers, though ownership is not established. These associations are a fraud and account-hijacking signal and do not by themselves establish an intrusion. The 4,191 employee-classified devices are the intrusion-relevant subset; both groups require validation.
- **Universities and hospitals hold the employee-device problem.** Education has 1,708 employee-classified devices, 41% of the national total in our list, and the largest credential count. Healthcare has 942. In both sectors staff, students and patients can share domains, so "employee" may include them.
- **Concentration varies.** In healthcare, two organisations hold 89% of credential records; in government the two largest hold 24%. A sector total is therefore a poor guide to a typical organisation.
- **The median organisation is modest.** The median organisation has 9 infected devices and 196 credential records. The heaviest single organisations carry thousands of devices or tens of thousands of credential records.

3.4 Current credential listings: the first signal to triage

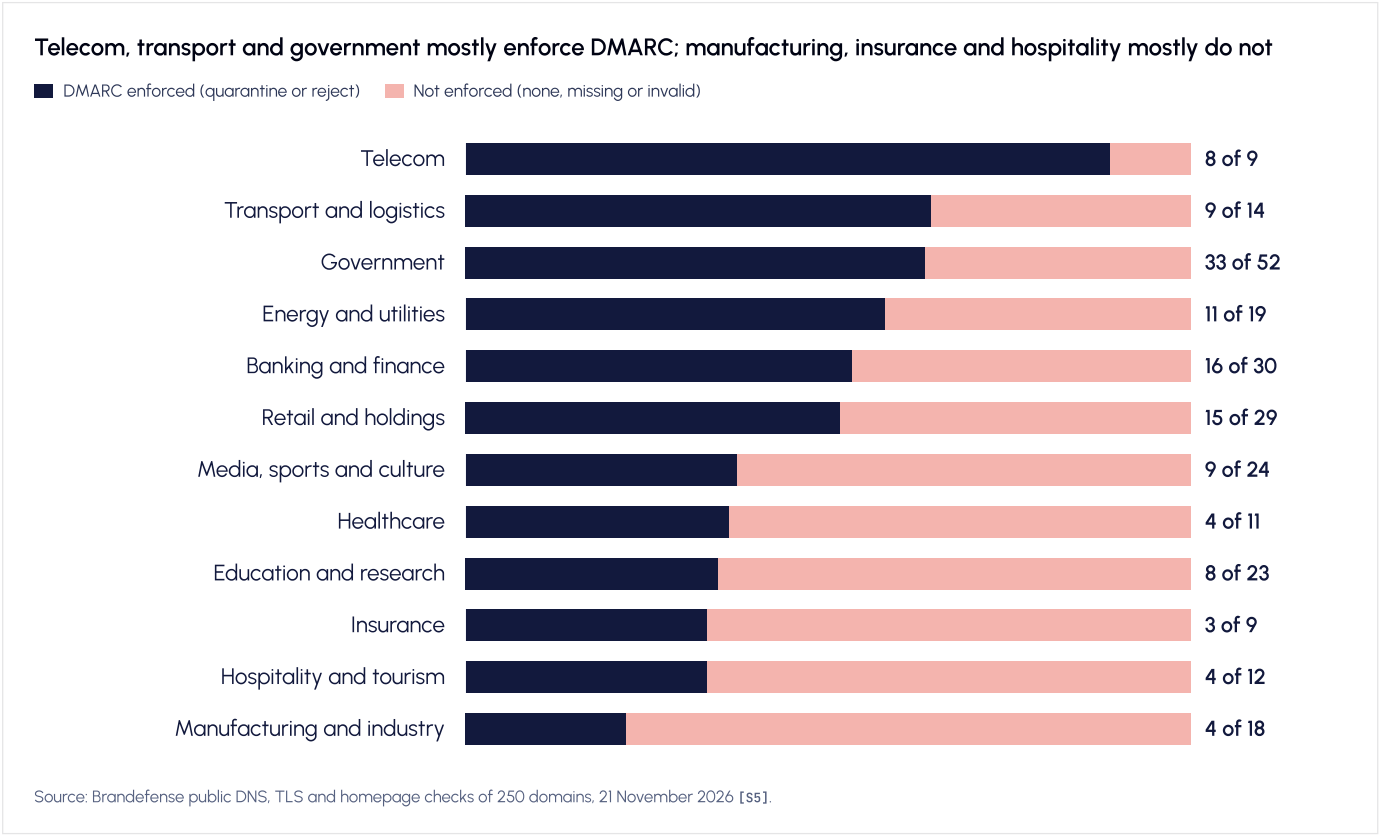
73 of 250 organisations had at least one credential tied to their domain listed on a monitored credential market at the time of the check. Of those 73, 45 also have a listing history.

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 what validation must establish. 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:** Lookalike domains newly observed in the 30 days to 18 November were found for 149 organisations. Lookalikes are candidates, not confirmed phishing sites.
- **Exposed documents:** 103 organisations have at least one exposed document that references their domain (359 in total).
- **Mentions:** 41 organisations were mentioned in dark-chat sources in the last 365 days and 17 in dark-web (onion) sources. Counts are small; the highest for any single organisation is 36. Mention counts measure visibility, not hostility.

3.6 Email and web hygiene



Source: Brandefense public DNS, TLS and homepage checks of 250 domains, 21 November 2026 [S5].

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

Control	Result (of 250 unless stated)	Reading
DMARC reject	47	Spoofed mail from the domain should be refused
DMARC quarantine	77	Spoofed mail should go to spam
DMARC p=none or missing	126 (57 none, 69 missing)	No enforcement; spoofing the domain is easier
SPF ending -all / ~all / ?all / other / none	154 / 52 / 1 / 4 / 39	39 domains publish no SPF policy
DKIM observed	147	Not observing DKIM is not proof that it is absent

Control	Result (of 250 unless stated)	Reading
DS record observed (DNSSEC delegation)	6	No DS record observed for 244 domains; a DS record alone does not prove a valid chain of trust
TLS certificate invalid	23 of 220 assessed (30 not assessed)	Expired, mismatched or untrusted certificates found
HSTS on homepage	93 of 182 reachable	Many sites do not force HTTPS for returning visitors
Mail provider	107 Microsoft 365, 10 Google, 37 no MX	The rest run their own or regional mail

Homepage checks were unavailable for 68 sites and TLS checks for 30. DNS checks are complete for all 250 domains.

Telecom and transport lead; manufacturing lags. 8 of 9 telecom organisations enforce DMARC, as do 9 of 14 transport and 33 of 52 government bodies. Manufacturing (4 of 18), insurance (3 of 9) and hospitality (4 of 12) enforce least; education (8 of 23), healthcare (4 of 11) and media (9 of 24) are close behind. Banking sits in the middle at 16 of 30. On the passive hygiene index (Appendix A.5; 0-100, higher is weaker), manufacturing and education (56 each) have the weakest sector index values and telecom (34) the strongest.

DNS signing is almost absent. Only 6 of 250 primary domains show a DNSSEC delegation record. That leaves DNS answers for national portals, banks and energy companies unauthenticated for resolvers that validate.

KEY TAKEAWAYS

01

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

02

73 of 250 organisations had a credential listed for sale when checked; listings are the first item to triage.

03

Half of the domains do not enforce DMARC and only 6 of 250 publish DNSSEC delegation.

CHAPTER 4

What we see on the dark web

THIS CHAPTER ANSWERS

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

7,867-8,175

cleaned posts remain from 55,241 tagged posts

INSIDE THIS CHAPTER

4.1 Universe card | 4.2 Platforms, languages and volume | 4.3 Crime families after cleaning | 4.4 Specific claims against Qatari organisations | 4.5 Case studies | 4.6 What the forums add

IN SHORT

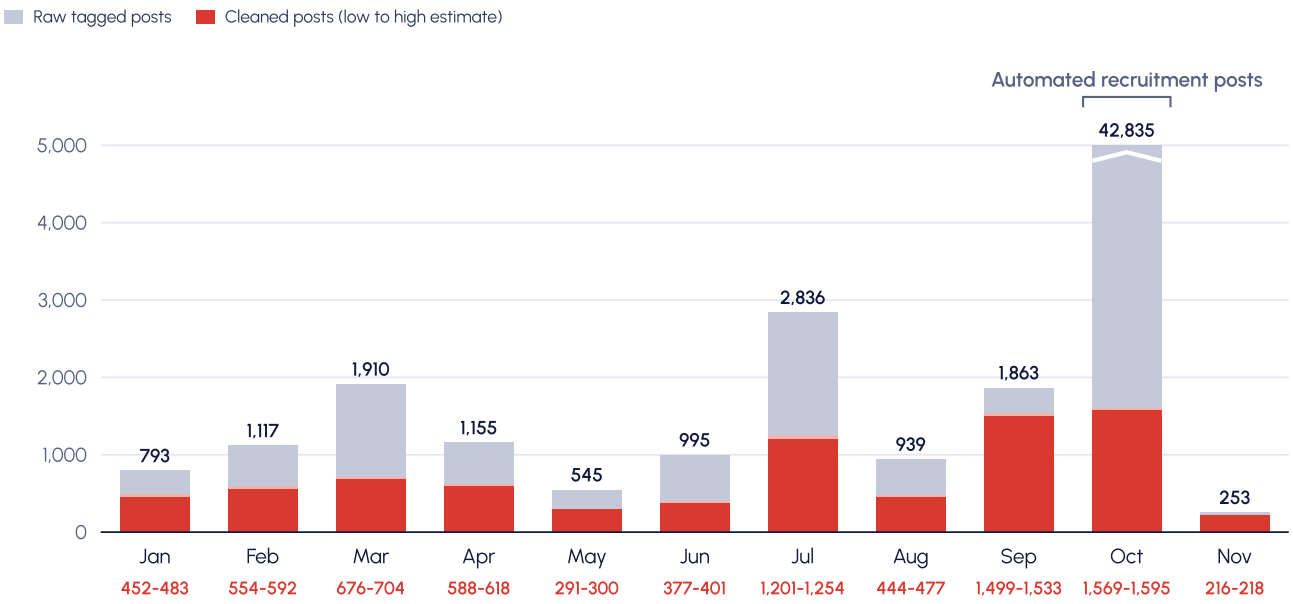
Most Qatar-tagged underground traffic is bulk advertising, and automated Turkish-language recruitment posts alone made up 41,000 posts in October. After cleaning, about 8,000 posts remain. Qatar appears mostly as one market among many in carding, identity and account-trading channels. A small number of posts make specific claims against Qatari energy, banking, security, education and public-sector bodies. Triage each claim by provenance, sample and age before anyone speaks of a breach.

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	Posts tagged as concerning Qatar ("this post is about, targets or mentions Qatar"), plus posts that mention Qatar or Qatari organisations
Window	Post time 1 January-20 November 2026 (November partial). Collection time is never used
Tagged set	55,241 posts
Combined corpus	74,809 distinct posts tagged as or mentioning Qatar
Cleaned set	Posts left once spam and automated posts are set aside (Appendix A.2)
Not established	That a tagged post targets Qatar, that a claim is true, or that two posts concern the same file

4.2 Platforms, languages and volume

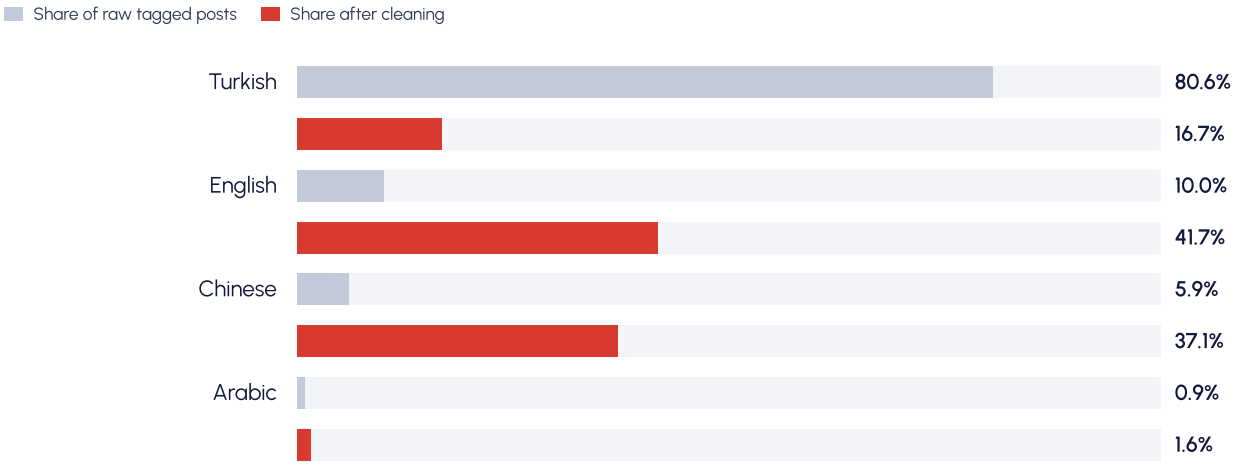
Automated October posts inflate the raw count; cleaned volume stays between 291 and 1,595 posts in every complete month



Source: Brandefense Blackhole, posts tagged as concerning Qatar, post dates 1 January–20 November 2026, November partial [S1]. Cleaned counts are an upper bound.

Measure	Value
Telegram share of tagged posts	99.7% (55,095)
Forum posts	90 (plus 334 further forum posts mentioning Qatar)
Paste, Discord, onion sites	23, 33, 0
Turkish / English / Chinese / Russian / Arabic	80.6% / 10.0% / 5.9% / 1.4% / 0.9% of raw posts
After cleaning: English / Chinese / Turkish / Arabic	41.7% / 37.1% / 16.7% / 1.6%
Raw posts per month	42,835 in October; 253–2,836 in other months

Turkish dominates the raw tag; after cleaning, English and Chinese posts carry most of the weight



Telegram carries 99.7% of tagged posts. Source: Brandefense Blackhole, posts tagged as concerning Qatar, post dates 1 January-20 November 2026, November partial [S1]. Cleaned counts are an upper bound.

The October spike is not an attack wave. 78% of the year's tagged posts fall in October, and 41,438 of them are in Turkish. They are automated recruitment adverts for Turkish bank accounts, posted to hundreds of chats and tagged to Qatar. After spam and automated posts are set aside, October holds 1,569-1,595 cleaned posts, in line with July and September.

Collection appears lower from mid-year. Tagged volume for Türkiye also falls sharply between May and July. We do not read declines from mid-year as threat trends.

Arabic is almost absent. Arabic posts make up under 2% of the cleaned corpus. Qatar-relevant criminal trade in our collection happens mostly in English and Chinese, in channels that serve many countries. Closed Arabic-language groups are outside our collection (Appendix A.8).

4.3 Crime families after cleaning

Carding and data-leak posts lead the cleaned corpus; account trading, phishing and identity services follow



Source: Brandefense Blackhole, posts tagged as concerning Qatar, post dates 1 January-20 November 2026, November partial [S1]. Cleaned counts are an upper bound.

Family	Cleaned posts (low-high)	What it contains
Carding	2,885-2,919	Card-shop updates listing Qatar among dozens of countries, checker outputs naming Qatari issuers, buyers of "Middle East" cards
Data leaks and databases	2,346-2,374	Card-shop "bases", Gulf lead lists, database offers naming Qatari organisations
Bank and payment-account trading	1,635-1,756	Account rental and sale; many posts concern a Turkish bank, not a Qatari one
Phishing and scams	1,618-1,657	Scam pages, SMS and caller-ID services listing Qatar, buyers of Qatar-registered accounts
KYC and identity documents	534-567	Verified trading-platform accounts "for Qatar", document templates, verification services
Combolists	171-175	Country- and domain-labelled credential lists, including airline loyalty accounts
Access sales	139-147	Remote access, panels and buyers seeking government access
Malware and exploits	124-137	Tool sales and exploit discussion, mostly global
Stealer logs	40-44	Log sales naming Qatari services
Ransomware (relays)	31	Tracker bots relaying leak-site claims (Chapter 7)
DDoS and hacktivism (tagged)	31	Small within the tag; Chapter 6 draws on actor channels and public reporting

Families overlap and must not be added. Many cleaned posts are multi-country lists or concern a Turkish bank rather than Qatar. Treat cleaned counts as an upper bound.

Prices quoted. In cleaned posts, the median quoted price was 14 USD per card and 15 USD for data and lead offers. It was 32 USD for bank and wallet accounts and 50 USD for KYC and document services. These are asking prices, not completed sales (Chapter 8).

4.4 Specific claims against Qatari organisations

Sixteen offers stand out because they name a Qatari organisation, or a Qatari sector, and claim access or data. None was independently verified, and we did not obtain any file.

Date	Claimed target	Claim	Venue	Post
17 Jan	A financial-sector body	An 800,000-line "financial database", 400 USD	Telegram channel	None
5 Feb	An energy-sector engineering contractor	A database with names, contact details, documents and passports	Telegram channel of a group calling itself LulzSec Hackers	None
19 Feb	An energy-sector company	Live access to cloud and identity systems; employee records	Breach forum	B01
3 Mar	An aviation-sector organisation	A database offered on a private channel	Leak-monitor relay	None
9 Mar	Civil data for Qatar and four other markets	560 GB of "fresh" personal and company records	Arabic-language Telegram channel	B17
10 Mar	The same energy-sector company	A database "dump" with employee records; the poster says it wiped a server	Telegram channel	B02
10 Mar	A government security body	Personnel data on 1,900 members, 10,000 USD	Two breach forums; Telegram relay	B03

Date	Claimed target	Claim	Venue	Post
16 May	A consumer discount app	About 300,000 user records from a breach the poster dates to 2023	Forum; earlier relays in January and March	B18
19 May–22 Jul	A private hospital	About 12 GB said to include patient and insurance records (May), then about 31,000 CV files of medical staff (Jul)	Telegram relays of two listings	B16
8 Jun	A private school group	Over 100 GB, including passports, ID cards and staff data; the poster says it deleted the databases	Breach forum	B06
16 Jun	An events company	A user database with emails, passwords and phone numbers	Forum	None
25 Jul	Online shoppers	"Qatar shopping data", 36,000 records	Leak-monitor relay	None
26 Aug	A large bank	A dataset said to span 2024–2026, including government and defence records	Telegram relay of a forum listing	B05
3 Sep	A public-sector body	Sample rows with application access tokens	Forum	B07
10–14 Nov	The same large bank	A very large number of customer records and staff records, 1,500 USD	Two breach forums	B04
16 Nov	A sports club	108 files with IDs, passports, player contracts and bank details, from a breach the poster dates to 2025	Forum	None

What this tells defenders. Claims concentrate on organisations that hold large staff or customer populations: energy, banking, security, education and the public sector. Two pairs show repetition rather than independent confirmation. The energy-sector company was named by two different posters three weeks apart, with different figures. The large bank was named in April, August and November; the April thread is described in Case C and is not one of the sixteen. Repetition raises the priority of a check; it does not establish a breach.

Several claims are also implausible in their own terms. One seller claims a very large customer file yet prices it at 1,500 USD. Another dates its file to 2023 while selling it as new. Neither detail establishes fabrication.

EVIDENCE CARD B01 — 19 Feb 2026

Unnamed poster (a public monitor names Montaro) Breach forum · Forum · English

ORIGINAL

```
TARGET PROFILE Entity: [energy-sector company] [...] Status:
Active Session - All Systems Accessible [...] Employee
registry extracted [...] Cloud credentials discovered in
connection strings [...] Global Administrator privileges
obtained [...]
```

HELD	The claim, its claimed timeline and the kinds of systems it names (cloud, identity directory, building security); a public monitor's relay of a similar claim a day earlier.
NOT ESTABLISHED	Any access or data theft; whether the poster is the persona the monitor names.

EVIDENCE CARD B02 — 10 Mar 2026

ELIPHAS SYNDICATE Telegram channel · Telegram · English

ORIGINAL

```
WE JUST PULLED A MASSIVE RELIABLE DUMP FROM [energy-sector
company] [...] WE WIPED THE WHOLE SERVER CLEAN AFTER
EXFILTRATION [...] INCLUDING [...] FULL EMPLOYEE RECORDS
[...] WE DONT CARE ABOUT THE POLITICS WE CARE ABOUT THE
PAYOUT
```

HELD	The claim, the claimed record types and the poster's stated financial motive.
NOT ESTABLISHED	Any wiping, any exfiltration, or a link to the February poster.

EVIDENCE CARD B03 10 Mar 2026

TheAshborn Breach forum · Forum · English

ORIGINAL

```
We had Access to [government security body] [...] We Sell
1900X personnel data (Dumped data) 2 Screenshots as proof:
[link removed] Data includes: {Full Name Email Business
Fixed Number Home Fixed Number Mobile Number Fax Number Job
Title Department Company Nationality} Price : 10,000$
```

HELD	The offer, the claimed fields, the price and two forum copies the same day.
NOT ESTABLISHED	The data's origin or age, or any sale.

EVIDENCE CARD B17 9 Mar 2026

Data seller Telegram channel · Telegram · Arabic, with the seller's own Russian and English

ORIGINAL

للبيع - 560 GB - بيانات مدنية حديثة بالكامل من 2 يناير 2026 - الدول المشمولة: السعودية مصر قطر دول أوروبية الولايات المتحدة - المحتويات: بيانات أفراد - سجلات خاصة - مستندات شخصية - صور - معلومات بنوك وشركات

TRANSLATION

For sale: 560 GB of completely fresh civil data from 2 January 2026. Countries covered: Saudi Arabia, Egypt, Qatar, European countries, the United States. Contents: personal data, private records, personal documents, photos, bank and company information.

HELD	The offer, the claimed volume and the five markets named.
NOT ESTABLISHED	Which Qatari data, if any, the file holds, or its origin.

EVIDENCE CARD B16 22 Jul 2026

Security news relay Telegram relay of a forum listing · Telegram · English

ORIGINAL

```
[About 30,000] Medical Professionals' CVs Leaked from
[private hospital] [...] containing [about 31,000] CV files
belonging to healthcare professionals. [file-format counts
removed]
```

HELD	That a relay described a listing of staff CV files attributed to the hospital.
NOT ESTABLISHED	The listing itself, the files or their origin.

Smaller identity and credential offers. Beyond the sixteen claims, we observed narrower offers that point the same way. None was verified.

Date	Observed offer	Our reading
Jan-Feb	Credential lists labelled with a government domain and with a Qatari telecom domain (about 9,000 lines on one forum)	Typical combolist recycling; users' own devices and reused passwords, not the systems, are the likely source
Mar	A seller advertising "Qatar RAT 2026" on a carding forum	Malware sale with a country label; no target named
Apr	Passport photographs with contact details for 13 countries, Qatar among them	Identity material for KYC fraud; origin unknown
Jun-Jul	Automated forum uploads of a recruitment-site database and of "Qatar logs"	Bot uploads; size and age unknown
Jul	A 4,000-line combolist labelled for Qatari education domains	Could support credential reuse against university systems
Oct	A regional retailer's database "for Saudi Arabia, Kuwait and Qatar", 27 million rows	A foreign retailer's customers include Qatar residents

4.5 Case studies

Each case gives the claim, what we can establish and a proportionate response, with chronology, alternatives and limits where we have them.

A

CASE A

Two posters claim the same energy-sector company

Evidence card B01 | 19 Feb 2026 | Breach forum | Energy

TWO CLAIMS, UNVERIFIED

Claim	On 19 February a breach-forum post described access to the cloud, identity directory and building-security systems of a Qatari energy-sector company, with employee records. A public monitor relayed a similar claim the day before, attributed to a persona called Montaro.
Chronology	On 10 March a second poster, *ELIPHAS SYNDICATE*, claimed a database dump of the same company, with employee records, and said it had wiped a server.
What we can establish	That two posters made overlapping claims three weeks apart, with different volumes, and that both posts include employee-style fields. The posts do not establish access, data theft or any wiping.
Alternatives	One actor using two names; a second poster copying the first; recycled HR or contractor data; data taken from a supplier.
Limits	No sample was assessed, and no official or company statement was found by our cut-off.
Response	Review privileged directory roles, cloud keys stored in application settings and accounts on building-security systems. Check supplier access to the same systems.
BOTTOM LINE	**Two posters named the same company: check privileged roles and supplier access before anyone speaks of a breach.**

B

CASE B

Personnel data of a government security body offered

Evidence card B03 | 10 Mar 2026 | Breach forum | Government (security)

CLAIM UNVERIFIED

Claim	On 10 March a persona we record as *TheAshborn* offered personnel data on 1,900 members of a government security body for 10,000 USD, with two screenshots.
What we can establish	The offer, the claimed fields (names, contact numbers, job titles, departments and nationality) and two forum copies on the same day. A Telegram channel relayed it the same day.
Alternatives	A staff directory exported from a third-party system; an older contact list; a genuine compromise.
Response	Compare the claimed fields with directory and HR exports. Warn staff of targeted phishing and impersonation, because contact data of security personnel is useful for both.
BOTTOM LINE	**Whatever its origin, staff contact data supports targeted phishing: warn staff and compare fields with directory exports.**

C

CASE C

The same large bank claimed twice

CLAIM UNVERIFIED (REPEATED)

Evidence card B04 | 10 Nov 2026 | Breach forum | Banking

Claim	On 10 and 14 November sellers on two breach forums offered a very large number of customer records and staff records attributed to a large Qatari bank. The asking price was 1,500 USD, or 900 USD for half.
Chronology	In April a forum thread offered employee, transfer and user data attributed to the same bank. In August a Telegram relay described a forum listing said to span 2024-2026. We found no statement by the bank or the authorities confirming it by our cut-off.
What we can establish	That the offers name the bank, list a customer-record schema that includes a card-number field, and recur across venues. They do not establish the file's origin, its age or a sale.
Alternatives	Aggregated or older data rebranded as new; data from a partner or card processor; a genuine compromise.
Response	Compare the claimed schema with core-banking and card-system exports. Watch for customer phishing that quotes account details, and prepare a customer notice in case a sample is verified.
BOTTOM LINE	**A recurring claim with a card-number field in its schema: compare with exports and prepare customer messaging.**

D

CASE D

A private school group

CLAIM UNVERIFIED

Evidence card B06 | 8 Jun 2026 | Breach forum | Education

Claim	On 8 June a forum poster said it had taken over a private school group's systems, extracted over 100 GB and deleted the databases. It listed passports, ID cards, staff records and home addresses.
What we can establish	The post, the claimed data types and a list of database names. We found no statement by the school or an authority.
Alternatives	Exaggeration of a smaller website compromise; data from a school-management software provider.
Response	Schools should check backups, web-hosting accounts and software-provider access, and treat parents' and children's identity data as a priority for notification if a sample is confirmed.
BOTTOM LINE	**Children's identity data raises the stakes: check backups and provider access, and prepare notification.**

E

CASE E

Application tokens in a sample attributed to a public-sector body

SAMPLE POSTED

Evidence card B07 | 3 Sep 2026 | Forum | Public sector

Claim	On 3 September a forum post said a Qatari public-sector body had been breached. It published a short sample of what look like application access tokens and user rows.
What we can establish	The sample's structure. Tokens in a public post are a risk whether or not the wider claim is true, because anyone can try them.
Response	Rotate any exposed tokens and keys, restrict the exposed service to known networks and review access logs from the dates in the sample.
BOTTOM LINE	**Rotate exposed tokens now; a public token is a risk whether or not the breach claim is true.**

F

CASE F

Buyers seek access to government networks

DEMAND OBSERVED (TWO POSTS)

Evidence card B08 | 3 Sep 2026 | Forum, with the same text on Telegram | Government

Claim	On 3 September a forum user and a Telegram user posted the same request: remote-desktop, VPN or database access to government bodies in Qatar and two other states in the region. A similar request in April named a dozen countries.
What we can establish	Demand for access, not access itself.
Why it matters	Demand of this kind is what turns stealer logs and exposed remote services into intrusions.
Response	Monitor government VPN and remote-desktop sign-ins for new devices and unusual hours. Prioritise employee-device associations from Chapter 3.
BOTTOM LINE	**Buyers want government remote access: watch VPN and remote-desktop sign-ins and validate employee devices.**

EVIDENCE CARD B04 — 10 Nov 2026

UNC6783 (self-applied channel name) Breach forum · Forum · English

ORIGINAL

```
a leak occurred targeting one of the Banks in Qatar in large
amounts [[...] customer data, and [...] employees in several
branches of [large bank] in 2026.] [...] Data include [...]
CUSTOMERID, SEX, NAME, TYPE [...] ADDRESS [...]
MOBILENUMBER, ATMCARDNUMBER [samples removed]
```

HELD	The claim, the claimed schema and a near-identical offer on a second forum four days later at 1,500 USD.
NOT ESTABLISHED	The file's origin or age, any sale, or a breach of the bank.

EVIDENCE CARD B05 — 26 Aug 2026

Security news relay Telegram relay of a forum listing · Telegram · English

ORIGINAL

```
[large bank] Data Offered on Underground Forum. A hacker is
advertising a database originating from [large bank]
sources, with the listing referencing data spanning 2024-
2026. [...] User data, Transaction data [...] Government-
related records, Defence-related records
```

HELD	That a relay described a forum listing attributed to the bank in August.
NOT ESTABLISHED	The listing itself, its contents or any link to the November offer.

EVIDENCE CARD B06 — 8 Jun 2026

Unnamed poster Breach forum · Forum · English

ORIGINAL

```
[private school group] in Qatar was hacked, and all
databases and domains were compromised. After extracting the
data, we deleted all databases and took the website offline.
The data obtained included passports, ID cards, full names
[...] The total amount of data obtained exceeded 100
gigabytes. [sample link removed] To purchase all data,
please contact us [contact removed]
```

HELD	The claim, the claimed data types and listed database names.
NOT ESTABLISHED	Any deletion, outage or data theft; we found no statement by the school or an authority.

EVIDENCE CARD B07 — 3 Sep 2026

Unnamed poster Forum · Forum · English

ORIGINAL

```
[public-sector body] breached. [address removed] Sample:
ID,Name,Token,Status,Expire At [...] [tokens removed]
```

HELD	A sample whose rows look like application access tokens and user records.
NOT ESTABLISHED	Whether the tokens are valid or the wider breach claim is true.

EVIDENCE CARD B08 — 3 Sep 2026

Anonymous buyer Forum, with the same text on Telegram · Forum · English

ORIGINAL

```
hi I look for RDP, VPN Or Any Network Access in any GOV
organs in Qatar, Jordan And Saudi Arabia Or Any Leaked
Secret Data Bases From There Networks. Any Things You Have
for Sale?
```

HELD	Demand for government network access in three countries, posted twice the same day.
NOT ESTABLISHED	That anyone supplied such access.

EVIDENCE CARD B18 — 16 May 2026

Unnamed poster Forum · Forum · English

ORIGINAL

```
DATABASE [Qatar] [consumer discount app] [about 300k] users
data, format: csv fields: id, full_name, mobile, email,
password [...] dob, nationality, residence [...] Sample:
[removed]
```

HELD	The offer and fields; relays in January and March describe the same file and one dates the breach to 2023.
NOT ESTABLISHED	The file's age or origin, or any current exposure.

4.6 What the forums add

Forums contributed only 90 tagged posts and 334 further posts mentioning Qatar in the year, but they carry most of the specific claims above. Most other forum hits are search-spam pages and multi-country lead lists. Forum buyers also posted requests for Qatari government access (Case F). Demand for Qatari access and identity data is itself a finding.

KEY TAKEAWAYS

01

Raw volume is dominated by automated Turkish-language posts; read only cleaned counts, and treat them as an upper bound.

02

Specific claims concentrate on energy, banking, security, education and the public sector; none was confirmed by our cut-off.

03

Repeated naming of the same organisation is a reason to check quickly, not proof of a breach.

CHAPTER 5

Targeting examples by sector

THIS CHAPTER ANSWERS

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

10
sectors with observed activity, from government to retail

IN SHORT

The posts below show how criminal and political actors talk about Qatari organisations. Political actors name state websites and claim disruption. Criminal sellers name large employers and data holders, or list Qatar as one market among many. Official reports and vendor research add espionage and fraud. Check each claim with the organisation it names, and start with the sector's first response.

Victims are described by role under the policy in Appendix A.9. Examples are drawn from Blackhole posts and the public sources in Appendix C.

Government

`DDoS claim` `data claim` `access demand` `espionage`

EXAMPLE OF OBSERVED ACTIVITY (ANONYMISED)

DDoS claims against government portals, ministries and a financial regulator (Mar; Chapter 6); personnel data of a government security body offered (Mar); sample tokens attributed to a public-sector body (Sep); buyers seeking government VPN and remote-desktop access (Apr, Sep); China-nexus espionage against government and energy targets (vendor research, Mar)

WHAT IT MEANS

Availability claims are noisy; the material risks are staff data, exposed application tokens and remote access

FIRST RESPONSE

Pre-agree status statements; rotate exposed tokens; watch VPN sign-ins

Energy

`Access and data claims` `ransomware listing` `DDoS claim` `espionage`

EXAMPLE OF OBSERVED ACTIVITY (ANONYMISED)

Two posters claimed the same energy-sector company (Feb, Mar; Case A); a group claimed an engineering contractor's database (Feb); an oil-services contractor listed by an extortion group (Jul; outside the Ransompedia count); an energy-sector site on a DDoS list of regional energy sites (Mar); lures about strikes on oil and gas facilities (vendor research, Mar)

WHAT IT MEANS

Identity, supplier and building-security systems are the claimed routes; contractors are part of the exposure

FIRST RESPONSE

Review privileged roles and supplier access; hunt for archive and shortcut lures

Banking

`Data claim` `carding` `account trading` `DDoS claim`

EXAMPLE OF OBSERVED ACTIVITY (ANONYMISED)

A large bank named in a customer-record offer (Nov; Case C) and earlier offers (Apr, Aug); a financial-sector body's "database" offered (Jan); card-checker outputs naming seven Qatari issuers; Qatar-registered trading accounts sold; a financial regulator on a DDoS list (Mar)

WHAT IT MEANS

Most posts are fraud tooling; the first signals to act on are current credential listings, then staff devices (Chapter 9)

FIRST RESPONSE

Triage current credential listings; compare claimed schemas with exports; alert on checker declines

Telecom

`Ransomware listing` `combolist` `DDoS`

EXAMPLE OF OBSERVED ACTIVITY (ANONYMISED)

A telecom infrastructure company listed by an extortion group (May); credential lists labelled with a telecom domain (Feb); measured DDoS fell mostly on carriers

WHAT IT MEANS

Carriers absorb most measured DDoS; customer credentials circulate in recycled lists

FIRST RESPONSE

Confirm upstream DDoS capacity; force resets for listed customer accounts

Aviation and transport

`Data claim` `account resale`

EXAMPLE OF OBSERVED ACTIVITY (ANONYMISED)

An aviation-sector organisation named in a "database" offer (Mar, unverified); a Gulf carrier's loyalty accounts in miles shops throughout the year

WHAT IT MEANS

Loyalty and email takeover is the observed fraud route, not an airline breach

FIRST RESPONSE

Add MFA to loyalty accounts; watch redemption anomalies

Education

`Data claim` `ransomware listing` `combolist`

EXAMPLE OF OBSERVED ACTIVITY (ANONYMISED)

A private school group claimed (Jun; Case D); a research institute listed by an extortion group (Apr); a combolist for education domains (Jul)

WHAT IT MEANS

The claims concern children's and parents' identity data and research systems; none is confirmed

FIRST RESPONSE

Check backups and software-provider access; enforce MFA for staff

Media

`Spyware (Citizen Lab finding)`

EXAMPLE OF OBSERVED ACTIVITY (ANONYMISED)

Candiru commercial spyware targeted at least 45 Al Jazeera devices in 2024 and 2025 through targeted advertising, and devices were infected (Citizen Lab, Oct; Chapter 7)

WHAT IT MEANS

Devices at media organisations can be targeted with commercial spyware

FIRST RESPONSE

Keep staff devices patched; treat unusual ad-driven redirects as an incident signal

Healthcare

`Data claims`

EXAMPLE OF OBSERVED ACTIVITY (ANONYMISED)

Patient and insurance records (May) and CV files of medical staff (Jul) attributed to a private hospital

WHAT IT MEANS

Patient records and recruitment files both carry identity documents

FIRST RESPONSE

Review recruitment-platform exports and retention

Retail and consumer

`Data claims` `mostly recycled`

EXAMPLE OF OBSERVED ACTIVITY (ANONYMISED)

A discount app's file of about 300,000 users re-offered (Jan-May); "Qatar shopping data" (Jul); a regional retailer's database naming Qatar (Oct)

WHAT IT MEANS

Old consumer data powers phishing and account takeover

FIRST RESPONSE

Force password resets where a match is confirmed

Professional services and construction

`Ransomware listings`

EXAMPLE OF OBSERVED ACTIVITY (ANONYMISED)

A law firm and several contractors listed by extortion groups (Apr-Nov)

WHAT IT MEANS

The listings name mid-sized firms rather than large brands

FIRST RESPONSE

Test restores; review remote access for suppliers

Reading across sectors. Organisation-specific claims fall into two groups. Political actors name state websites and claim disruption. Criminal actors name large employers and data holders, or treat Qatar as one market among many. Espionage, reported by vendors, targets government and energy and did not appear in the leak-site and forum data we searched.

KEY TAKEAWAYS

01

Political actors name state websites; criminal sellers name large employers and data holders.

02

Energy faces both data claims and espionage lures, and its contractors appear in extortion listings.

03

For banks and airlines, the observed fraud route runs through customer, email and loyalty accounts.

CHAPTER 6

Hacktivism and DDoS

THIS CHAPTER ANSWERS

Who claimed attacks on Qatar in 2026, what did measurement and reporting show, and how should an organisation prepare for the next burst?

31,836

DDoS attacks on Qatar measured by NETSCOUT in January-June 2026

INSIDE THIS CHAPTER

6.1 Timeline | 6.2 The March burst: claims against measurement | 6.3 Other claims in their own words | 6.4 Lessons for defenders

IN SHORT

Hacktivist claims against Qatar clustered between 28 February and 25 March 2026, after the regional escalation began. Four groups claimed DDoS against government portals, ministries, a public-service billing and payment portal, a financial regulator and an energy-sector site. We found no official statement confirming an outage. Measured DDoS traffic was high, and NETSCOUT classed most targets as telecom carriers; its data does not show whether the named sites were hit. Contract upstream mitigation and pre-agree who confirms service status before the next burst.

6.1 Timeline

28 Feb 2026 — **CloudSEK situation report**
Records a self-reported DDoS by BD Anonymous Team on a ministry's online service, 28 Feb-1 Mar

28 Feb 2026 — **CloudSEK situation report**
Records DieNet's claimed DDoS on government portals, telecoms, airports and banks in six countries, Qatar among them

3 Mar 2026 — **Keymous Plus**
Claims a public-service billing and payment portal offline, with an availability-check link

6 Mar 2026 — **DieNet relay channel**
Nine automated posts name Qatari government sites as "currently targeted"

9 Mar 2026 — **Intel 471**
Places Qatar among the ten most claimed-against locations for the week from 27 Feb

12 Mar 2026 — **Keymous Plus**
Lists 13 state websites, including portals, ministries and a financial regulator

14 Mar 2026 — **313 Team**
Claims a government portal "completely disabled" for one hour; extends it on 15 Mar

24 Mar 2026 — **Ministry of Interior**
Warns of calls and messages "that take advantage of the current situation" to obtain bank details and one-time codes

24 Mar 2026 — **Keymous Plus**
"Testing visit" against five ministries; says some sites were up again

25 Mar 2026 ● **Keymous Plus**
Names an energy-sector site among 12 regional energy sites

10 Apr 2026 ○ **The National**
Reports early claims against energy-sector and media sites, then a decline in direct hacktivism

19 Jun 2026 ● **BD Anonymous Team**
Claims a security force's website taken down, citing a foreign military presence

Dark markers are actor posts, outlined markers are relays and reporting by third parties, coral markers are official statements. Dates are post dates in UTC; Doha time is UTC+3. The Ministry of Interior's warning concerns fraud, not DDoS; it is the only official statement tied to the escalation that we found.

6.2 The March burst: claims against measurement

Claims. Between 28 February and 25 March four groups claimed DDoS against Qatari targets. Keymous Plus posted four lists, naming a public-service billing and payment portal, 13 state websites, five ministries and an energy-sector site [S2]. A relay channel published nine automated DieNet posts on 6 March, each naming a government site with an availability-check result [S34]. 313 Team claimed a government portal on 14 and 15 March. CloudSEK recorded a BD Anonymous Team claim against a ministry's online service [S29].

EVIDENCE CARD B10 — 12 Mar 2026

Keymous Plus Actor channel · Telegram · English, as posted

ORIGINAL

```
A visit been planned to be back on the heat [...] Qatar:
[state body] Check Host [government portal] Check Host
[ministry] Check Host [ministry] Check Host [...] [financial
regulator] Check Host [links removed]
```

HELD	A list of 13 Qatari state websites with availability-check links, followed by sites in another state.
NOT ESTABLISHED	Any outage or impact.

EVIDENCE CARD B11 — 14 Mar 2026

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

ORIGINAL

نفذت [...] فريق 313 هجوم سيبراني استهدف [بوابة حكومية] حيث ادى الهجوم لتعطيل الموقع الالكتروني بالكامل. سيستمر الهجوم لمدة ساعة واحدة.

TRANSLATION

313 Team carried out a cyberattack targeting [a government portal], completely disabling the website. The attack lasted for one hour [sic; the Arabic says it 'will continue' for one hour]. (Group's own English, redacted.)

HELD	The claim, a check link and an update the next day claiming several more hours.
NOT ESTABLISHED	An outage; no official or organisation statement was found.

Official account. We found no statement from a Qatari authority or a named organisation confirming a DDoS outage in the window. The Ministry of Interior warned on 24 March about fraud that exploited "the current situation" [S35]. That warning is about phishing calls and messages, not service availability.

Measurement. NETSCOUT recorded 31,836 DDoS attacks on Qatar in January-June 2026, with an average duration of 20.97 minutes. Wired telecom carriers took 29,808 of them, and DNS amplification was the most common vector [S32]. StormWall reported that attacks on Qatar rose 75% year on year in the first quarter, and that Qatar's share of regional DDoS rose from 8% to 14% [S31].

What we can establish. The claims and the telemetry describe different things. Telemetry counts attacks on networks, mostly carriers, and names no group. The claims name state websites and rest on availability-check links. Neither confirms an outage at a named organisation, so we do not combine them into a ratio or a success rate.

Point	Groups' claims	Official account	Measurement and reporting
Timing	28 Feb-25 Mar, one further claim in June [S2][S29]	No DDoS statement found	Qatar in Intel 471's weekly top ten from 27 Feb [S30]; decline reported by April [S33]

Point	Groups' claims	Official account	Measurement and reporting
Targets	Government portals, ministries, a public-service billing and payment portal, a financial regulator, an energy-sector site [S2]	None confirmed	29,808 of 31,836 measured attacks hit wired telecom carriers [S32]
Effect	"Completely disabled", "down", availability-check links	Not stated	Intel 471: groups "frequently exaggerate" impact [S30]
Volume	Not stated	Not stated	Average 20.97 minutes; DNS amplification the top vector [S32]
Tooling	Keymous Plus and 313 Team posts both carry referral links to the same commercial stresser brand [S2]	Not stated	CloudSEK: attribution "self-reported", technical validation limited [S29]
Attribution	Own claims	None	Unit 42 describes 313 Team and DieNet as pro-Iran groups [S28]

What it means. A burst of DDoS claims coincided with the escalation, and measured attacks rose. The claimed outages at state websites remain claims. The shared stresser links show that at least two of the groups promote the same rented capacity. That supports a commercial-service association, not a common operator.

6.3 Other claims in their own words

EVIDENCE CARD B09 — 3 Mar 2026

Keymous Plus Actor channel · Telegram · English, as posted

ORIGINAL

```
Lately [QA flag] [public-service provider]. Services for
[service names], billing, and payment. Check Host [link
removed] : 1000sec
```

HELD	The claim and an availability-check link.
NOT ESTABLISHED	An outage; a check link records a moment of unreachability at most.

EVIDENCE CARD B12 — 6 Mar 2026

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

ORIGINAL

```
DieNet network is currently targeting [government portal]
and it may be down for you at the moment. Check-Host [...]
Connection timed out [...] This is an automated [...]
```

HELD	Nine automated posts the same day naming Qatari government sites.
NOT ESTABLISHED	Who ran the attacks, or any outage beyond a timed-out check.

EVIDENCE CARD B15 — 24 Mar 2026

Keymous Plus Actor channel · Telegram · English, as posted

ORIGINAL

```
A testing visit. Qatar: [ministry] Check Host [...]
[ministry] [...] [ministry] [...] [ministry] [...]
[ministry] [links removed] Some websites still down others
are up after the test is down, Next visits will be focusing
on downtime.
```

HELD	A list of five ministries and the group's own statement that some sites were up again.
NOT ESTABLISHED	Any outage or its length.

EVIDENCE CARD B13 — 19 Jun 2026

BD Anonymous Team Actor channel · Telegram · English, as posted

ORIGINAL

```
We have successfully took down The Official site of
[security force] Cheakhost [link removed] [...] [motive
statement shortened] BD Anonymous Team
```

HELD	The claim and a check link; the post cites a foreign military presence as its motive.
NOT ESTABLISHED	An outage; no public reporting on this claim was found.

Not counted as hacktivism. On 30 October a security-news relay reported that an aviation website had been down for about 24 hours and tagged it as a cyberattack. No group claimed it and we found no official explanation, so we do not count it.

The June claim by BD Anonymous Team named a security force's website and cited a foreign military presence as its motive. We report the stated motive as the group's own and take no position on it. We found no public reporting on this claim.

6.4 Lessons for defenders

1. **Pre-agree the public line.** A group's screenshot and a carrier's telemetry rarely measure the same thing. Decide in advance who confirms service status, within what time and through which channel.
2. **Protect portals at the upstream.** Volumetric attacks are absorbed upstream or not at all. Contract mitigation for citizen-facing portals and payment pages before an event, and test it.
3. **Watch the target lists.** Keymous Plus published lists before and between its claims. Treat a new list naming your sector as a signal to raise DDoS readiness.
4. **Expect fraud to ride the same news.** The Ministry of Interior's warning shows that scammers exploit the same events. Pair any DDoS alert with a fraud and phishing alert to staff and customers.

KEY TAKEAWAYS

01

Hacktivist DDoS claims against Qatar clustered in March 2026; none was confirmed as an outage by an authority or an organisation.

02

NETSCOUT classed most measured targets as wired telecom carriers; its data does not show whether the sites the groups named were among them.

03

Two groups promote the same rented stresser; upstream mitigation is the control either way.

CHAPTER 7

Threat actors

THIS CHAPTER ANSWERS

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

7

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

INSIDE THIS CHAPTER

7.1 How the actors connect | 7.2 Espionage and commercial spyware (as attributed by vendors and researchers) | 7.3 Hacktivist and DDoS actors | 7.4 Ransomware and extortion | 7.5 Criminal personas seen in Blackhole | 7.6 Advisories from the national agency

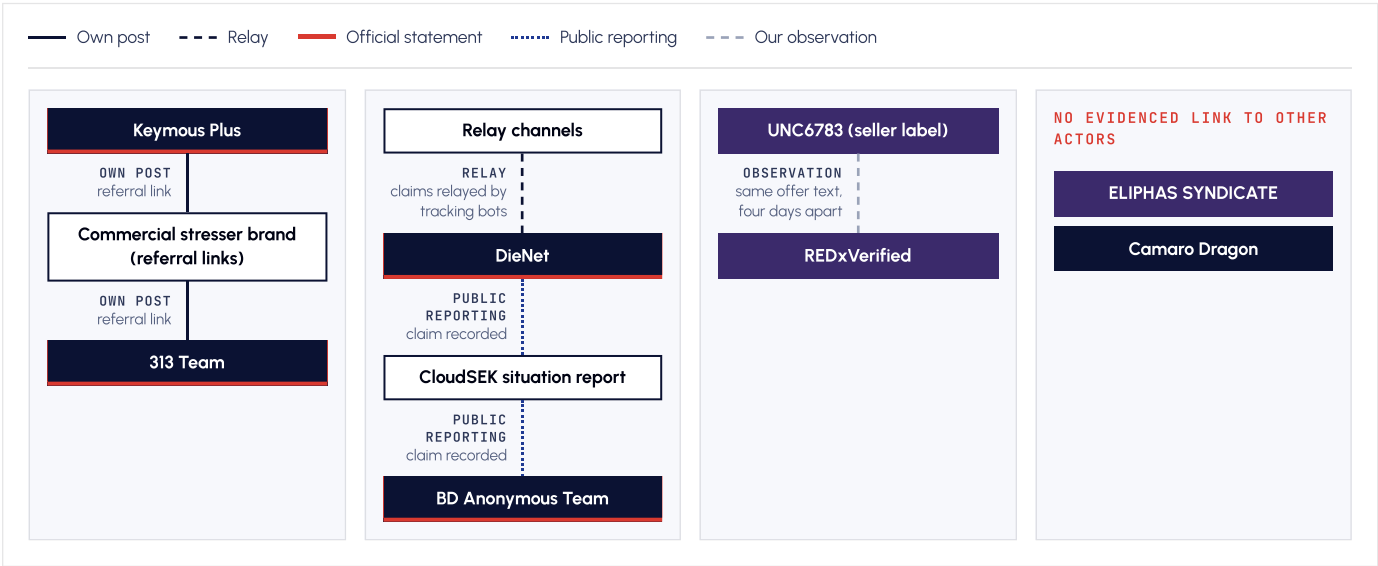
IN SHORT

Check Point attributed one 2026 espionage campaign to China-nexus Camaro Dragon and assessed a second, with low confidence, as China-aligned. Citizen Lab reported Candiru spyware attacks targeting at least 45 Al Jazeera devices, and found devices infected. Hacktivist groups claimed DDoS in March. Ransompedia holds listings for eight Qatari organisations, mostly mid-sized firms. Data sellers named energy, banking and security bodies. Block external archive and shortcut attachments, patch edge systems that NCSA flags as exploited, and verify every 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.



7.2 Espionage and commercial spyware (as attributed by vendors and researchers)

Camaro Dragon

Linked by Check Point to clusters reported as Mustang Panda and Earth Preta

Espionage (China-nexus per Check Point)

China-nexus (vendor attribution; no confidence level stated)

AGAINST QATARI TARGETS, MARCH 2026

1-2 Mar	PlugX variant against Qatari targets within a day of the escalation
Mar	Lure: archive posing as photos of missile damage, with a shortcut file

TARGETED SECTORS

Government and energy-related entities (Check Point weekly summary)

SEEN IN PUBLIC REPORTING

- [S26] Check Point Research (9 Mar 2026): PlugX keys seen in earlier campaigns attributed to Camaro Dragon
- [S27] Check Point weekly report (16 Mar 2026): said the campaigns targeted government and energy-related entities

OUR ASSESSMENT

The clearest documented espionage activity against Qatari targets in 2026. Lures tracked the news within a day; the chain depended on a user opening an archive, not on an exploited server.

CONFIDENCE **Vendor attribution, no confidence level stated**

Check Point reported that Camaro Dragon attempted to deploy a PlugX variant against Qatari targets within a day of the regional escalation. The lure was an archive disguised as photographs of missile damage. A shortcut file started a chain that ended in DLL hijacking of a legitimate cloud-storage client. Check Point tied the activity to Camaro Dragon through PlugX configuration keys seen in earlier campaigns it attributes to that group [S26].

Unnamed China-aligned cluster

Rust loader and Cobalt Strike campaign

Espionage (low-confidence vendor assessment)

China-aligned, assessed with low confidence by Check Point

AGAINST QATARI TARGETS, MARCH 2026

Mar	Password-protected archive on strikes at Gulf oil and gas facilities, likely by email
Mar	Rust loader, screen-reader DLL hijack, Cobalt Strike

TARGETED SECTORS

Qatari organisations (Check Point); government and energy-related entities per the weekly summary of the campaigns

SEEN IN PUBLIC REPORTING

- [S26] Check Point Research: assessed as China-aligned with low confidence
- [S44] Proofpoint describes a suspected China-aligned cluster sideloading the same component of NVDA, an open-source screen reader, with a Gulf oil-and-gas lure, to deliver Cobalt Strike to Middle Eastern government and diplomatic targets. It describes no Rust stage and does not name Qatar; neither vendor links the two

OUR ASSESSMENT

A second, separate espionage attempt in the same weeks. Attribution is weak; the defensive lessons are the same as for Camaro Dragon.

CONFIDENCE **Low (vendor)**

The second campaign used a password-protected archive about strikes on Gulf oil and gas facilities, likely delivered by email. A previously unseen Rust loader abused a screen-reader component through DLL hijacking and delivered Cobalt Strike [S26]. Proofpoint separately described a suspected China-aligned cluster that sideloaded the same component of NVDA, an open-source screen reader, to deliver Cobalt Strike [S44]. Its archive used the same Gulf oil-and-gas theme, and its targets were Middle Eastern government and diplomatic bodies. It describes no Rust stage and does not name Qatar, and neither vendor links the two [S44]. We keep them separate.

Selected techniques from Check Point's description are shown below. Check Point did not publish ATT&CK identifiers; the mapping is ours.

TECHNIQUES NAMED IN THE VENDOR RESEARCH, BY TACTIC

Initial access	Execution	Defence evasion	Persistence / evasion
T1566.001 Spearphishing attachment (archive likely sent by email; second campaign)	T1204.002 User execution: malicious file (shortcut inside the archive)	T1036 Masquerading (archive posing as photos)	T1574.001 Hijack execution flow: DLL (cloud-storage client and screen-reader component)

Check Point did not publish ATT&CK identifiers. This mapping is Odin's reading of Check Point's description of 9 March 2026, checked against ATT&CK on 21 November 2026; it is not the vendor's. [S26]

Commercial spyware against Al Jazeera. On 15 October 2026 Citizen Lab reported that at least 45 devices within Al Jazeera were targeted in 2024 and 2025, in zero-click attacks delivered through targeted online advertising [S48]. It found that devices were infected with Candiru spyware and analysed malware recovered from one of those devices [S48]. Al Jazeera reported the findings the same day and condemned the targeting [S47]. Neither report names the customer on whose behalf the spyware was used [S47][S48].

Unresolved. For the Check Point campaigns, the victims, any data taken and whether either campaign succeeded. Check Point's weekly summary said the campaigns targeted government and energy-related entities [S27]. **Meaning.** Lures followed the news within a day. For government and energy organisations, the decisive controls are blocking archive and shortcut attachments from outside, alerting on legitimate signed binaries that load DLLs from user folders, and hunting for Cobalt Strike beacons. Nothing in these campaigns appeared in the leak-site and forum data we searched.

7.3 Hacktivist and DDoS actors

Keymous Plus

Keymous

Hacktivist DDoS brand

No stated alignment in the excerpts shown; CloudSEK lists it among actors active during the escalation

IN QATAR, 2026

3 Mar	A public-service billing and payment portal (B09)
12 Mar	13 state websites (B10)
24 Mar	Five ministries; says some sites were up again (B15)
25 Mar	An energy-sector site among 12 regional energy sites

CLAIMED TARGETS

Government portals, ministries, a financial regulator, a public-service billing and payment portal, an energy-sector site

IN THEIR WORDS

> *"Some websites still down others are up"* B15

SEEN IN PUBLIC REPORTING

- [S29] CloudSEK (2 Mar 2026): announced large-scale intended operations against other states with limited technical substantiation

OUR ASSESSMENT

The most frequent claimant against Qatar in our data. Its posts carry referral links to a commercial stresser brand, which suggests rented capacity; its own words admit that sites recovered.

CONFIDENCE **High that it made the claims; impact unverified**

DieNet

DieNet Network V5

Hacktivist DDoS brand

Pro-Iran (per Unit 42); listed by CloudSEK among pro-Iran actors

IN QATAR, 2026

28 Feb-1 Mar	Claimed DDoS on government, telecom, airport and bank sites in six countries (CloudSEK)
6 Mar	Nine automated relay posts naming Qatari government sites (B12)

CLAIMED TARGETS

Government sites

IN THEIR WORDS

> *"it may be down for you at the moment"* B12

SEEN IN PUBLIC REPORTING

- [S28] Unit 42: a pro-Iran hacktivist group conducting DDoS attacks across the Middle East
- [S29] CloudSEK: attribution self-reported, technical validation limited
- [S34] DailyDarkWeb (6 Mar): claimed sites temporarily inaccessible; no confirmation

OUR ASSESSMENT

A regional DDoS claimant whose Qatar claims reach us through automated relays. The relays record timed-out checks, not outages.

CONFIDENCE **Medium that DieNet made the claims (relayed); impact unverified**

313 Team

Self-styled "Islamic Cyber Resistance in Iraq" (name as reported by Unit 42)

Hacktivist (DDoS) | Pro-Iranian hacktivist cell (per Unit 42)

IN QATAR, 2026

14 Mar	Claims a government portal disabled for one hour (B11)
15 Mar	Update: claims several more hours offline

CLAIMED TARGETS

A government portal

IN THEIR WORDS

> *"completely disabling the website"* B11

SEEN IN PUBLIC REPORTING

- [S28] Unit 42: an active pro-Iranian hacktivist cell that claimed attacks on Kuwaiti armed forces, defence ministry and government websites

OUR ASSESSMENT

A repeat regional claimant. Its Qatar posts link to the same stresser brand as Keymous Plus; that is a shared service, not proof of a shared operator.

CONFIDENCE **High that it made the claim; impact unverified**

BD Anonymous Team

BD Anonymous

Hacktivist (DDoS)

Framed its actions around geopolitical grievances (per CloudSEK)

IN QATAR, 2026

28 Feb-1 Mar	Self-reported DDoS on a ministry's online service (CloudSEK)
19 Jun	Claims a security force's website taken down (B13)

CLAIMED TARGETS

Ministry and security websites

IN THEIR WORDS

> *"We have successfully took down"* B13

SEEN IN PUBLIC REPORTING

- [S29] CloudSEK: targeted a ministry's online services with DDoS activity; attribution self-reported

OUR ASSESSMENT

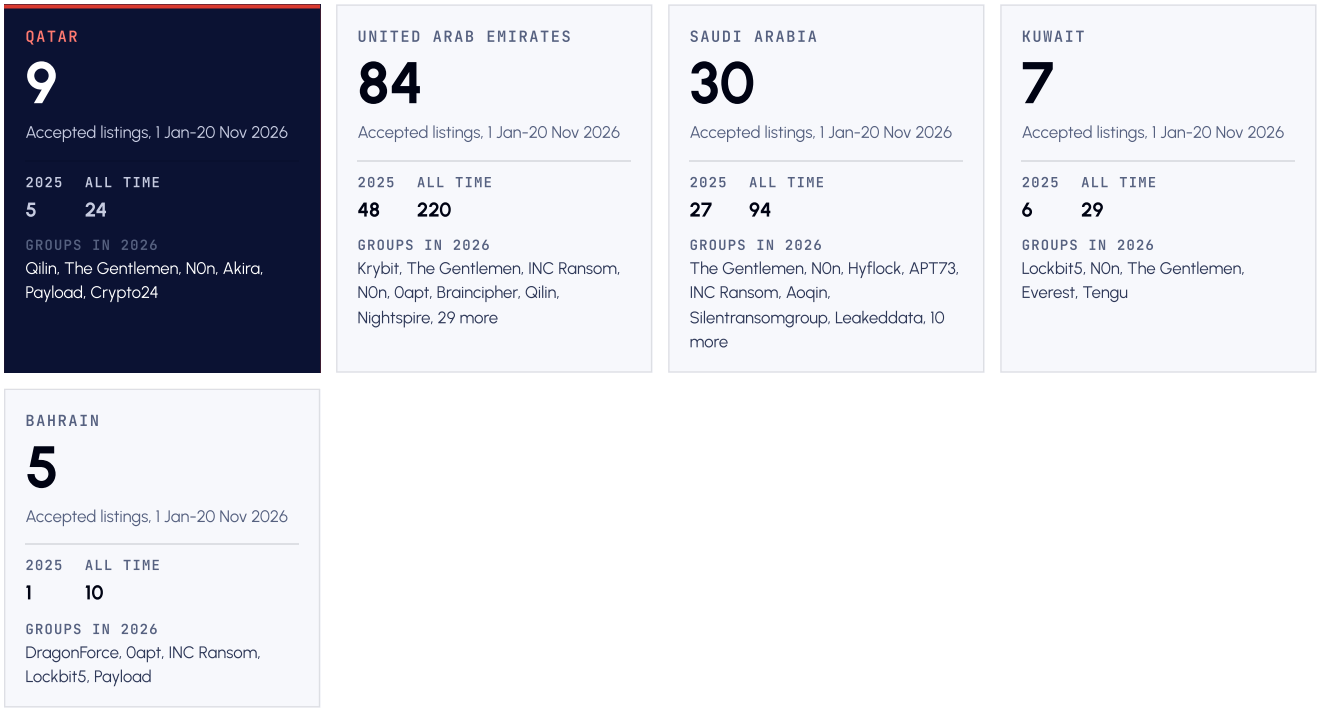
A small claimant with two Qatar episodes. The June claim cites a stated political motive; we report it as the group's own.

CONFIDENCE **Medium that it made the claims; impact unverified**

Not counted as hacktivism. Several Telegram channels posted claims about physical damage to Qatari energy facilities during the escalation. They are commentary on the escalation, not cyber claims, and we exclude them.

7.4 Ransomware and extortion

Nine Qatari ransomware listings in 2026, against 84 in the UAE, 30 in Saudi Arabia, seven in Kuwait and five in Bahrain



Source: Brandefense Ransompedia accepted listings, all dates, to 20 November 2026 [S6]; ransomware.live as a cross-check [S7].

Ransompedia holds nine accepted listings for Qatar dated 1 January–20 November 2026, naming eight distinct organisations; one construction firm was listed twice [S6]. Qilin posted three of the nine, The Gentlemen two, and Akira, Crypto24, N0n and Payload one each. Ransompedia's sector labels for the nine listings are construction (two), consulting, engineering consulting, legal consulting, telecommunications, technologies, manufacturing and one unclassified. Its labels do not always match our description of an organisation, such as the research institute named below. In the same window Ransompedia holds 84 listings for the UAE, 30 for Saudi Arabia, seven for Kuwait and five for Bahrain.

Cross-check. A public tracker lists seven Qatari victims in 2026 [S7]. Its seven entries correspond to seven of Ransompedia's nine listings; it does not hold the other two. Relay channels also tagged two further claims as Qatari, one naming a small company we do not identify; Ransompedia does not hold them as Qatari listings, so we do not count them. The tracker also files one listing under another country that concerns a company we place in Qatar. That is a ninth organisation (§5), which we count outside Ransompedia's eight. Relay channels in our corpus repeated the same claims.

What this means. A listing is an extortion group's claim, not a confirmed intrusion. Ransomware claims against Qatar in 2026 named a telecom infrastructure company, a research institute, a law firm and several contractors. Contractors and consultancies, of the kind that often serve energy and government, are part of the exposure. Unpublished and negotiated incidents are invisible here.

7.5 Criminal personas seen in Blackhole



IN QATAR, 2026

10 Mar — Claims a database dump of an energy-sector company and a wiped server (B02)

CLAIMED TARGETS

An energy-sector company

IN THEIR WORDS

> *"WE DONT CARE ABOUT THE POLITICS WE CARE ABOUT THE PAYOUT"* B02

SEEN IN PUBLIC REPORTING

OUR ASSESSMENT

No reputable public reporting found. Its claim followed a different poster's claim against the same company by three weeks (Case A).

CONFIDENCE **High that it made the claim; claim unverified**

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

Persona or brand	Observed role in 2026	Own claim	Unresolved
Montaro (per a public monitor)	Energy-sector access claim (Feb)	Cloud and identity access	Whether it wrote the forum post (Case A)
ELIPHAS SYNDICATE	Telegram seller (Mar)	Energy-sector database dump; server wiped	Any sample; link to Montaro
TheAshborn	Breach-forum seller (Mar)	Security-body personnel data	Origin of the data (Case B)
UNC6783 (self-applied channel name)	Breach-forum seller (Nov)	Bank customer records	Any verification (Case C); the name is the seller's own label
REDxVerified	Second forum seller of the same bank offer (Nov)	Same offer, same price	Whether one seller
X FORUMS (bot)	Automated uploader of small files, including Qatari domains	None	Not a person; a distribution bot
Miles shops (several channels)	Sellers of airline loyalty accounts, including a Gulf carrier's	Accounts "with email access"	Account owners; whether accounts are hijacked

7.6 Advisories from the national agency

NCSA's public advisory feed is the clearest official signal of what defenders in Qatar were asked to patch. We counted 163 dated advisories between 11 January and 19 November 2026 [S43]. By our reading of their titles, 65 mention active exploitation or a zero-day, and 49 concern network, remote-access or security products from vendors such as Cisco, Fortinet, Citrix, Ivanti, Palo Alto Networks and SonicWall. In March NCSA also warned iPhone users about actively exploited iOS flaws, naming iOS 13 and 14 as specifically targeted [S38].

KEY TAKEAWAYS

01 — Check Point attributed one 2026 espionage campaign against Qatari targets to Camaro Dragon and assessed a second as China-aligned with low confidence.

02 — Two hacktivist groups promote the same stresser; a shared service is not a shared operator.

03 — Ransomware claims named contractors and infrastructure suppliers more than large household names.

CHAPTER 8

The fraud economy

THIS CHAPTER ANSWERS

How do criminals turn Qatari identities, accounts and cards into money, and what did the authorities warn about?

32 USD

median asking price for a bank or wallet account in cleaned posts

INSIDE THIS CHAPTER

8.1 Bank, wallet and platform accounts | 8.2 Card material in posts: a narrow view | 8.3 Loyalty and email accounts | 8.4 Payment links and brand scams

8.5 Identity, KYC and telephony services | 8.6 Prices in context | 8.7 What the authorities warned about

IN SHORT

Qatar appears in the underground mainly as a market. Sellers list Qatari cards, Qatar-registered trading and email accounts, and airline loyalty accounts alongside dozens of other countries. Authorities warned repeatedly about messages impersonating government bodies, the tax authority and well-known companies. Confirm payment instructions out of band, protect loyalty and email accounts with strong MFA, and assume impersonation will follow every major news event.

8.1 Bank, wallet and platform accounts

Account trading is a large cleaned family (1,635-1,756 posts), but it needs careful reading. Many account-rental posts concern a Turkish bank rather than a Qatari one. The Qatar-specific posts are different. Buyers ask for "ready-made" accounts on foreign trading platforms registered to Qatari identities, typically for 25-40 USD each. Such accounts let a buyer move money under someone else's verified identity. The posts show demand and offers; they do not show that any account was opened at a Qatari institution.

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 Qatar.

Within that narrow scope, 110 distinct Qatar-associated cards appeared in clear text in collected posts. Of these, 85 were attributed to one of seven named Qatari banks, and the other 25 were labelled only as Qatari, without an issuer. 81 of the 110 appeared in card-checker output. No card data is published in this report (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 Loyalty and email accounts

"Miles shops" on Telegram advertised airline and hotel loyalty accounts in 2026, listing point balances and "full email access". A Gulf carrier's programme appeared in dozens of these posts beside other airlines [S1]. The offer of email access matters most. If genuine, it suggests the seller controls the mailbox used to reset the account, which is consistent with stolen credentials or stealer logs rather than a breach of the airline. Loyalty points are converted into tickets and vouchers that are hard to claw back.

EVIDENCE CARD B14 1 Jan 2026

Miles shop Loyalty-account shop channel · Telegram · English

ORIGINAL

```
[Gulf carrier] 310k point available with email access.
Escrow
```

HELD	An offer of a loyalty account with a point balance and access to the linked mailbox; similar offers recur through the year.
NOT ESTABLISHED	Whose account it is, or how it was obtained.

8.4 Payment links and brand scams

Card cashers also misuse legitimate Qatari payment pages. In March a channel shared a public bill-payment page as a route to spend stolen cards. In September and October sellers offered invoice links from a Qatari payment gateway to "loaders" at 65-70% of face value [S1]. Sellers in May and June offered scam pages styled on a large Qatari bank, and in April a fake investment platform used the same bank's name. The pages and links are real services; the abuse is in who pays and with what card.

8.5 Identity, KYC and telephony services

KYC and document posts (534-567 cleaned) offer verification services, document templates and accounts verified with Qatari identities. Telephony sellers list Qatar among the destinations for SMS sending, caller-ID spoofing and one-time-password bots. Combined with the identity datasets in §4.4, these services lower the cost of impersonating residents and organisations.

8.6 Prices in context

Product (cleaned posts)	Median asking price	Spread
Card (per card)	14 USD	10-25 USD
Data or lead offer	15 USD	10-30 USD
Combolist	27 USD	15-35 USD
Bank, wallet or platform account	32 USD	25-60 USD
KYC or document service	50 USD	20-100 USD
Access offer	171 USD	Wide, 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. Single offers sit outside it, such as the 10,000 USD security-body file and the 1,500 USD bank file in Chapter 4.

8.7 What the authorities warned about

The posts show offers. The warnings below describe what Qatari authorities saw and told the public; all were published in 2026.

Date	Reported by	What it said
3 Feb	National Cyber Security Agency	Binding decision (No. 3 of 2025) against a sports-sector company after a personal-data breach, for inadequate protection measures [S25]

Date	Reported by	What it said
26 Feb	General Tax Authority	Coordinated phishing emails and SMS impersonating the authority, with refund, detail-update and account-verification lures [S36]
22 Mar	National Cyber Security Agency	Actively exploited iOS flaws; older iOS 13 and 14 devices specifically targeted; update immediately [S38]
24 Mar	Ministry of Interior	Calls and messages impersonating government agencies to obtain bank details, transfers and one-time codes [S35]
19 Sep	National Cyber Security Agency	Fraudulent SMS and emails impersonating government entities and major companies [S45]
28 Sep	Ministry of Interior	Fake websites copying the colours, fonts and designs of well-known companies; online extortion carries up to three years in prison [S37]
3 Nov	Communications Regulatory Authority	New .qa registry policies from 22 October to reduce domain misuse, impersonation and phishing [S39]

What this tells defenders. The official warnings and the underground offers describe the same weak point: trust in a familiar name. Government bodies, the tax authority and big brands are imitated by SMS, email, calls and lookalike websites. In April 2025 Silent Push listed Qatar among the countries targeted by the China-based smishing operation it calls Smishing Triad [S46]. The controls are procedural and technical: out-of-band confirmation of payment instructions, phishing-resistant MFA, brand and domain monitoring, and public warnings that name the real channels.

KEY TAKEAWAYS

01

Qatar is mostly a market in the posts we collected: cards, verified accounts and loyalty accounts are sold alongside many other countries.

02

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

03

Impersonation of government bodies and big brands is the fraud pattern authorities warned about most.

CHAPTER 9

Banking and finance deep dive

THIS CHAPTER ANSWERS

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

9 of 9

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

IN SHORT

Every one of the nine card-issuing banks on our list had a credential tied to its domain listed for sale on the day of the check. Most other visible exposure is most plausibly on the customer side: 4,415 non-employee device associations and card-checker activity. The staff-side signal is small: 64 employee-classified devices at six banks. Triage each current credential listing first, then validate employee devices, and monitor checker declines on your BIN ranges.

This chapter covers the nine card-issuing banks among the 30 banking-and-finance organisations in Chapter 3; the other 21 are the central bank, market infrastructure, exchange houses, investment firms and payment providers. That is why 4,415 non-employee devices here differs from 5,257 for the whole sector, and 9 of the sector's 12 organisations with a current listing are issuers. Aggregates only; individual banks are not named.

9 of 9

card-issuing banks with a current credential listing (9 of the sector's 12 organisations with a current listing)

9 of 9

issuers with non-employee device associations (4,415 in total; ownership and current infection unverified)

6 of 9

issuers with employee-classified devices (64 in total)

8 of 9

card-issuing banks enforcing DMARC (16 of 30 across the sector)

7 of 9

card-issuing banks with cards in clear text in collected posts (85 of the 110 cards name one of them; narrow scope, §8.2)

The top three issuers account for 71% of the attributed cards and 85% of the non-employee device associations.

What it means for banks.

1. **Current listings come first.** All nine issuers had one on the day of the check; apply Decision 1 (disposition within 5 working days).
2. **Employee exposure is small but real.** 64 employee-classified devices across six banks 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.** 4,415 device associations 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. 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 on merchant gateways. Issuers can detect clusters of declined low-value attempts from foreign gateways on their BIN ranges, check the authorisation and fraud signals of the cards involved, and reissue those confirmed at risk under issuer policy.
5. **A recurring data claim needs a prepared answer.** One large bank was named in data offers in April, August and November (Case C). Banks should be able to compare a claimed schema with their own exports within a day and to brief customers if a sample is confirmed.

Sector resilience work is under way. Qatar Central Bank ran its first sector-wide Cyber Resiliency Exercise, according to coverage of its 2025 Financial Stability Review [S41]. Banks also operate under its Cloud Computing Regulation, issued in April 2024 [S23].

KEY TAKEAWAYS

01

Current credential listings at all nine card issuers come first, then the 64 employee-classified devices; the 4,415 non-employee ones also need validation.

02

Card issuers enforce DMARC widely (8 of 9); the other finance organisations mostly do not (8 of 21).

03

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

CHAPTER 10

Regulatory and national response

THIS CHAPTER ANSWERS

Which Qatari rules set reporting clocks for a cyber incident, and what should an organisation have in place before the next one?

72 h

to notify a serious personal-data breach under NCSA privacy guidance

INSIDE THIS CHAPTER

10.1 What we could verify | 10.2 The privacy regime is enforced | 10.3 Which clocks apply to you

IN SHORT

Qatar's cyber rules sit mainly with the National Cyber Security Agency (NCSA): a national strategy, a baseline standard and, from October 2026, national and enterprise risk frameworks. Several clocks can run at once after one incident. They include 72 hours for a serious personal-data breach under NCSA guidance, and reporting duties under the national standard and the 2026 frameworks whose deadlines this edition could not confirm. Map which clocks apply, obtain unconfirmed deadlines from NCSA in writing, and name who starts each one.

10.1 What we could verify

The table lists the instruments we checked, with the duties that matter most during an incident. The caution column marks what this edition could not confirm.

Measure	What we could verify	Status and caution
National Cyber Security Agency	Established by Amiri Decision No. (1) of 2021, dated 14 March 2021 and published 24 March 2021. Its listed competences include the national strategy, standards and compliance, classifying critical-sector institutions, the national incident response plan, licensing of cybersecurity service providers and implementing personal-data privacy law [S14]	State entities must cooperate with the agency and remain responsible for protecting their own systems [S14]
National Cyber Security Strategy 2024-2030	Five pillars, from resilience of critical national infrastructure to international cooperation, monitored by a strategy office within NCSA [S15]	A strategy, not a duty in itself; duties come from the standards below
National Information Assurance Standard (V2.1, May 2023)	In our reading, the standard states that baseline controls "are mandatory and must be implemented". Control IM 8 sets a deadline for reporting Critical incidents to NCSA [S16]	The IM 8 deadline is not confirmed in this edition; obtain it in writing from NCSA. Assets must first be classified under the national data classification policy [S16]
National and Enterprise Information Security Risk Management Frameworks (V1.0)	Launched on 5 October 2026 [S18]. In our reading of the framework text, adoption is "strongly encouraged" and the frameworks include reporting risks to NCSA and an annual attestation [S17]	The reporting duties and their timing are not confirmed in this edition; obtain written clarification from NCSA. The text does not make clear whether the reporting duty applies beyond adopting entities. New in 2026; expect guidance on scope and format to follow
Controls for financial-market participants (V1.0, March 2026)	Supplementary controls to the national standard for entities regulated by the Qatar Financial Markets Authority, announced with a compliance programme [S17][S18]	Applies to market participants, not to every financial firm; confirm the version with NCSA

Measure	What we could verify	Status and caution
Cybercrime Prevention Law No. (14) of 2014	Unlawful access carries up to three years and QAR 500,000; online threats and extortion up to three years and QAR 100,000; a legal person can be fined up to QAR 1,000,000. State bodies and their companies must report offences "immediately upon discovery" and keep IT data for at least 120 days; service providers keep subscriber information for one year [S19]	Law No. (11) of 2025 added an offence on publishing images of people in public places without consent [S20]
Personal Data Privacy Protection Law No. (13) of 2016	A controller must inform the individual and the competent department of a breach that may cause serious damage. Fines reach QAR 1,000,000 or QAR 5,000,000 depending on the article breached [S21]	The law sets no hour limit; NCSA guidance sets 72 hours for serious breaches [S22]. NCSA acts as the competent authority [S21]
QCB Cloud Computing Regulation	Issued in April 2024 for QCB-licensed entities, to govern their use of cloud services [S23]	Its data-location and prior-approval duties are not confirmed in this edition; check them, and QCB's related data-handling rules, with QCB. Read with QCB incident-reporting instructions for banks, whose timelines annex we could not read
QFC Data Protection Regulations 2021	Under Article 31, a data controller must notify the QFC Data Protection Office of a personal-data breach within 72 hours. The exception is where the controller determines the breach is unlikely to risk data subjects' rights and legitimate interests [S24]	The duty sits with the controller; processors' and other parties' duties are not covered here. A separate regime from the national privacy law
.qa domain registry policies	Updated policies took effect on 22 October 2026, with clearer eligibility rules aimed at reducing domain misuse, impersonation and phishing [S39]	Lookalikes under other top-level domains are not covered

10.2 The privacy regime is enforced

In February 2026 NCSA's privacy office announced a binding decision (No. 3 of 2025) against a sports-sector company after a personal-data breach. It found inadequate technical, administrative and physical protection measures under Articles 8(3), 13 and 14 of the privacy law, and ordered the company to review and strengthen them [S25]. The company was not named. According to the report, the breach was detected by the agency's own specialised teams [S25]. For organisations, the lesson is that the privacy regulator acts on breaches it identifies itself, not only on complaints.

10.3 Which clocks apply to you

Several reporting clocks can start from one event. The table reads the instruments above for four common cases. It is a planning aid, not legal advice.

Organisation	Clocks to plan for	Action now
State body or state-owned company	Critical incident to NCSA within the national-standard deadline (obtain it in writing from NCSA) [S16]; immediate report of a cybercrime offence [S19]; risk reporting under the 2026 frameworks (scope and timing unconfirmed; obtain clarification from NCSA) [S17]; serious personal-data breach within 72 hours [S22]	Name one incident reporter for all four, with a deputy
QCB-licensed bank or payment provider	QCB incident reporting (timeline not verified); privacy breach within 72 hours where serious [S22]; QCB cloud and data rules (duties to confirm with QCB) [S23]	Map the QCB and NCSA routes in one playbook
QFC firm	As controller, the QFC Data Protection Office within 72 hours, unless the breach is unlikely to put data subjects' rights at risk [S24]	Record the risk assessment behind any decision not to notify; confirm which privacy regime covers each data set
Any other organisation holding personal data	Serious personal-data breach within 72 hours [S22]; NCSA standard where it applies to you [S16]	Keep a breach register and a pre-filled notification draft

What CISOs should do now. Confirm in writing which instruments apply to your organisation and your sector regulator. Name the person who reports to NCSA, to the privacy regulator and, for financial firms, to QCB or the QFC office. Rehearse the Critical-incident clock, because classifying an incident as Critical and reporting it inside the deadline needs a decision path that already exists. Keep dated records of controls, because the 2026 frameworks will bring further guidance.

KEY TAKEAWAYS

01

Plan for several clocks: 72 hours for a serious personal-data breach, the Critical-incident deadline and the 2026 risk-framework duties; obtain the last two deadlines in writing from NCSA.

02

The privacy regulator announced in February 2026 a binding decision (No. 3 of 2025) after a breach its own teams identified.

03

Banks face QCB rules on top, including its 2024 cloud regulation; confirm its data-location duties with QCB.

CHAPTER 11

Outlook

THIS CHAPTER ANSWERS

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

5
key judgements, each with a signal to watch

INSIDE THIS CHAPTER

11.1 Key judgements | 11.2 What would change the assessment | 11.3 Conditional scenarios

IN SHORT

Plan for the same evidence types, not a new threat: identity exposure that stays invisible until it is used, news-driven hacktivist DDoS, espionage lures in attachments, and recurring data claims against large employers. 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 Qatar's leading organisations	High for the 250-organisation list	182 with devices, 213 with credential records, 73 with current listings; not national prevalence
If a major regional event recurs, plan for a burst of hacktivist DDoS claims against state websites within days	Medium (planning assumption)	Four groups claimed in March 2026, starting within a day; claims unconfirmed; signal: target lists in actor channels
If escalation or crisis themes dominate, plan for espionage lures against government and energy within a day	Medium (planning assumption)	Two vendor-reported campaigns in March 2026; small sample; signal: vendor advisories
Plan for further data claims naming large Qatari employers and data holders	Medium (planning assumption)	Sixteen specific offers in 2026, two repeated; authenticity unverified; signal: new offers in monitored venues
Ransomware listings will keep naming contractors and suppliers more than household names	Medium for observed listings	9 listings in 2026, mostly mid-sized firms; unpublished incidents invisible

11.2 What would change the assessment

Current interpretation	Evidence that would change it	Decision affected
Data claims against energy, banking and security bodies are unverified	A sample matched to a specific system's schema, or an official confirmation	Trigger notification and customer- or staff-protection actions for that dataset
Hacktivist figures exceed what anyone confirmed	Official confirmation of a sustained outage of a critical service	Revisit upstream mitigation capacity and service-continuity plans
Current listings mean "validate", not "breached"	Validation shows a listed credential or session still works, or finds unauthorised access, with or without MFA	Escalate to incident response; revoke sessions, reset credentials and enforce MFA for the affected population
Espionage evidence is two vendor-reported campaigns	Further vendor or official reports of intrusions at Qatari government or energy bodies	Fund mail, endpoint and identity telemetry ahead of other projects

Current interpretation	Evidence that would change it	Decision affected
Ransomware claims name mostly mid-sized firms	A listing that names a critical-infrastructure operator with a confirmed outage	Run the restore test in §12.1 first and review supplier access

11.3 Conditional scenarios

- **If** a new regional escalation or high-profile event involving Qatar dominates the news, **then** plan for DDoS claims against state websites and impersonation fraud in the same week. This is a planning assumption, not a measured interval; **signal:** target lists in actor channels and official fraud warnings. **Decision:** activate the pre-agreed communication line, upstream mitigation and a customer fraud warning together.
- **If** a new critical flaw in a network or remote-access product is disclosed, **then** plan for exploitation attempts at government, energy and telecom organisations; **signal:** an NCSA advisory marking the flaw as actively exploited. **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, news-driven DDoS, espionage lures and recurring data claims.

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

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

INSIDE THIS CHAPTER

12.1 30/60/90 days | 12.2 By role | 12.3 How Brandefense can help

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, exposed tokens and mail attachments. Then close the phishing, payment-approval, email and DNS gaps, and rehearse a DDoS burst combined with a data claim. 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.

1 Days 1-30

Confirm that you receive credential-listing and infected-device alerts for your primary domains; if not, arrange them; until alerts arrive, review remote-access sign-ins for new devices and enforce MFA for remote access

OWNER
CISO and threat intelligence

COMPLETION EVIDENCE
Alert source named and first alert received, or sign-in review recorded and MFA enforced for remote access

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

2 Days 31-60

Where DMARC is p=none or missing, 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 and payment pages

OWNER
Infrastructure and procurement

COMPLETION EVIDENCE
Mitigation test record

Review privileged directory roles, cloud keys in application settings and accounts on building-security systems (Case A)

OWNER
Identity and infrastructure

COMPLETION EVIDENCE
Review recorded; unused privileged roles removed

3 Days 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

Register lookalike and impersonation monitoring for your brand, and publish your real contact channels

OWNER
Brand and communications

COMPLETION EVIDENCE
Monitoring live; channels page published

Run a tabletop combining a DDoS burst with a simultaneous data-leak claim, including the Critical-incident reporting decision

OWNER
CISO, communications, legal

COMPLETION EVIDENCE
Decision log and timings

Report the scorecard against targets (below)

OWNER
CISO to board

COMPLETION EVIDENCE
Board paper with remaining gaps and owners

Block archive and shortcut attachments from external senders, and alert on signed programs loading DLLs from user folders (§7.2)

OWNER
Messaging and SOC

COMPLETION EVIDENCE
Mail policy changed; alert tested with an authorised sample

Rotate any application token, key or password seen in a public post or sample naming your organisation (Case E)

OWNER
Application owners

COMPLETION EVIDENCE
Rotation logged; old values rejected

Name the person and deputy who report to NCSA, the privacy regulator and, for financial firms, QCB or the QFC office (§10.3)

OWNER
CISO and legal

COMPLETION EVIDENCE
A one-page playbook naming each clock and reporter, approved

Name the spokesperson and channel for service-status statements during DDoS

OWNER
Communications

COMPLETION EVIDENCE
Statement templates approved

Review supplier remote access, including building-security and school-management providers

OWNER
Third-party risk

COMPLETION EVIDENCE
Supplier access list with owners and expiry dates

Move privileged and remote users to phishing-resistant MFA (FIDO2 security keys, passkeys or certificate-based sign-in)

OWNER
Identity team

COMPLETION EVIDENCE
Coverage recorded per user group

Require out-of-band confirmation for payment-instruction and payee changes, including requests that cite an official body

OWNER
Finance and fraud

COMPLETION EVIDENCE
Procedure signed off; one simulated request caught

Add MFA and redemption alerts to loyalty and customer accounts

OWNER
Digital and fraud teams

COMPLETION EVIDENCE
Alert live; MFA coverage recorded

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)

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
External archive and shortcut attachments blocked	In place by day 30
Primary domains with DMARC at quarantine or reject	100%, or a dated plan, by day 90
Privileged and remote users on phishing-resistant MFA	100%, or a dated plan, by day 90

Measure	Target
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

The national cyber drill gives a ready rehearsal date: NCSA scheduled its 13th drill for 30 November 2026, with more than 150 entities in 14 sectors [S40].

12.2 By role

Role	First decision
Board	Ask for the current-listing and employee-device numbers for your organisation and the date by which each is validated, and confirm the monitoring that produces them
CISO	Put listing and device monitoring in place first, then the attachment controls and the reporting-clock playbook
SOC	Add detections for archive and shortcut execution, signed binaries loading DLLs from user folders, Cobalt Strike beacons and sign-ins from new devices to VPN and remote desktop
Fraud	Use device and session risk at login and payee changes; monitor clustered card-checker declines on your BINs; warn customers about impersonation of government bodies
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 and block external archive attachments in the first 30 days.

02

Stage DMARC, phishing-resistant MFA and payment-change controls by day 60; report the scorecard by day 90.

03

Rehearse a DDoS burst combined with a data claim, including the Critical-incident reporting decision.

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

Appendix A. Method

A.1 Window, sources and priority

The research window is 1 January–20 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 only after the supporting passage was read. Data were extracted on 21 November 2026. Sources S1–S6 and S8 are Brandefense's own data and have no public address; every external source in Appendix C carries a link and the date we opened it.

A.2 Blackhole posts

Item	Value
Posts with the Qatar country tag	55,241
Posts after cleaning	7,867–8,175 (a range, not a point estimate)

Spam and automated posts are set aside before analysis. Many remaining posts are multi-country lists, so cleaned counts are still an upper bound for criminal activity concerning Qatar.

Three collection limits shape every trend in this report. We do not compare post categories across the year. Collection appears lower from mid-year, so we do not read declines as threat trends. And some posts that mention Qatar are unrelated: posts about a Turkish bank, and posts using the Arabic word for Qatar in its other sense, "diameter".

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. Device, credential and listing counts were read on 21 November 2026.

A.4 Atlas ratings

Each organisation received an Atlas exposure rating from these signals, and the list as a whole a single headline score. Treat a current credential-market listing as a reason to validate accounts, not as proof of a breach.

A.5 DNS, TLS and web checks

We made public DNS queries for mail, SPF, DMARC, DKIM and DNSSEC 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.

Only aggregate counts by issuer are reported; no card data is published.

A.7 Ransomware

We used Ransompedia accepted listings for Qatar, the United Arab Emirates, Saudi Arabia, Kuwait and Bahrain, all dates, dated by publication. A public tracker and relayed Blackhole posts are used only as cross-checks.

A.8 Incident coverage

Incidents in this report were checked against Blackhole data and public reporting, including national press, official agency pages, vendor research and public monitoring accounts.

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.
- Arabic dialect and slang may be misread.
- Several official and press websites, and parts of the Arabic-language press, could not be read directly.
- 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 or company is named only where an official statement confirms the incident and it was widely reported. 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, tokens, samples 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	2026-02-19	Breach forum	Unnamed poster	English	§4.4
B02	2026-03-10	Telegram channel	ELIPHAS SYNDICATE	English	§4.4
B03	2026-03-10	Breach forum	TheAshborn	English	§4.4
B04	2026-11-10	Breach forum	UNC6783 (self-applied)	English	§4.5
B05	2026-08-26	Telegram relay of a forum listing	Security news relay	English	§4.5
B06	2026-06-08	Breach forum	Unnamed poster	English	§4.5
B07	2026-09-03	Forum	Unnamed poster	English	§4.5
B08	2026-09-03	Forum, same text on Telegram	Anonymous buyer	English	§4.5
B09	2026-03-03	Actor channel	Keymous Plus	English, as posted	§6.3

Card	Posted	Venue	Alias as shown	Language	Shown in
B10	2026-03-12	Actor channel	Keymous Plus	English, as posted	§6.2
B11	2026-03-14	Actor channel	313 Team	Arabic, with the group's own English	§6.2
B12	2026-03-06	Relay channel of an automated tracking bot	DieNet (relayed)	English	§6.3
B13	2026-06-19	Actor channel	BD Anonymous Team	English, as posted	§6.3
B14	2026-01-01	Loyalty-account shop channel	Miles shop	English	§8.3
B15	2026-03-24	Actor channel	Keymous Plus	English, as posted	§6.3
B16	2026-07-22	Telegram relay of a forum listing	Security news relay	English	§4.4
B17	2026-03-09	Telegram channel	Data seller	Arabic, with the seller's own Russian and English	§4.4
B18	2026-05-16	Forum	Unnamed poster	English	§4.5

Appendix C. Sources

S1 Brandefense Blackhole posts concerning Qatar, post dates 1 January–20 November 2026, extracted 21 November 2026.

S2 Brandefense Blackhole posts of hacktivist channels and relay channels naming Qatari targets, 28 February–19 June 2026.

S3 Brandefense Blackhole infected-device, breach-database, stealer-log and combolist associations for 250 domains, as held on 21 November 2026.

S4 Brandefense Atlas exposure ratings and signals for the 250 domains, 21 November 2026, including credential-market listings, lookalike domains, exposed documents and mentions.

S5 Brandefense public DNS, TLS and homepage checks of the 250 domains, 21 November 2026.

S6 Brandefense Ransompedia, accepted listings for Qatar, the United Arab Emirates, Saudi Arabia, Kuwait and Bahrain, all dates, extracted 21 November 2026.

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

S8 Brandefense Blackhole, aggregate counts of Qatar-associated cards seen in clear text in collected posts, 21 November 2026.

S9 DataReportal (Kepios), *Digital 2027: Qatar*, 5 November 2026 (data for October 2026). https://datareportal.com/reports/digital-2027-qatar. Verified on 21 November 2026.

S10 Qatar News Agency, "Qatar achieves one of the world's highest scores in ITU ICT Development Index 2026", 24 August 2026, citing the Communications Regulatory Authority. https://qna.org.qa/en/News-Area/News/2026-8/24/qatar-achieves-one-of-the-worlds-highest-scores-in-itu-ict-development-index-2026. Verified on 21 November 2026.

S11 US Energy Information Administration, Qatar country analysis brief, last updated 20 October 2025. https://www.eia.gov/international/analysis/country/QAT. Verified on 21 November 2026.

S12 Hamad International Airport, press release on 2025 operational performance, 21 January 2026. https://dohahamadairport.com/press-releases/news/2025-operational-performance. Verified on 21 November 2026.

S13 Qatar Central Bank, "Retail Payment Systems" (undated page). https://www.qcb.gov.qa/en/Pages/Retail-payment-systems.aspx. Verified on 21 November 2026.

S14 Amiri Decision No. (1) of 2021 establishing the National Cyber Security Agency, dated 14 March 2021, Official Gazette 24 March 2021. Official text on Al Meezan: https://almeezan.qa/legislations/16ffa013-351b-4a84-8b03-7752c25ce4f1. Verified on 21 November 2026.

S15 National Cyber Security Agency, National Cyber Security Strategy 2024–2030 (page and strategy document). https://www.ncsa.gov.qa/en/national-cyber-security-strategy. Verified on 21 November 2026.

S16 National Cyber Security Agency, National Information Assurance Standard, version 2.1, May 2023. https://www.ncsa.gov.qa/en/publications (document library). Library page accessed 21 November 2026; document text not confirmed in this edition.

S17 National Cyber Security Agency, National and Enterprise Information Security Risk Management Frameworks, version 1.0 (2026). Also its controls for financial market participants, version 1.0 (March 2026). https://www.ncsa.gov.qa/en/publications (document library). Library page accessed 21 November 2026; document text not confirmed in this edition.

S18 National Cyber Security Agency, "NCSA Organizes the Fifth Annual Cyber Governance and Assurance Conference", 5 October 2026. https://www.ncsa.gov.qa/en/media/news/x-551750. Verified on 21 November 2026.

S19 Law No. (14) of 2014 Promulgating the Cybercrime Prevention Law, dated 15 September 2014, Official Gazette 2 October 2014. Official text on Al Meezan: https://almeezan.qa/legislations/71b9f8f2-61dc-44b9-825d-b16c490ed583. Verified on 21 November 2026.

S20 Law No. (11) of 2025 amending certain provisions of the Cybercrime Prevention Law, dated 21 July 2025, Official Gazette 4 August 2025. Official text on Al Meezan: https://almeezan.qa/legislations/2af771cb-8553-4a91-ab94-1f6fede99cf9. Verified on 21 November 2026.

S21 Law No. (13) of 2016 on Personal Data Privacy Protection, dated 3 November 2016, Official Gazette 29 December 2016. Official text on Al Meezan: https://almeezan.qa/legislations/9c7dca4b-8722-4212-9368-ea3abba0c95c; penalty articles read in the National Cyber Security Agency's English text, which it marks as unofficial, and its PDPPL page https://www.ncsa.gov.qa/en/pages/personal-data-privacy-personal-data-privacy-protection-law. Verified on 21 November 2026.

S22 National Cyber Security Agency, "Personal Data Breach Notifications: Guidelines for Regulated Entities", version 2.0, September 2022. https://www.ncsa.gov.qa/en/pages/personal-data-breach-notification. Verified on 21 November 2026.

S23 Qatar Central Bank, Cloud Computing Regulation, issued April 2024. https://www.qcb.gov.qa/Documents/InformationSecurity/Cloud%20Computing%20Regulation.pdf. Verified on 21 November 2026.

S24 Qatar Financial Centre, Data Protection Office, "Data Protection Regulations and Rules 2021 Guidance", data-protection page and personal-data breach reporting form (citing Article 31 of the Data Protection Regulations 2021). https://www.qfc.qa/en/operate/data-protection/ and https://www.qfc.qa/media/stxham4h/qfc_data_protection_breach_reporting_form.pdf. Verified on 21 November 2026.

S25 Gulf Times, "National Cyber Security Agency takes action against sports sector firm over data breach", 3 February 2026. https://www.gulf-times.com/article/719867/qatar/national-cyber-security-agency-takes-action-against-. Verified on 21 November 2026.

S26 Check Point Research, "China-nexus activity against Qatar observed amid expanding regional tensions", 9 March 2026. https://blog.checkpoint.com/research/china-nexus-activity-against-qatar-observed-amid-expanding-regional-tensions/. Verified on 21 November 2026.

S27 Check Point Research, weekly Threat Intelligence Report, 16 March 2026. https://research.checkpoint.com/2026/16th-march-threat-intelligence-report/. 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 CloudSEK, situation report on the Middle East escalation and cyber activity, 2 March 2026. https://www.cloudsek.com/blog/middle-east-escalation-israel-iran-us-cyber-war-2026. Verified on 21 November 2026.

S30 Intel 471, blog on the surge in hacktivist activity after the start of the regional escalation, 9 March 2026. https://www.intel471.com/blog/israeli-us-strikes-against-iran-triggers-a-surge-in-hacktivist-activity. Verified on 21 November 2026.

S31 StormWall, "Q1 2026 DDoS report: MENA" (undated page). https://stormwall.network/resources/blog/q1-2026-ddos-report-mena. Verified on 21 November 2026.

S32 NETSCOUT, Threat Intelligence Report, country page for Qatar, January-June 2026. https://www.netscout.com/threatreport/country/qatar/. Verified on 21 November 2026.

S33 The National, "Iranian cyber attacks move from disruptive to complex threats in Gulf", 10 April 2026. https://www.thenationalnews.com/future/technology/2026/04/10/iranian-cyber-attacks-move-from-disruptive-to-complex-threats-in-gulf/. Verified on 21 November 2026.

S34 DailyDarkWeb, report on DieNet's claimed DDoS against Qatari government sites (title names the bodies), 6 March 2026. https://dailydarkweb.net/ (article URL withheld). Verified on 21 November 2026.

S35 Gulf Times (QNA), "Ministry of Interior warns against calls exploiting ongoing situation", 24 March 2026. https://www.gulf-times.com/article/722806/qatar/ministry-of-interior-warns-against-calls-exploiting-. Verified on 21 November 2026.

S36 Qatar Tribune, "GTA issues urgent warning over scam messages impersonating officials", 26 February 2026. https://www.qatar-tribune.com/article/221421/business/gta-issues-urgent-warning-over-scam-messages-impersonating-officials. Verified on 21 November 2026.

S37 Gulf Times, "Blackmailing can lead to 3-year jail term, QR100,000 fine, MoI official warns", 28 September 2026. https://www.gulf-times.com/article/734377/qatar/blackmailing-can-lead-to-3-year-jail-term-qr100000-fine-moi-official-warns. Verified on 21 November 2026.

S38 Gulf Times, "National Cyber Security Agency Urges Immediate iPhone Security Update for Users in Qatar", 22 March 2026. https://www.gulf-times.com/article/722733/qatar/national-cyber-security-agency-urges-immediate-iphone-security-update-for-users-in-qatar. Verified on 21 November 2026.

S39 Gulf Times, "CRA launches updated Qatar Domains Registry policies to strengthen digital security and trust", 3 November 2026. https://www.gulf-times.com/article/737448/qatar/cra-launches-updated-qatar-domains-registry-policies. Verified on 21 November 2026.

S40 Qatar News Agency, interview with the head of the national cyber exercises committee on the 13th National Cyber Drill, 15 November 2026. https://qna.org.qa/en/News-Area/News/2026-11/15/cyber-exercises-committee-head-to-qna-national-drill-to-test-institutional-preparedness-for-cyber-incidents. Verified on 21 November 2026.

S41 Gulf Times, "Qatar financial system demonstrates strong resilience in 2025: QCB", 3 August 2026. https://www.gulf-times.com/article/730424/business/qatar-financial-system-demonstrates-strong-resilience-in-2025-qcb. Verified on 21 November 2026.

S42 Microsoft Learn, "List of Azure regions" (updated 17 November 2026), and Google Cloud, "Regions and zones". https://learn.microsoft.com/en-us/azure/reliability/regions-list and https://docs.cloud.google.com/compute/docs/regions-zones. Verified on 21 November 2026.

S43 National Cyber Security Agency, Cybersecurity Advisories listing, 1 January–20 November 2026. https://www.ncsa.gov.qa/en/media/cybersecurity-advisories. Verified on 21 November 2026.

S44 Proofpoint, "Iran conflict drives heightened espionage activity against Middle East targets", 11 March 2026. https://www.proofpoint.com/us/blog/threat-insight/iran-conflict-drives-heightened-espionage-activity-against-middle-east-targets. Verified on 21 November 2026.

S45 Marhaba, "NCSA Warns Public About Rise in Phishing and Impersonation Scams", 19 September 2026. https://marhaba.qa/ncsa-warns-public-about-rise-in-phishing-and-impersonation-scams/. Verified on 21 November 2026.

S46 Silent Push, report on Smishing Triad, 10 April 2025. https://www.silentpush.com/blog/smishing-triad/. Verified on 21 November 2026.

S47 Al Jazeera, "Israeli ad-tech firm helped place spyware on Al Jazeera devices", 15 October 2026, reporting Citizen Lab findings. https://www.aljazeera.com/news/2026/10/15/israeli-ad-tech-firm-helped-spy-on-al-jazeera-devices. Verified on 21 November 2026.

S48 Citizen Lab (Bill Marczak et al.), "Exposing AdFection: How Discover-Tech Turned Targeted Ads Into a Pipeline for Zero-Click Mercenary Spyware", 15 October 2026. https://citizenlab.ca/research/how-discover-tech-turned-targeted-ads-into-a-pipeline-for-spyware/. Verified on 21 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; an "employee" device is one labelled as a staff device, and employment is not verified.
- **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.
- **Availability-check link:** a link to a public service that tests whether a website answers from several locations; it records a moment, not an outage.
- **Breach forum:** a forum where stolen data and network access are advertised and traded.
- **Card casher:** a criminal who turns stolen card data into money or goods.
- **Loader (fraud):** a criminal who tops up accounts or pays invoices with stolen cards for a cut; in §7.2 "loader" instead means a malware stage.
- **Dark-chat:** closed messaging channels, such as Telegram groups, used for criminal trade.
- **OTP bot:** an automated service that calls or messages victims to trick them into revealing a one-time password.

- **DNS amplification:** a DDoS technique that sends small DNS queries with a forged source address so that large answers flood the target.
- **Card-not-present fraud:** online or phone payments made with stolen card details alone.
- **Web shell:** a malicious script placed on a web server that gives an attacker remote control of it.
- **Stresser:** a DDoS-for-hire service, often sold as a "stress test".
- **Miles shop:** a channel that sells airline and hotel loyalty accounts, often with access to the linked mailbox.
- **DMARC / SPF / DKIM:** email-authentication standards; DMARC tells receivers what to do with mail that fails.
- **DNSSEC:** signatures that let resolvers verify DNS answers.
- **DS record:** the record in the parent zone that links a domain to its DNSSEC keys.
- **HSTS:** a web header telling browsers to use HTTPS only.
- **TLP:CLEAR:** may be shared without restriction; other legal duties still apply.
- **PlugX / Cobalt Strike:** a remote-access malware family long used in espionage, and a commercial attack-simulation tool that criminals and spies also use.
- **DLL hijacking:** making a legitimate program load a malicious library placed where the program looks first.
- **BIN:** the issuer's card-number prefix (bank identification number).
- **KYC:** "know your customer" identity checks at banks, exchanges and other services.
- **MFA (multi-factor authentication):** a sign-in that needs a second factor beyond the password.
- **Phishing-resistant MFA:** sign-in tied to the real site (FIDO2 security keys, passkeys or certificates), so a relay page cannot reuse it.
- **Headline score:** the national Atlas summary score for all 250 organisations.
- **Passive hygiene index:** an Odin analytical composite of email, DNS, TLS and header checks; 0-100, higher means weaker.
- **NCSA:** the National Cyber Security Agency of Qatar, the national cyber authority and personal-data privacy regulator.

About this report

Prepared by Odin by Brandefense. Version 1.0 was completed on 21 November 2026.

Research cut-off: 20 November 2026 (primary data window). 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 Qatar. Recommendations describe what organisations could do; they do not state that any organisation has or has not done them. An Arabic-language edition of version 1.0 is published alongside; the English edition prevails where they differ.

© 2026 Brandefense. All rights reserved.