COUNTRY REPORT · BRANDEFENSE COUNTRY REPORT · UNITED ARAB EMIRATES 2026 · TLP:CLEAR · 81 MIN READ

Brandefense United Arab Emirates Cyber Threat Landscape Report 2026

Identity exposure, a residents' account market and crisis-period destructive claims in a highly digitised Gulf economy

BY
Odin by Brandefense

PUBLISHED
21 November 2026

READING TIME
81 min read

EDITION
Version 1.0 · Public Research Edition · TLP:CLEAR

RESEARCH WINDOW
1 January-20 November 2026

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

130,477
posts tagged as concerning the UAE, 1 January-20 November 2026

10
DDoS claims in the actor posts we read against UAE targets, all between 2 March and 8 April

12 of 23
banks in our list with a credential listed for sale on the day of the check

CONTENTS

01 Executive summary
Report map
02 The United Arab Emirates' digital and threat context
03 National exposure: 250 leading organisations
04 What we see on the dark web
05 Targeting examples by sector
06 Hacktivism, DDoS and destructive claims
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 UAE 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 leading UAE organisations we assessed, the main measured exposure is identity: infected-device and credential associations, and credentials listed for sale at 109 of them. The underground trades UAE residents' verified accounts and real-estate data all year. Destructive and DDoS claims against state, energy and transport targets clustered in March and April, and the named bodies did not confirm them. Act in this order: validate listings, test backup restores, then harden account opening.

This report combines three of Brandefense's own data sources with verified public reporting. **Brandefense Blackhole** supplied 130,477 posts tagged as concerning the UAE and 1,271 distinct forum posts mentioning the UAE. 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 the UAE and four Gulf comparators. **Atlas** exposure ratings were computed for the 250 organisations. These are separate populations and are never added together.

1. Credential and infected-device associations touch almost every leading organisation. 234 of the 250 organisations have infected devices associated with their domains (at least 522,128 in total). Most (491,713) are not employee-classified, and many are probably residents' and customers' own devices, though ownership is not established; 30,415 are employee-classified. 241 have historical credential records (1,856,314 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, residents or customers. These are association counts: whether any login is still usable, and whose it is, requires validation. [S2][S3]

2. 109 of 250 organisations had a credential listed for sale when checked. Atlas gives the 250 organisations a national headline rating of 53 on a 0-100 scale, where 0 means no risk observed; it is a summary rating, not an average. A listing tells a defender to look for an active account; it does not say how many accounts or whose. [S3]

3. Destructive and DDoS claims clustered during the crisis and remained unconfirmed. Hacktivist DDoS claims in the actor posts we read against federal and emirate websites fell between 2 March and 8 April. Handala, a brand Security Affairs describes as widely seen as a front for an Iran-backed actor, claimed wiper attacks and data theft at several public-sector bodies in one emirate. Its claimed volumes were 6 PB destroyed and 149 TB stolen. Neither the named bodies nor the authorities confirmed these claims by our cut-off. The national cybersecurity authority itself warned of an active regional wiper campaign in April. [S1][S11][S26]

4. Residents' accounts and property data led UAE offers; ransomware listings outpaced Gulf comparators. The most persistent UAE-specific thread is trade in bank, wallet, remittance and exchange accounts tied to an Emirates ID or residence card, and in mule recruitment. Real-estate owner, tenant and portal data was the most frequently advertised UAE-specific dataset category in the reviewed posts, from at least nine sellers. Ransompedia lists 84 UAE ransomware listings in the window, far above Saudi Arabia (30), Qatar (9), Oman (9) and Kuwait (7). [S1][S5]

5. Few incidents in the reviewed public reporting had detailed confirmation. The head of the UAE Cybersecurity Council described a hacker who exploited an unpatched vulnerability at a private-sector organisation and demanded 5 million USD. In November Landmark Group confirmed unauthorised access to its Shukran loyalty programme in which names, contact details and birth dates may have been exposed, a day after a leak-site group listed the company. Separately, vendors reported state-linked espionage against UAE entities through hijacked mailboxes and job lures. [S17][S67][S24][S31][S32]

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. Contain privileged, remote-access or no-MFA (multi-factor authentication) accounts the same day, and record a disposition for the rest within 5 working days. Arrange monitoring of credential listings and infected devices for your domains from day 1, through an internal team or a provider (§12.1 rows 1-2).
2. **Prove you can recover from a wiper.** The Council's own advisory describes destructive malware entering through phishing, stolen VPN credentials and unpatched systems. Restore a critical system from offline backup within the promised time, and patch or isolate end-of-life edge systems (§6.4; §12.1 rows 4 and 6).
3. **Prepare for claims that outrun the facts.** Agree in advance who confirms service status publicly during a hacktivist campaign, and pre-arrange upstream DDoS mitigation for public portals before the next heightened period (§12.1 rows 9 and 16).
4. **Break the account-fraud chain.** Residence-card KYC, mule accounts and remote-access takeover are one chain. Move approvals off SMS codes and test account opening and recovery with synthetic cases (§8, §10.3; §12.1 rows 10 and 18).

The year in numbers

130,477

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

WHAT IT IS NOT

Not a count of attacks; October alone holds 32,435, mostly one account-trading bot family

23,663-24,456

relevant posts in January-July and November, given as a range (of 65,544 tagged)

WHAT IT IS NOT

Not unique incidents; of 30 random relevant posts, only 10 named the UAE specifically

250

leading public and private organisations assessed with Atlas methodology

WHAT IT IS NOT

Not a random sample; not a national prevalence estimate

522,128+

infected devices associated with those 250 domains (30,415 employee-classified); cumulative, all records held on 21 Nov 2026

WHAT IT IS NOT

Not 2026-only, not unique people, not verified current infections; a lower bound

109 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

84

Ransompedia accepted ransomware listings for the UAE dated 1 Jan–20 Nov 2026 (74 distinct plausible UAE organisations)

WHAT IT IS NOT

Not confirmed intrusions; listings are criminal claims

128

incidents the national cybersecurity authority counted as confirmed by 18 February 2026

WHAT IT IS NOT

Not comparable with our counts; a different population and method

10

hacktivist DDoS claims in the actor posts we read, all between 2 March and 8 April

WHAT IT IS NOT

Not confirmed outages

631

distinct UAE-associated payment cards seen in clear text in collected dark-web posts (504 attributed to a named UAE issuer)

WHAT IT IS NOT

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

82%

of the 250 organisations enforcing DMARC (204)

WHAT IT IS NOT

Not a measure of phishing success

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 UAE 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 notification rules apply?

GO TO 6 10 12

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

02 **Context**
Which features of the UAE shape its threat picture

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

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

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

06 **Hacktivism**
What was claimed, what was officially said, 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 rules apply and what changed in 2026

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

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

CHAPTER 2

The United Arab Emirates' digital and threat context

THIS CHAPTER ANSWERS

Which features of the UAE shape its cyber threat picture in 2026, and what did the national authorities report?

99%

internet penetration (the source's cap), with 23.0 million cellular connections

INSIDE THIS CHAPTER

2.1 A connected, mobile-first population

2.2 Centralised digital identity and government

2.3 A regional crisis and the official attack figures

2.4 Official attribution statements

IN SHORT

Three features shape the UAE's threat picture: near-universal, mobile-first connectivity; a centralised digital-identity model; and a regional crisis from late February, which the national cybersecurity authority linked to a sharp rise in attack attempts. Official figures describe pressure, not outcomes. Plan for destructive malware and identity fraud at once: test offline backups and harden account recovery.

2.1 A connected, mobile-first population

DataReportal counted 11.4 million inhabitants in October 2025 and 11.3 million internet users at the end of 2025, a penetration of 99.0% (DataReportal caps adoption at 99%). It counted 23.0 million cellular connections, 202% of the population, and 12.5 million social-media user identities, which may not be unique people [S8].

Two consequences follow for defenders. Fraud aimed at UAE residents arrives in many languages: the criminal posts we hold about the UAE are mostly in English and Russian, with Arabic a small share (Chapter 4). Mobile numbers, messaging apps and app-based banking are also the main channels for both service delivery and fraud.

2.2 Centralised digital identity and government

The UAE runs a single national digital identity, UAE PASS, which the state news agency WAM reported had more than 12 million registered users [S55]. Federal and emirate-level portals sit behind it. Centralised identity makes services faster and also concentrates value: a working UAE PASS session or a copy of an identity document opens many doors. In March, Dubai Police warned of callers posing as crisis-management staff to obtain UAE PASS and Emirates ID details for SIM-swap and banking-app takeover [S49].

The UAE Cybersecurity Council, set up by Cabinet decision in November 2020 [S54], leads national cyber policy. The Cabinet approved the current National Cybersecurity Strategy on 3 February 2025, built on five pillars: governance, protection, innovation, building capability and partnership [S43]. In June 2026 a new Federal Authority for Artificial Intelligence and Data was

announced, which, according to a law-firm analysis, consolidates AI oversight, digital government and data regulation [S41]. Chapter 10 sets out what this means for organisations.

2.3 A regional crisis and the official attack figures

The Council's head reported a heightened period of cyber activity from 28 February to early April 2026, during what he called a regional crisis [S22]. In early March, Amazon's cloud division reported a fire at a UAE data centre after objects struck the facility, which affected service availability; that outage was physical, not a cyberattack. Some online and phone banking services were unavailable the same day, with the cause publicly unknown [S29].

The Council published figures throughout the year. They come from different events, periods and wording, and the Council did not publish a method, so they are not a time series. On 21 October the Council itself stressed that more detected attempts "does not necessarily indicate" more successful breaches [S20].

Date	What the Council said	Source
2026-02-18	128 confirmed incidents since 1 January; 90,000-200,000 breach attempts a day	[S9]
2026-02-21	Organised attacks "of a terrorist nature" on national platforms thwarted: network intrusion, ransomware and phishing attempts	[S10]
2026-04-01	Daily attacks up from about 200,000 to about 600,000	[S13]
2026-04-20	About 800,000 attacks a day during the truce, against about 200,000 before the crisis	[S14]
2026-07-03	More than 800,000 attempts a day; attacks on financial-sector entities thwarted	[S15]
2026-08-10	Advanced and organised attacks on aviation, energy and education countered	[S16]
2026-09-15	640,000 attacks recorded in a single day	[S17]
2026-10-21	Nearly 750,000 attempts thwarted "in recent months"	[S20]
2026-10-28	National teams remediated a widespread PHP vulnerability; no CVE was given	[S21]
2026-11-18	More than 40 groups from over 20 countries tried to exploit the crisis	[S22]

The February breakdown is the most useful official baseline. Of the 128 confirmed incidents, the Council classed 38.3% as defacement, 25.8% as data leaks, 13.3% as data breaches, 10.2% as initial access, 7.8% as ransomware and 4.7% as DDoS. Telegram carried 49.2% of the related activity, the open web 40.6% and Tor sites 10.2%. Government (9.4%) and financial services (9.3%) were the most affected sectors [S9]. Telegram also dominates our own collection (99.6% of tagged posts); otherwise the official mix and our post families measure different things and are not compared.

2.4 Official attribution statements

Official statements about who was behind the activity varied by occasion. We record them as reported, without our own attribution.

Date	Statement as reported	Source
2026-02-18	The Council said "a significant proportion" of attacks were carried out by state-sponsored advanced threat groups. 15 of the 21 tracked APT groups were state-sponsored. The Council also tracked 60 hacktivist and criminal actors	[S9]
2026-04-20	The Council's head listed groups including, as reported, groups with links to Iran	[S14]
2026-09-16	In a CNN interview reported by The National, the Council's head named Iran and the IRGC (Islamic Revolutionary Guard Corps)	[S18]
2026-09-17	Euronews wrote that the same official did not attribute the operations to any state	[S19]
2026-11-18	At the World Police Summit, the Council's head named Iran and networks linked to the Revolutionary Guard among more than 40 organisations	[S23]

What this means for defenders. The attribution debate does not change the controls. The Council's own warnings describe destructive wiper malware, phishing, stolen VPN credentials and unpatched internet-facing systems as the entry points [S11]. Those are the same controls whoever the operator is.

KEY TAKEAWAYS

01

Near-universal connectivity and a central digital identity make identity data and sessions the prize.

02

Official attack figures measure attempts on different bases; read them as pressure, not as a trend.

03

The Council's own advisories name the entry points: phishing, VPN credentials and unpatched edge systems.

CHAPTER 3

National exposure: 250 leading organisations

THIS CHAPTER ANSWERS

How exposed are the UAE's 250 leading public and private organisations when they are scored the way Brandefense Atlas scores a customer, and which signal should a defender triage first?

109 of 250

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

INSIDE THIS CHAPTER

3.1 Universe card | 3.2 National rating and current listings by sector | 3.3 Devices and credentials | 3.4 Current credential listings | 3.5 Lookalike domains, exposed documents and mentions | 3.6 Email and web hygiene

IN SHORT

We assessed 250 leading UAE organisations using Brandefense Atlas exposure ratings. Almost all have infected devices and credential records associated with their domains, and 109 had a credential listed for sale when we checked. Email hygiene is comparatively strong: 204 of 250 enforce DMARC. DNSSEC is rare. Triage current listings first, then employee devices, then large credential stores at universities and government bodies.

3.1 Universe card

Item	Definition
Population	250 organisations: 68 government bodies, 35 banking and finance, 19 energy and utilities, 19 transport and logistics, 18 education, 16 retail and holdings, 11 insurance, 11 technology, 11 healthcare, 10 real estate and construction, 9 manufacturing and industry, 9 hospitality and tourism, 8 media and 6 telecom. 184 state or state-linked, 60 private, 6 foreign
Selection	Purposive: federal and emirate bodies and portals, central-bank-licensed banks and payment firms, state-linked enterprises and market leaders. Selected for size or systemic role, not ranked by revenue; no published UAE top-250 ranking was used
Unit	One primary domain per organisation. All 250 resolve in DNS (21 November 2026). For 173 domains the homepage was read to confirm ownership; the other 77 could not be read and were assigned by the domain matching the organisation's official name. 68 of 318 candidates were dropped as duplicates, out of scope or not matching their organisation
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

Item	Definition
Date	Counts read 21 November 2026. Device, credential and listing counts are all records held on that date, regardless of capture date (cumulative, not 2026-only). Mention counts cover the 365 days to 18 November 2026; lookalike counts cover the last 30 days
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 National rating and current listings by sector

Atlas rates each organisation from 0 (no risk observed) to 100. Atlas gives the 250 organisations a national headline rating of 53 on this 0-100 scale; it is a summary rating, not an average. By sector, the report gives the signal counts.

How to read Atlas ratings.

Term	Meaning
Headline	The national summary rating Atlas reports; it is not an average
Current listing	A credential tied to the domain on sale at the time of the check
Listing history	A credential tied to the domain was offered for sale at some earlier time

205 organisations had candidate lookalike matches; those matches were not all validated.

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

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

	Infected devices	Employee devices	Credential records	Current listing	Listing history	Lookalikes (30 days)	Exposed documents
Media and entertainment (8)	100%	75%	88%	62%	62%	75%	62%
Technology (11)	91%	91%	100%	55%	55%	100%	82%
Government (68)	94%	75%	96%	54%	53%	85%	59%
Telecom (6)	67%	67%	100%	50%	50%	83%	33%
Banking and finance (35)	100%	83%	100%	46%	37%	94%	66%
Education (18)	100%	100%	100%	44%	44%	89%	78%
Hospitality and tourism (9)	89%	44%	100%	44%	44%	78%	56%
Retail and holdings (16)	100%	75%	100%	44%	38%	69%	81%
Transport and logistics (19)	89%	79%	95%	42%	32%	79%	58%
Healthcare (11)	100%	82%	100%	36%	36%	64%	55%
Insurance (11)	100%	82%	100%	27%	27%	73%	36%
Manufacturing and industry (9)	89%	78%	78%	22%	11%	56%	56%
Energy and utilities (19)	84%	84%	89%	21%	16%	79%	53%
Real estate and construction (10)	80%	70%	100%	20%	10%	80%	70%

Source: Brandefense Blackhole associations and Atlas ratings for 250 organisations, read 21 November 2026 [S2][S3]. Records are cumulative, not 2026-only.

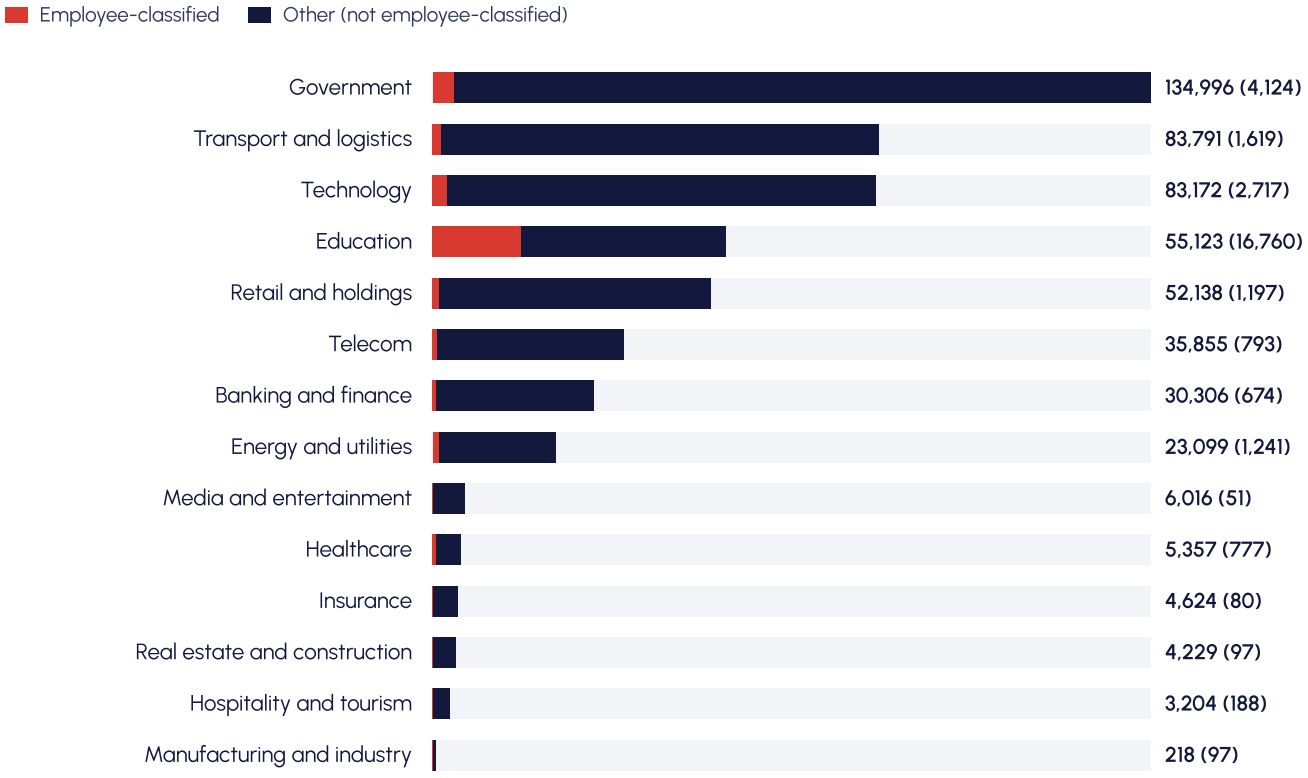
Sector	Orgs	Orgs with a current credential listing
Government	68	37
Banking and finance	35	16
Energy and utilities	19	4
Transport and logistics	19	8
Education	18	8
Retail and holdings	16	7
Insurance	11	3
Technology	11	6
Healthcare	11	4

Sector	Orgs	Orgs with a current credential listing
Real estate and construction	10	2
Manufacturing and industry	9	2
Hospitality and tourism	9	4
Media and entertainment	8	5
Telecom	6	3
All 250	250	109

Reading the table. Triage from the listing column. Government (37 of 68) and banking and finance (16 of 35) have the most organisations with a current listing. In media (5 of 8), telecom (3 of 6) and technology (6 of 11) half or more are listed, but all three sectors are small.

3.3 Devices and credentials

Government, transport and technology carry the most infected-device associations; universities hold most employee-classified devices



Source: Brandefense Blackhole associations and Atlas ratings for 250 organisations, read 21 November 2026 [S2][S3]. Records are cumulative, not 2026-only.

Sector	Orgs with infected devices	Devices (employee)	Credential records	Credential share, two largest orgs
Government	64 of 68	134,996 (4,124)	157,226	57%
Transport and logistics	17 of 19	83,791 (1,619)	232,300	63%
Technology	10 of 11	83,172 (2,717)	92,414	71%
Education	18 of 18	55,123 (16,760)	958,690	58%
Retail and holdings	16 of 16	52,138 (1,197)	65,414	60%
Telecom	4 of 6	35,855 (793)	38,288	94%
Banking and finance	35 of 35	30,306 (674)	90,638	31%
Energy and utilities	16 of 19	23,099 (1,241)	76,227	56%
Media and entertainment	8 of 8	6,016 (51)	10,707	69%
Healthcare	11 of 11	5,357 (777)	43,262	63%
Insurance	11 of 11	4,624 (80)	9,162	61%
Real estate and construction	8 of 10	4,229 (97)	21,979	58%
Hospitality and tourism	8 of 9	3,204 (188)	48,669	85%
Manufacturing and industry	8 of 9	218 (97)	11,338	64%
All	**234 of 250**	**522,128 (30,415)**	**1,856,314**	**30%**

Device totals are lower bounds. Credential records split into 466,560 breach-database records, 579,220 stealer-log lines and 810,534 combolist entries. The infected devices hold more than 3.7 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.** 491,713 of 522,128 devices are not employee-classified. Many are most plausibly residents' and customers' own computers, though ownership is not established. They are a fraud and account-hijacking signal and do not by themselves establish an intrusion. The 30,415 employee-classified devices are the intrusion-relevant subset; both groups require validation.
- **Universities hold the employee-device problem.** Education has 16,760 employee-classified devices, more than half of the national total in our list, and 958,690 credential records. Staff and students share domains, so "employee" here may include students.
- **Concentration is high.** In telecom, two organisations hold 94% of credential records. A sector total is therefore a poor guide to a typical organisation.
- **The median organisation is modest.** The median organisation has 274 infected devices and 782 credential records; the heaviest carry tens of thousands.

3.4 Current credential listings

109 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 109, 99 also have a listing history.

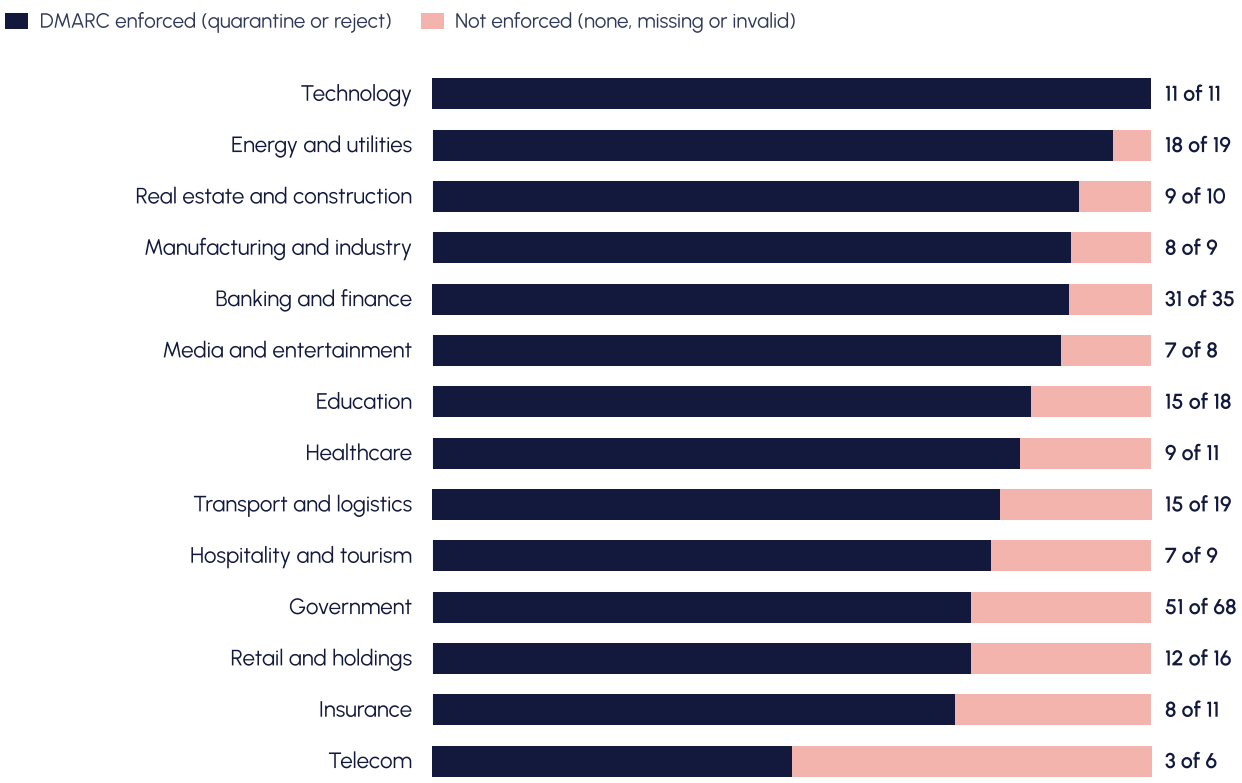
For a defender, a current listing is the most direct market signal that a login tied to the domain is on offer. Whether that login still works is exactly what validation must establish. The listing does not say how many accounts, whose accounts, or whether the account is active, protected by multi-factor authentication (MFA) 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:** 205 organisations had at least one newly observed candidate lookalike domain in the last 30 days. Those matches were not all validated; validate each domain before acting. Lookalikes are candidates, not confirmed phishing sites.
- **Exposed documents:** 154 organisations have at least one exposed document that references their domain (3,104 in total), most of them in government.
- **Mentions:** 89 organisations were mentioned in dark-chat (messaging-channel) sources in the last 365 days and 24 in dark-web sources. Mention counts measure visibility, not hostility; news sites and portals linked in Telegram channels collect many.

3.6 Email and web hygiene

Most sectors enforce DMARC; telecom has the largest share without enforcement and government the largest number



Source: Brandefense public DNS, TLS and homepage checks of 250 domains, 21 November 2026 [S4].

Results from our public DNS, TLS and homepage checks [S4]:

Control	Result (of 250 unless stated)	Reading
DMARC reject	120	Spoofed mail from the domain should be refused
DMARC quarantine	84	Spoofed mail should go to spam
DMARC p=none or missing	46 (36 none, 10 missing)	No enforcement; spoofing the domain is easier
SPF ending -all / ~all / ?all / redirect / none	170 / 69 / 1 / 3 / 7	7 domains publish no SPF policy
DKIM record found	184	Absence is not proof of no DKIM
DS record observed (DNSSEC delegation)	12	No DS record observed for 238 domains; a DS record alone does not prove a valid chain of trust
TLS certificate invalid	8 of 222 checked	Expired, mismatched or untrusted certificates

Control	Result (of 250 unless stated)	Reading
HSTS (HTTP Strict Transport Security) on homepage	143 of 173 reachable	Most reachable sites force HTTPS for returning visitors
Mail provider	106 Microsoft 365, 10 Google, 8 with no mail (MX) record	The rest run their own or regional mail

Hygiene is stronger than exposure. 204 of 250 organisations (82%) enforce DMARC, including 31 of 35 in banking and finance and 51 of 68 government bodies. Telecom (3 of 6 without enforcement) and government (17 without enforcement) have the largest gaps (§12.1 row 8). On the passive hygiene index (Appendix A.5; 0-100, higher is weaker), insurance (38) and telecom (36) have the weakest hygiene index by sector and technology (17) and real estate (19) the strongest. Good email hygiene does not offset credential exposure: the listings in §3.4 concern logins, not spoofing.

KEY TAKEAWAYS

01

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

02

109 of 250 organisations had a current credential listing; triage those listings first.

03

DMARC enforcement is strong at 82%; DNSSEC delegation is rare at 12 of 250.

CHAPTER 4

What we see on the dark web

THIS CHAPTER ANSWERS

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

130,477

posts tagged as concerning the UAE, 1 January-20 November 2026

INSIDE THIS CHAPTER

4.1 Universe card | 4.2 Platforms, languages and volume | 4.3 Crime families after cleaning | 4.4 UAE-specific data offers: real estate leads | 4.5 Government-themed offers and recirculated material | 4.6 Case studies | 4.7 What the forums add

IN SHORT

Most UAE-tagged underground traffic is multi-country advertising in English, Russian and Chinese Telegram channels. After cleaning, about one in three posts remains, and most of those are card-checker output, account trading and multi-country data leaks naming the UAE among many countries. The UAE-specific offers that matter are real-estate customer data, identity and residence-card verification, and access to government web systems. Triage each claim by provenance before comment.

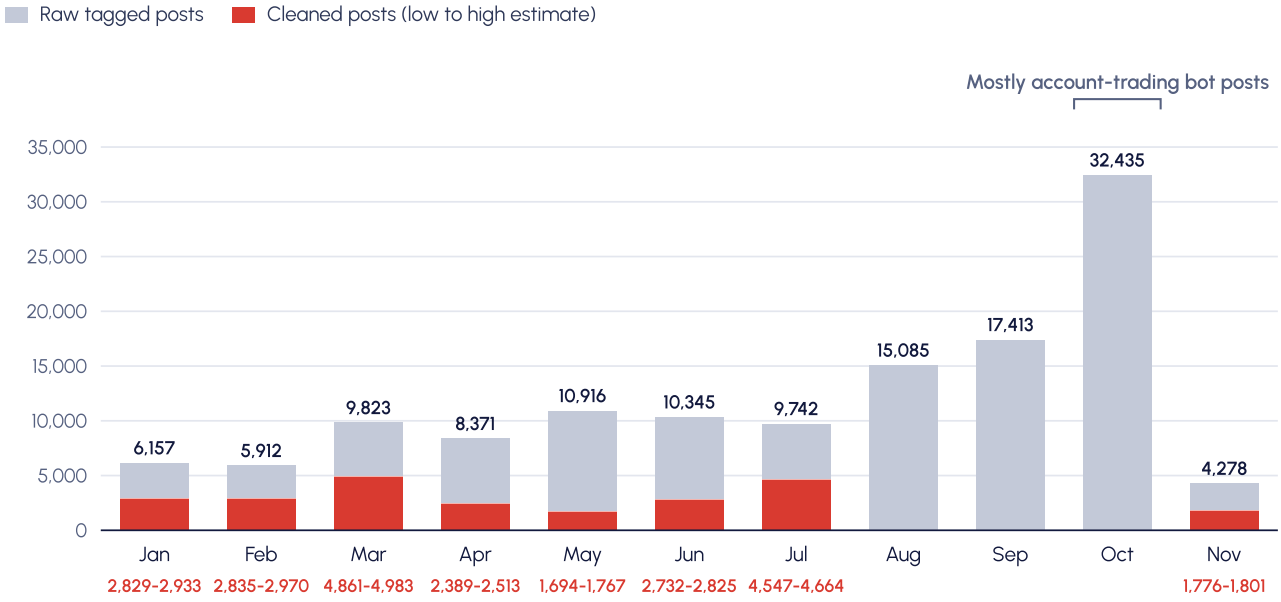
4.1 Universe card

Item	Definition
Source	Brandefense Blackhole: Telegram channels and groups, a set of cybercrime forums, paste sites and Discord, collected continuously `[S1]`
Country definition	A country tag ("this post is about, targets or mentions the UAE"), plus forum posts mentioning the UAE
Window	Post time 1 January-20 November 2026 (November partial)
Tagged set	130,477 posts counted
Coverage	Relevant-post ranges cover January-July and November (65,544 tagged posts); August and October are covered only in part, and September posts were not available
Forum posts	1,271 distinct forum posts mentioning the UAE
Relevant posts	Given as a range for January-July and November (Appendix A.2)

Item	Definition
Not established	That a tagged post targets the UAE, that a claim is true, or that two posts concern the same file

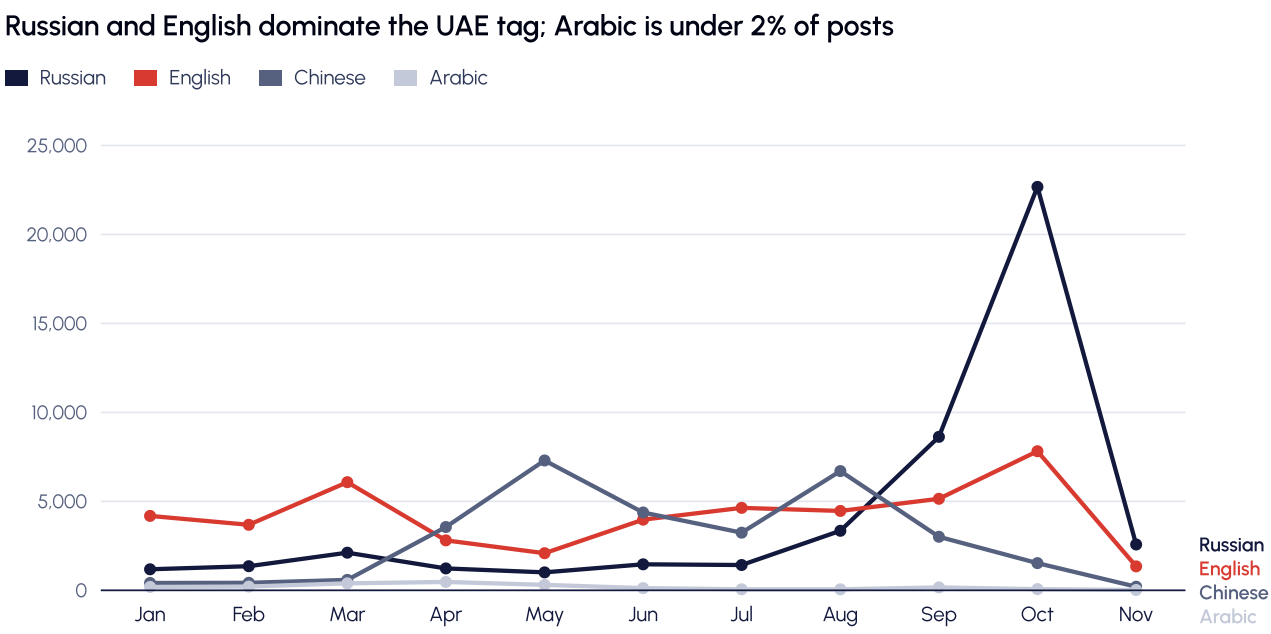
4.2 Platforms, languages and volume

One account-trading bot family makes October the largest month; volume otherwise runs at about 6,000-17,000 tagged posts a month



August to October have no relevant-post range: coverage for those months is incomplete. Source: Brandefense Blackhole, posts tagged as concerning the UAE, post dates 1 January-20 November 2026, November partial [S1]. Cleaned counts are an upper bound.

Measure	Value
Telegram share of tagged posts	99.64% (130,007)
Forum posts	381 tagged, plus 1,271 distinct forum posts mentioning the UAE
Paste, Discord	39, 50
Russian / English / Chinese / Arabic	36.0% / 35.4% / 24.0% / 1.6% of tagged posts (a post can carry more than one language)
Largest month	October, 32,435 posts, of which 19,924 were account-trading posts



Telegram carries 99.64% of tagged posts. Language labels can overlap. Source: Brandefense Blackhole, posts tagged as concerning the UAE, post dates 1 January–20 November 2026, November partial [S1]. Cleaned counts are an upper bound.

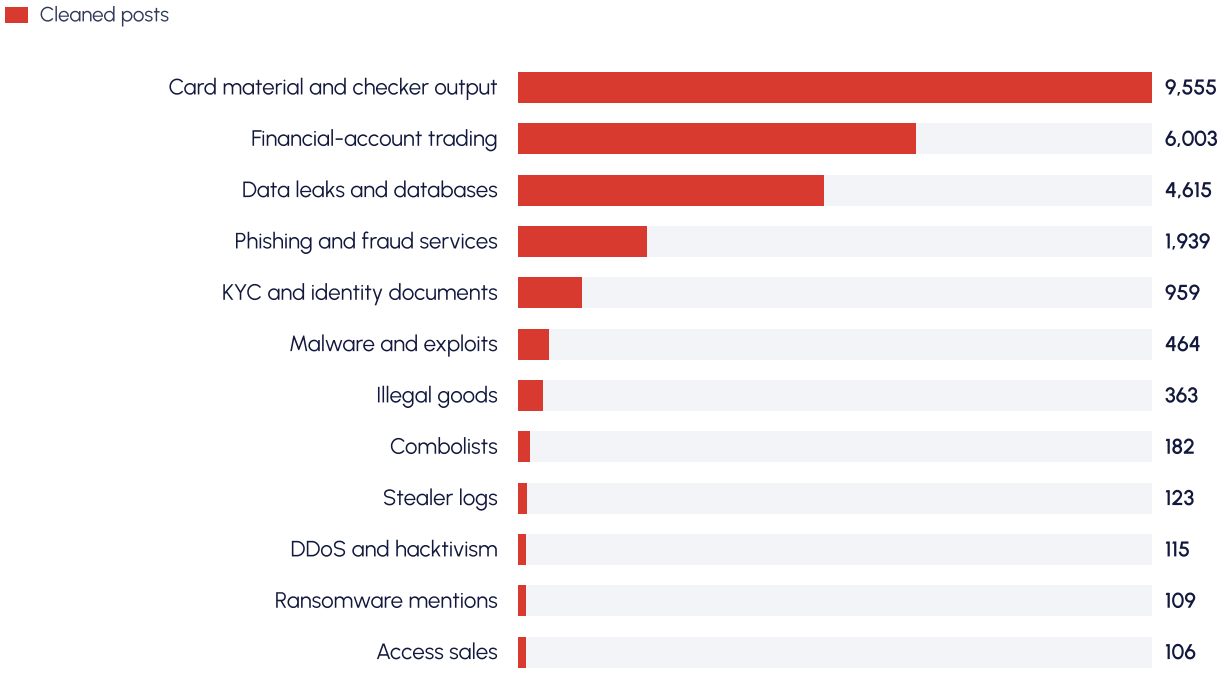
October is a bot month, not an attack month. 61% of October's tagged posts were account-trading posts, dominated by repeated price-list templates. Chinese-language advertising inflated April–August in the same way. Saudi Arabia shows an even larger January–February spike (729,186 posts in two months), and Qatar an October spike (42,835), so spikes of this kind say more about bot campaigns than about a country.

Arabic is rare in the UAE underground we observe. Only 2,070 tagged posts (1.6%) are in Arabic. Criminal trade about the UAE runs mostly in English and Russian, aimed at a resident population that is itself multilingual (§2.1).

4.3 Crime families after cleaning

In January–July and November, the relevant (cleaned) posts number 23,663–24,456 of 65,544 tagged posts (36.1–37.3%), given as a range. Of 30 random relevant posts, 27 were crime-related, but only 10 named the UAE specifically. Cleaned counts are therefore an upper bound for UAE-specific criminal activity.

Card-checker output and account trading dominate the cleaned posts; access sales are rare



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

Family (cleaned posts, January–July and November)	Posts	What dominates
Card material and checker output	9,555	Bot output testing cards, many issued by UAE banks (§8.2)
Financial-account trading	6,003	Bank, wallet and exchange accounts; mule recruitment
Data leaks and databases	4,615	Multi-country lead lists; a minority of UAE-specific datasets
Phishing and fraud services	1,939	Payment-link abuse, fraud tooling, "shooter" recruitment
KYC and identity documents	959	Residence-card and passport verification services
Malware and exploits	464	Tool sales; few UAE-specific
Combolists and stealer logs	305	Credential lines for UAE banks, portals and airlines
DDoS and hacktivism	115	March claims against federal sites (Chapter 6)
Access sales	106	Government and corporate web-system access (§4.5)
Other families	472	Illegal goods (363) and ransomware mentions (109)

Family counts are not compared across June 2026. A post can belong to more than one family.

4.4 UAE-specific data offers: real estate leads

Real-estate data was the most frequently advertised UAE-specific dataset category in the reviewed posts. Across the year, at least nine sellers listed data on property owners, tenants and portal users. Claims ranged from a 74,000-line owner list for one community to 986,506 account records from a UAE real-estate service, with password-related fields. Asking prices were low, up to 1,200 USD, and one set was posted free. A buyer asked for a multi-million-line agency database in February, before the April-May wave of listings.

Date	Offer (claimed)	Price	Card
2026-02-18	Buyer seeks a multi-million-line Dubai agency CRM	n/a	B20
2026-04-02	A Dubai developer's customer, sales and identity-document data	100 USD	B02
2026-04-13	400,000 owner and tenant records attributed to a major developer, raised to 700,000 six days later	not stated	B04
2026-05-06	986,506 account records from a UAE real-estate service	free	B06
2026-09-10	49GB property-platform database, with a claim that it was then wiped	not stated	B05

One seller insisted its set was not the "public data" of Dubai owners that, it said, "everyone" sells, which concedes that such lists already circulate. That weakens the uniqueness of each claim but not the risk. Owner, tenant and transaction details are exactly what payment-instruction and fake-handover fraud needs.

EVIDENCE CARD B20 — 18 Feb 2026

Anonymous buyer Breach forum · Forum · English

ORIGINAL

```
I am looking for a big Realty Estate Agency database from United Arab Emirates (Dubai if i'm not wrong) with couple millions lines also in thread title was just domain name and description was said that base from CRM. I lost link to thread
```

Note. Demand for property data came before the April-May wave of developer and portal listings.

HELD	A buyer looked for a multi-million-line Dubai real-estate agency CRM database seen earlier on the forum.
NOT ESTABLISHED	It does not establish that such a database exists.

EVIDENCE CARD B04 — 13 Apr 2026

ksa901 Breach forum · Forum · English

ORIGINAL

```
I am selling here [major Dubai property developer] - owners & rentals information, Datasets have more than 400k records of owners and rentals and even they car information and even their parking and address, phone numbers, emails. and included 4gb of Docs. [...] is not public Data of Dubai owners which everyone sell
```

Note. Six days later the same alias raised the claim to 700,000 records covering a second developer.

HELD	A seller advertised 400,000 owner and tenant records, with car and parking details, attributed to a major Dubai developer.
NOT ESTABLISHED	It does not establish the source system; the seller's own wording admits that similar Dubai owner lists already circulate.

EVIDENCE CARD B02 — 2 Apr 2026

Seller of B01 (alias withheld) Breach forum · Forum · English

ORIGINAL

```
[Dubai real-estate developer] is Real estate company in dubai [...] Price: 100$ [...] I got customers Info / sales info / id,passport pics + bank transactions / CRM
```

Note. A second alias offered the same CRM column set on another forum on 19 Apr, claiming 350GB from a sales-manager account.

HELD	The same actor family offered a Dubai property developer's customer, sales and identity-document data for $100.
NOT ESTABLISHED	It does not establish the volume of records or that passport images are genuine.

EVIDENCE CARD B06 — 6 May 2026

attackercompany Breach forum · Forum · English

ORIGINAL

```
UAE REAL ESTATE DATA REPORT [...] Total Records: 986,506 Region: United Arab Emirates Sector: Real Estate [...] Fields Observed • Name • Login Identifiers • Password-Related Values • Phone / Cell Numbers • Email Addresses • WhatsApp Information • IP Addresses
```

Note. Part of a year-long cluster of at least nine property-owner and real-estate datasets.

HELD	A post advertised a claimed dataset containing 986,506 records from a UAE real-estate service, with password-related and contact fields.
NOT ESTABLISHED	It does not establish which platform the records came from; a later repost named a UAE property portal without evidence.

4.5 Government-themed offers and recirculated material

Government-themed offers in 2026 were mostly entry points and recirculated files, not fresh national datasets.

- **Recirculation.** A student dataset that posters date to March 2025 was reposted on at least five forums from January to May (B07).
- **Access.** Super-administrator access to an emirate's finance department web system was offered for 800 USD in April (B08).
- **Reconnaissance.** A March package mapped a government department's AI service back-ends and an end-of-life PHP portal (B09).
- **Population lists.** One actor advertised 30,000 police personnel records in February and 180,000 records on foreign residents of one nationality two weeks later (B10).
- **Credential lines.** Automated log uploads carried credential lines for a government e-services login page (B12).
- **Exposure lists.** A free list of about 185,000 internet-exposed camera streams in the UAE was shared on 5 March (B11).

EVIDENCE CARD B07 — 26 Jan 2026

Retrogade Breach forum · Forum · English

ORIGINAL

```
In March 2025, [an education organisation]
experienced a significant data breach. The
compromised dataset includes [...] This breach
primarily affects students
```

Note. Reposted on at least five forums between January and May; download links were reported dead in several threads.

HELD	A student dataset attributed to an education organisation was reposted for free download in January 2026.
NOT ESTABLISHED	It does not establish a new 2026 incident; the post dates the original claim to March 2025.

EVIDENCE CARD B08 — 26 Apr 2026

Crimson Breach forum · Forum · English

ORIGINAL

```
Today I'm selling UAE [an emirate's finance
department] Super Administrator Access. Proof:
[link removed] Price: 800 USD Contact (session
only): [contact removed]
```

Note. Lowest-priced government access offer in the corpus.

HELD	A seller offered super-administrator access to an emirate's finance department web system for $800.
NOT ESTABLISHED	It does not establish which application the access covers or whether it was still valid.

EVIDENCE CARD B09 — 23 Mar 2026

rSosa Breach forum · Forum · English

ORIGINAL

```
I've spent the last week mapping [an emirate
government department] [...] AI BRAIN: [exposed
LLM-orchestration back-ends]. These are the
backends for [a government AI service] [...] THE
HOLE: [an end-of-life PHP portal] [...] ADMIN
ACCESS: [portal instances with authentication
misconfigurations].
```

Note. Early example of AI-platform reconnaissance being sold against a government AI service.

HELD	A seller offered a reconnaissance package on a government department's AI and web stack, naming exposed LLM-orchestration endpoints and an end-of-life PHP portal.
NOT ESTABLISHED	It does not establish that the seller got in or took any data.

EVIDENCE CARD B12 — 11 Aug 2026

X Forum Bot Leak aggregator forum · Forum · English

ORIGINAL

```
[a government e-services portal] Uploaded by X
FORUMS [...] Content Type: URL / Email / Password
Combo
```

Note. The same bot posted log extracts for a UAE retail bank, a UAE airline and luxury e-commerce sites.

HELD	Credential lines for a government e-services login page appeared in an automated log upload.
NOT ESTABLISHED	It does not establish that the accounts were valid or that the portal itself was breached; such lines usually come from infected user devices.

EVIDENCE CARD B10	24 Feb 2026

TheAshborn Breach forum · Forum · English

ORIGINAL

```
30,000 Police Personnel Information(PII) (Full Details) from United Arab Emirates Screenshot as proof: [link removed] for more proof just contact us No Telegram - No TOX - Just Session
```

Note. Two weeks later the same alias listed 180,000 records on foreign residents of one nationality, in the same format and with session-only contact.

HELD	An actor advertised personal data on 30,000 UAE police personnel, with screenshot proof only.
NOT ESTABLISHED	It does not establish the data's origin, completeness or accuracy.

EVIDENCE CARD B11	5 Mar 2026

CVDEAD Breach forum · Forum · English

ORIGINAL

```
I'm sharing this dataset, which contains a curated list of publicly accessible IoT devices within the United Arab Emirates (UAE) infrastructure that expose their video streams via RTSP (protected/unprotected) [...] UAE IoT | Vuls Server:Port | RTSP CAM | 185K
```

Note. Shared on 5 March; relevant to physical-security camera exposure.

HELD	A free list of about 185,000 UAE internet-exposed camera stream endpoints, built from scanning, was shared during the heightened period the Council described.
NOT ESTABLISHED	It does not establish that any stream was accessed without authorisation.

4.6 Case studies

Each case sets out the claim, what we can establish and a proportionate response, with chronology, alternatives and limits where the evidence supports them. Case responses are starting points; the owned actions, with owners and completion evidence, are in §12.1.

A

CASE A

An insurer's customer file posted on Telegram and three forums

CLAIM UNVERIFIED

Evidence card B01 | 30 Jan 2026 | Breach forum | Insurance

Claim	A seller advertised about 80,000 customer and broker records attributed to a UAE insurer for 200 USD, filtered, it said, from 500,000 rows. Listed fields include national ID numbers, contact details and amounts paid.
Chronology	A Telegram teaser on 28 January; the full listing on 30 January; relisted on two further forums on 2 and 25 April by the same alias.
What we can establish	That one alias kept the same organisation-specific listing alive for three months. The seller wrote that access was lost early, which fits a short-lived login rather than lasting access.
Alternatives	Data from a broker, a third-party CRM vendor or an aggregator; recycled older records.
Limits	We did not obtain the sample. Neither the insurer nor an authority had commented by our cut-off.
Response	Insurers and brokers should review CRM and payment-portal access logs for January 2026, rotate integration credentials and prepare for phishing that quotes policy details (**§12.1** rows 14-15).
BOTTOM LINE	**Prepare for possible misuse of the advertised fields; check CRM and broker access before anyone speaks of a breach.**

B

CASE B

Two listings name an emirate's transport authority

CLAIM UNVERIFIED

Evidence card B03 | 15 Nov 2026 | Breach forum | Government, transport

Claim	On 25 April one seller offered 301 files of permits, drawings and email for 800 USD. On 15 November a different seller listed a 50GB "database breach" for 5,000 USD, claiming 450,000 resident service records and 100,000 driver records with ID, passport and visa fields.
What we can establish	Two unrelated aliases named the same state body seven months apart and described different data: project documents, then an identity-linked customer dataset. No sample was published in the posts we read.
Alternatives	Contractor or consultant mailboxes for the April files; a field list built from other identity-linked sources, or invented to raise the price, for November.
Limits	No authority statement had addressed either listing by our cut-off.
Response	The authority and its contractors should review document-management and email exposure from the second quarter. Residents should be warned about impersonation using licence and visa details if a sample is verified (**§12.1** rows 4 and 15).
BOTTOM LINE	**Two unrelated sellers named the same body; verify any sample before comment and prepare resident warnings.**

EVIDENCE CARD B01 — 30 Jan 2026

Insurer-data seller (alias withheld) Breach forum · Forum · English

ORIGINAL

```
Welcome To Another UAE Data breach [UAE insurer]
(80k record) [...] Price: 200$ [...] CRM (Payments
invoice, customers info, brokers info) UAE Id
card, full name, email, phone number, address,
paid amount [...] the total was 500k record i
filtered so i got 80k [...] i lost the access
early
```

Note. Same listing posted on Telegram and three forums Jan-Apr; the alias links it to a Telegram handle that also advertised a Dubai developer dataset.

HELD	A seller advertised an 80,000-record customer and broker CRM extract attributed to a UAE insurer for $200, listing national ID numbers among the fields.
NOT ESTABLISHED	It does not establish that the data came from the insurer's systems or that any sale took place.

EVIDENCE CARD B03 — 15 Nov 2026

databreach000 Breach forum · Forum · English

ORIGINAL

```
[an emirate's transport authority] Database Breach
__50GB [...] Price : $5K Exposed Services and
Records : 1. Citizen and Resident Service (450K
Unique Records) [...] 2. Drivers Service (100K
unique Records + 35K Driver License PDF)
```

Note. An earlier, smaller listing (301 files, $800) for the same authority appeared on another forum on 25 Apr under a different alias.

HELD	A seller listed a 50GB dataset attributed to an emirate's transport authority for $5,000, with a field list that includes ID, passport and visa numbers.
NOT ESTABLISHED	It does not establish that the authority's systems were accessed; the field list could be assembled from other sources.

C

CASE C

Real-estate data as a market (B04, B06)

MARKET OBSERVED

Real estate

Claim	At least nine sellers listed owner, tenant, developer and portal data during the year (**§4.4**).
What we can establish	Real estate produced more UAE-specific organisation-level and population-level listings than any other sector in our data. Demand posts preceded the supply wave.
Alternatives	Many sets are probably rebuilt from broker lists, scraped portals and older extracts already in circulation.
Limits	Owner lists overlap heavily; record counts are claimed, not verified.
Response	Developers, brokers and portals should review CRM exports and partner access, and warn owners about payment-instruction and fake-handover fraud (**§12.1** rows 14-15).
BOTTOM LINE	**Owner and tenant data circulates widely; protect owners against payment-instruction and handover fraud.**

D

CASE D

A 2025 student dataset recirculates

RECIRCULATED DATA

Evidence card B07 | 26 Jan 2026 | Breach forum | Education

Claim	A student dataset with IDs, contact details, grades and school details, attributed to an education organisation, was reposted for free download.
What we can establish	Every poster frames it as the same March 2025 event; several threads report dead links. Nothing in our data points to a new 2026 intrusion.
Alternatives	A school-management vendor or a single platform as the original source.
Response	Schools should expect phishing aimed at students and parents that quotes school and grade details, and check whether any credential fields still work (**§12.1** rows 2 and 15).
BOTTOM LINE	**A 2025 claim keeps circulating; expect school-themed phishing and reset any reused credentials.**

E

CASE E

Access and reconnaissance offers against emirate government bodies (B08, B09)

Government

OFFER UNVERIFIED

Claim	Super-administrator access to a finance department web system (800 USD, April) and a reconnaissance package on a government department's AI and web stack (March).
What we can establish	Separate sellers offered entry points into government web and AI systems rather than finished datasets. The March package is the clearest example in our data of AI-platform reconnaissance offered for sale.
Alternatives	Access to a low-value sub-application; reconnaissance built from public scanning only.
Limits	No proof screenshots were available to us; validity and scope are unknown.
Response	Government entities should inventory internet-facing AI orchestration endpoints and end-of-life portals, enforce single sign-on on content-management platforms and remove local administrator accounts (**§12.1** row 4).
BOTTOM LINE	**Entry points, not datasets, were on sale; inventory internet-facing admin and AI endpoints.**

F

CASE F

A confirmed retail-loyalty incident and a leak-site listing in the same week

Retail

INCIDENT CONFIRMED BY THE COMPANY

Claim	On 10 November a ransomware leak-site group listed Landmark Group, the Dubai-based retail group, according to Ransompedia [S5].
Official account	On 11 November Landmark Group said it had identified unauthorised access to one of its systems affecting members of its Shukran loyalty programme. It said names, contact details and dates of birth may have been exposed, card details were not affected, and statutory and law-enforcement authorities had been informed [S24][S25].
What we can establish	A confirmed incident at the company and a leak-site claim against it within a day. The company did not mention a ransomware group, so we have not established that the two refer to the same event.
Response	Loyalty-programme members should expect phishing that quotes their name and birth date. Retailers running loyalty platforms should treat them as identity systems: monitor exports, protect administrator access with MFA and prepare member notices in advance (**§12.1** rows 14-15).
BOTTOM LINE	**A confirmed loyalty-platform incident; members' names and birth dates may have been exposed, so expect phishing that quotes them.**

4.7 What the forums add

Forums contributed only 381 tagged posts, but they carry almost all organisation-specific claims (Cases A-E). Most forum hits are still global lead lists that name the UAE among dozens of countries. Buyers also posted requests: for agency CRM data (B20), an international airport operator's customer data and an "Emirates ID database" in November. Demand for UAE identity and property data is itself a finding.

KEY TAKEAWAYS

01

Raw volume is dominated by multi-country bot templates; read cleaned counts as an upper bound.

02

Real-estate data is the most frequently advertised UAE-specific category in the reviewed posts; prepare owners for payment-instruction fraud.

03

Government-themed offers are mostly access, reconnaissance and recirculated files; triage provenance before comment.

CHAPTER 5

Targeting examples by sector

05

THIS CHAPTER ANSWERS

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

10

sectors with observed activity, from government to real estate

IN SHORT

The posts below show how criminal and hacktivist actors talk about UAE organisations. Hacktivist claimants named high-profile state, energy and transport targets and claimed disruption. Criminal sellers named real-estate, insurance, education and transport data, and treated the UAE as a market for accounts and identities. Official reports are cited separately. Verify each claim with the named organisation before escalating, and start with the sector's first response.

Victims are described by role under the policy in Appendix A.9, except where an incident was officially confirmed and widely reported. Examples come from the cleaned corpus, the forum posts mentioning the UAE and public reporting. The first responses are starting points; the owned actions, with owners and completion evidence, are in §12.1 (rows 2-4, 6, 14-19).

Government

`DDoS claim` `destructive claim` `access sale` `reconnaissance` `credential lines`

EXAMPLE OF OBSERVED ACTIVITY (ANONYMISED)

DDoS claims against federal government websites (Mar-Apr, Chapter 6); a hack-and-leak and wiper claim against several public-sector bodies in one emirate (Apr, unconfirmed); super-administrator access to a finance department system for 800 USD (Apr); AI-stack reconnaissance (Mar); credential lines for a government e-services login page (Aug); two listings against a transport authority (Apr, Nov)

WHAT IT MEANS

Availability, citizen-data integrity and administrator access are the three exposures

FIRST RESPONSE

Pre-agree status statements; enforce single sign-on and MFA on administrator interfaces

Real estate

`Data sale` `leak` `destructive claim`

EXAMPLE OF OBSERVED ACTIVITY (ANONYMISED)

At least nine owner, tenant, developer and portal datasets (Jan-Nov); a buyer seeking an agency CRM (Feb); a wipe claim against a property platform (Sep)

WHAT IT MEANS

The most frequently advertised UAE-specific data in the reviewed posts; feeds payment-instruction and handover fraud

FIRST RESPONSE

Review CRM exports and partner access; warn owners about payment-change requests

Banking and payments

`Carding` `mule accounts` `cash-out` `credentials`

EXAMPLE OF OBSERVED ACTIVITY (ANONYMISED)

Card-checker output naming 14 UAE issuers (Feb-Mar peak); a finance conference's attendee identity documents left exposed in a vendor's storage, confirmed and secured by the organiser (Feb) [S65]; mule recruitment for business and personal accounts at named banks; payment-link and terminal cash-out; credential lines for a retail bank's login

WHAT IT MEANS

Fraud tooling dominates; intrusion-relevant exposure sits in device data (Chapter 9)

FIRST RESPONSE

Triage current credential listings, then employee devices; monitor merchants for cash-out patterns

Energy and utilities

`Leak claim` `DDoS claim` `OT (operational technology) claim`

EXAMPLE OF OBSERVED ACTIVITY (ANONYMISED)

A relayed 1.3 TB leak claim against an emirate's oil company (Mar); DDoS lists naming an oil and gas company and a utility (Mar); an unspecified "electricity systems" intrusion claim (Jun)

WHAT IT MEANS

The Council's wiper advisory names energy among targeted sectors [S11]

FIRST RESPONSE

Verify OT claims with the system owner; test offline backups and wiper response

Transport and aviation

`Intrusion claim` `leak-site listing` `account resale`

EXAMPLE OF OBSERVED ACTIVITY (ANONYMISED)

A relayed claim of access to an international airport operator (Mar, repeated Aug); a port claim (May); extortion listings against an airline caterer and a low-cost airline (Aug, Oct); loyalty-miles accounts resold

WHAT IT MEANS

Passenger and identity documents are the material exposure

FIRST RESPONSE

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

Insurance

`Data sale`

EXAMPLE OF OBSERVED ACTIVITY (ANONYMISED)

An 80,000-record customer and broker file posted on Telegram and three forums (Jan-Apr; Case A)

WHAT IT MEANS

Policy and payment details make customer phishing credible

FIRST RESPONSE

Review CRM access logs; prepare customer notices

Education

`Recirculated data` `data claims` `ransomware listings`

EXAMPLE OF OBSERVED ACTIVITY (ANONYMISED)

A 2025 student dataset reposted (Jan-May); a school-management dump and passport sets claimed against school groups; eight leak-site listings in education

WHAT IT MEANS

Student and parent data supports phishing and identity fraud

FIRST RESPONSE

Check credential fields in old datasets; reset where reused

Healthcare

`Data sale claim` `extortion listing`

EXAMPLE OF OBSERVED ACTIVITY (ANONYMISED)

A relayed sale of files attributed to an emirate's health authority (Apr); leak-site listings naming three hospital groups by one group whose listings we could not corroborate (Feb)

WHAT IT MEANS

Health identifiers do not expire; verify before notification

FIRST RESPONSE

Compare claimed schemas with real systems before any notice

Retail and consumer

`Confirmed incident` `listing` `access sale`

EXAMPLE OF OBSERVED ACTIVITY (ANONYMISED)

A confirmed loyalty-programme incident at Landmark Group and a leak-site listing the same week (Nov; Case F); a grocery platform's access offered for 100 USD (Jun)

WHAT IT MEANS

Loyalty platforms are identity systems

FIRST RESPONSE

Protect loyalty-admin access with MFA; monitor bulk exports

Telecom

`SIM services` `phishing` `data claim`

EXAMPLE OF OBSERVED ACTIVITY (ANONYMISED)

SIM and virtual +971 number sales; a phishing kit aimed at a national operator; an unsupported claim of a 7-million-record operator database

WHAT IT MEANS

SIM and number services connect to account-recovery fraud

FIRST RESPONSE

Tighten SIM-swap and number-port checks (§12.1 row 18)

Reading across sectors. Organisation-specific claims fall into two groups. Hacktivist claimants named high-profile targets (state portals, energy, ports and airports) and claimed disruption or destruction, with most activity in March and April. Financially motivated sellers named real-estate, insurance and transport data, and otherwise treated the UAE as a market for verified accounts and identities. The second group was active all year and is less visible in the press.

KEY TAKEAWAYS

01

Hacktivist claimants named high-profile state, energy and transport targets, mostly in March-April.

02

Real estate was the most frequently advertised UAE-specific data category in the reviewed posts.

03

For banks and telecoms, the posts point to account-opening, mule and SIM controls rather than to intrusion.

CHAPTER 6

Hacktivism, DDoS and destructive claims

THIS CHAPTER ANSWERS

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

10

DDoS claims in the actor posts we read against UAE targets, all between 2 March and 8 April

INSIDE THIS CHAPTER

6.1 Timeline | 6.2 March-April: many short DDoS claims | 6.3 Destructive and hack-and-leak claims: claim against official account | 6.4 Lessons for defenders

IN SHORT

Hacktivist claims against the UAE clustered in March and April, during the heightened period the national cybersecurity authority described. Most were short DDoS claims against federal and emirate websites, backed only by availability-check links. Larger hack-and-leak and wiper claims against state bodies, an oil company, a port and an airport reached us only through relays and were not confirmed by the named bodies. Pre-agree who confirms service status and test offline backups.

6.1 Timeline

18 Feb 2026 — **UAE Cybersecurity Council**
128 confirmed incidents since 1 January; defacement 38.3% and data leaks 25.8% of the total

22 Feb 2026 — **RipperSec**
Claims leaks of four UAE company databases

28 Feb 2026 — **UAE Cybersecurity Council**
Start of the heightened period later described by the Council's head (to early April)

2 Mar 2026 — **313 Team**
Claims a one-hour DDoS on two federal government websites; further claims to 11 March against several federal bodies

3 Mar 2026 — **Leak-monitor bots**
Relay a Handala claim of 1.3 TB from an oil company in one emirate

6 Mar 2026
DieNet (own bot message, reposted)
DDoS claims against federal government websites

9 Mar 2026
Keymous+
First UAE DDoS target list; six federal sites with availability-check links on 12 March; further lists to 8 April, including energy and utility sites

19 Mar 2026
UAE Cybersecurity Council
Public warning on destructive wiper malware (press report updated 19 March)

27 Mar 2026
coderx
Posts a 16.6 GB database it attributes to a Dubai facilities-management company

30 Mar 2026
Monitor channels
Relay a Nasir Security claim of access to an international airport operator, with passport images claimed

4 Apr 2026
UAE Cybersecurity Council
Advisory on a destructive wiper campaign across sectors; "some organizations have already been impacted"

12 Apr 2026
Security press
Handala claims wiper and data theft at several public-sector bodies in one emirate: 6 PB destroyed, 149 TB stolen

4 May 2026
Aligned channels
Relay a Handala claim against an emirate's port

1 Jun 2026
Golden Falcon
Claims it has begun an intrusion into UAE electricity systems

10 Sep 2026
Aggregator account
Claims export and deletion of a UAE property platform's 49 GB database

15 Sep 2026
Head of the UAE Cybersecurity Council
A hacker who exploited an unpatched vulnerability demanded 5 million USD from a private-sector organisation

18 Nov 2026
Head of the UAE Cybersecurity Council
More than 40 groups from over 20 countries tried to exploit the regional crisis

Dark markers are actor posts, outlined markers are relays by third parties, coral markers are official statements. Dates are post or statement dates. Sources: actor posts and relays [S1]; official statements [S9][S12][S11][S17][S22]; Handala's April claim [S26].

6.2 March-April: many short DDoS claims

The DDoS claims were short, public and thinly evidenced. We hold 22 actor posts claiming action against UAE targets. In the posts we read, all ten DDoS claims among them fall between 2 March and 8 April, from 313 Team, Keymous+ and Cyber Fattah. DieNet's claims reached us only as reposts of its bot messages (from 1 March) and are not among the ten. The targets were federal government websites, emirate government and media-office sites, energy and utility websites and one bank's public site. The proof offered was availability-check links: snapshots of reachability from a handful of probe locations. They can record a moment of unreachability, not an outage.

EVIDENCE CARD B21 — 2 Mar 2026

313 Team Actor channel · Telegram · Arabic, English

ORIGINAL

هجوم سيبراني استهدف خوادم الرئيسية لحكومة الامارات حيث ادى الهجوم الى تعطل [موقع حكومي اتحادي 1] و[موقع حكومي اتحادي 2] [...] سيستمر الهجوم لمدة ساعة كاملة.

TRANSLATION

A cyberattack targeted the main servers of the UAE government, disrupting [federal government website 1] and [federal government website 2] [...] The attack will last a full hour.

Note. One of four 313 Team claims (2-11 Mar) against federal and emirate government websites.

HELD	The group claimed a one-hour DDoS against two federal government websites on 2 March.
NOT ESTABLISHED	It does not establish any outage beyond the actor's own Check-Host links.

EVIDENCE CARD B22 — 12 Mar 2026

Keymous+ Actor channel · Telegram · English

ORIGINAL

```
United Arab Emirates : [federal government website] Check Host [...] [federal ministry 1] Check Host [...] [federal ministry 2] Check Host [...] [federal ministry 3] Check Host [...] [federal ministry 4] Check Host [...] [federal ministry 5] Check Host
```

Note. Keymous+ posted at least five UAE target lists between 9 Mar and 8 Apr, including an oil and gas company and a utility.

HELD	Keymous+ listed six federal government sites as DDoS targets, with Check-Host links offered as proof.
NOT ESTABLISHED	It does not establish service impact; Check-Host results capture a moment from a few probe locations.

Independent measurement confirms more DDoS, mostly low-volume. StormWall reported that the UAE's share of regional DDoS activity rose from 14% to 26% between the first quarters of 2025 and 2026. It put attacks on the UAE up 86% year on year [S30]. Help AG counted 236,560 DDoS attacks on UAE networks in the first half of 2026, 91% of them low-volume [S35]. Neither source reported a lasting national outage.

6.3 Destructive and hack-and-leak claims: claim against official account

The most serious claims came from Handala, a brand that Security Affairs describes as presenting itself as a pro-Palestinian hacktivist group but widely seen as a front for an Iran-backed actor [S26]. Its posts reached our data only through relays.

Point	Handala's claim (12-13 April)	Official account	Independent reporting
Targets	Several public-sector bodies in one emirate	No statement addressing the claim found by our cut-off	Claims "remain unverified" [S26]

Point	Handala's claim (12-13 April)	Official account	Independent reporting
Effect	6 PB of data destroyed	The Council's 4 April advisory described an active regional wiper campaign without naming victims [S11]	Not measured
Data	149 TB stolen	Not stated	Not verified [S26]
Attribution	Own claim	The Council's head made attribution statements on other occasions (§2.4)	Front for an Iran-backed actor, as described by Security Affairs [S26]

What we can establish. A brand that Security Affairs links to an Iran-backed actor [S26] claimed a wiper attack on state bodies, and the national authority had warned of an active wiper campaign eight days earlier. The claimed volumes are very large for bodies of this kind, and no named body confirmed an incident by our cut-off. We do not compute or imply a ratio between claim and reality.

The same pattern held for the other large claims. Handala claimed 1.3 TB from an oil company in one emirate (3 March) and data from a port (4 May). Nasir Security claimed months of access to an international airport operator (30 March, repeated in August), and it also claimed a customs authority (August) [S66]. All were relayed but not confirmed by the named bodies by our cut-off. Public monitors reported both the port and airport claims as allegations [S27][S28].

The private-sector case the authorities did describe. On 15 September the head of the Council said a hacker exploited an unpatched vulnerability at an unnamed private-sector organisation, claimed access to its systems, threatened to expose its data and demanded 5 million USD. Khaleej Times reported that some information was later published on the dark web; Gulf News reported that the leak was prevented [S17][S67]. The organisation was not named.

EVIDENCE CARD B23 — 27 Mar 2026

coderx Breach forum · Forum · English

ORIGINAL

```
16GB [Dubai facilities-management company] DATABASE [...] Leaking 16GB Database Of [Dubai facilities-management company] [...] Number Of Files: 1 Original Size: 16.6 GB Compressed Size: 696 MB
```

Note. The post's political statements are left out here.

HELD	An actor posted a 16.6GB database it attributed to a Dubai facilities-management company.
NOT ESTABLISHED	It does not establish that the file is what the actor says it is.

EVIDENCE CARD B24 — 1 Jun 2026

Golden Falcon Actor channel · Telegram · English

ORIGINAL

```
The attack on the UAE's electricity systems has begun [...] It was just a small warning, and this time we just agreed to read the data
```

Note. Relayed by a monitor channel the next day; no follow-up in the corpus.

HELD	A group claimed it had begun an intrusion into UAE electricity systems and limited itself to reading data.
NOT ESTABLISHED	It does not name an operator or system, show proof, or establish any effect on power supply.

The only wiper-style claim against a UAE company in our data came later, in September, from an actor who said it exported and then deleted a property platform's database (B05). No outage or confirmation followed in the sources we reviewed.

EVIDENCE CARD B05 — 10 Sep 2026

Aggregator account (actor handle withheld)

Leak aggregator forum · Forum · English

ORIGINAL

```
49GB of [UAE real-estate platform] Database Leaks
[...] today I [contact removed] gained access to a
database of a real estate company in the United
Arab Emirates. After exporting the entire database
i also wiping everything out.
```

Note. This is the only wiper-style claim against a UAE company in the corpus.

HELD	An actor claimed to have exported a UAE property platform's 49GB database and then deleted it.
NOT ESTABLISHED	It does not establish that any deletion took place or that the platform lost service.

6.4 Lessons for defenders

1. **Prepare for wipers, not only for encryption.** The Council's own advisory describes destructive malware entering through phishing, stolen VPN credentials and unpatched systems [S11]. Test that offline backups restore within the recovery time you have promised (§12.1 rows 4, 6 and 17).
2. **Pre-agree the public line.** Hacktivist numbers are designed to be quoted. Decide in advance who confirms service status, within what time and through which channel (§12.1 row 16).
3. **Protect portals upstream.** Short, repeated DDoS claims target public portals. Contract upstream mitigation before the next heightened period (§12.1 row 9).
4. **Verify OT claims before escalation.** A claim of access to "electricity systems" without a named system owner is a reason to check, not to announce (B24; §12.1 row 16).

KEY TAKEAWAYS

01 — Hacktivist DDoS claims clustered in March-April and rested on availability-check links.

02 — Destructive and hack-and-leak claims against state bodies, energy, a port and an airport stayed unconfirmed by the named bodies.

03 — The authority's own wiper advisory names the controls: phishing defence, VPN credential hygiene, patching and restorable backups.

CHAPTER 7

Threat actors

07

THIS CHAPTER ANSWERS

Which actor types matter for the UAE, how are they connected, and what does public reporting say about each?

4

actor types: state-linked espionage, destructive hack-and-leak, ransomware and fraud networks

INSIDE THIS CHAPTER

7.1 How the actors connect | 7.2 State-linked espionage | 7.3 Destructive hack-and-leak and hacktivist actors | 7.4 Ransomware and extortion | 7.5 Fraud networks and criminal personas

IN SHORT

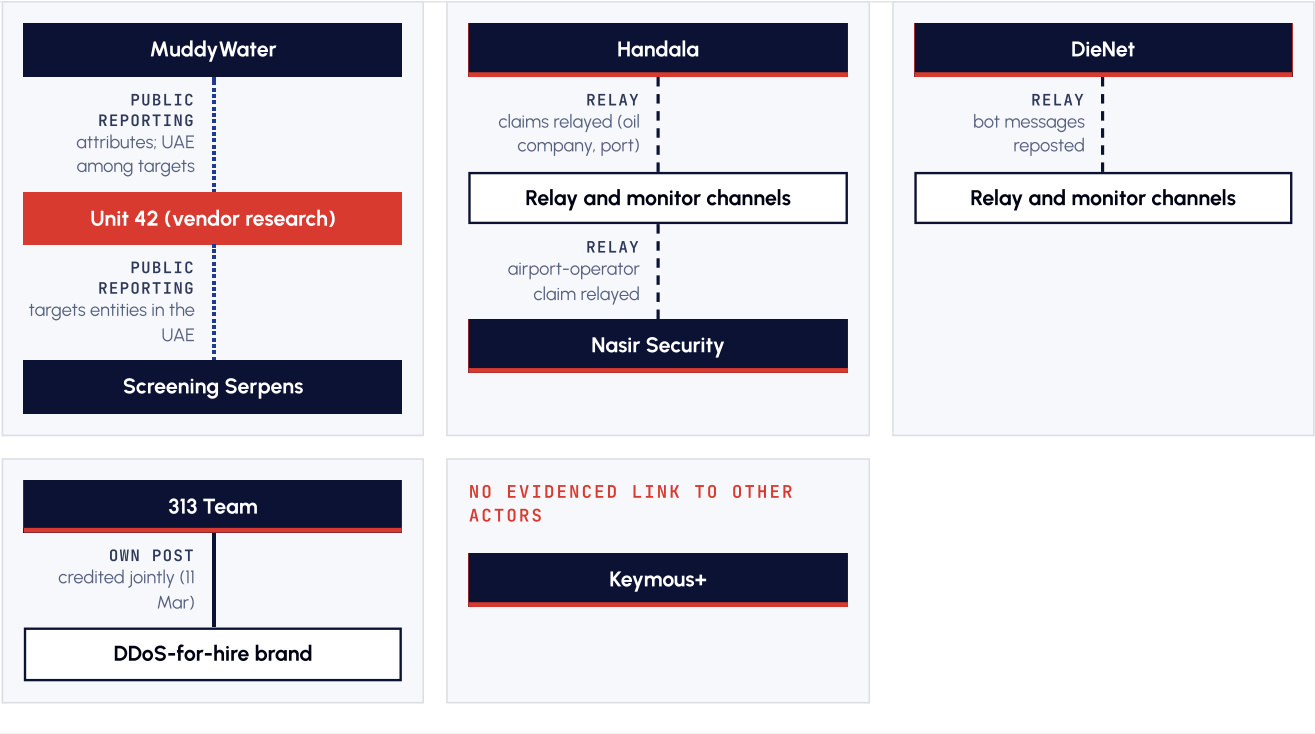
Four actor types matter for the UAE in 2026. Vendors reported state-linked espionage against UAE entities through phishing and job lures. A hack-and-leak brand claimed destructive attacks on state bodies, unconfirmed by them. Ransomware and extortion groups listed dozens of UAE companies, mostly private firms. Fraud networks abused UAE payment and identity channels. Patch edge systems; hunt side-loaded DLLs, remote-management tools and unusual outbound traffic from mail and CRM servers; verify every claim before comment.

Each profile separates **what the source observed**, **the attribution as the source states it**, **what remains unresolved** and **what it means for organisations**. Confidence applies to a specific proposition, not to an actor as a whole. Attributions are the sources' own; we make none.

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 State-linked espionage

MuddyWater (Boggy Serpens)

Boggy Serpens (Unit 42 name)

Espionage (state-linked per vendor)

Attributed by Unit 42 to Iran's Ministry of Intelligence and Security

UAE-RELEVANT REPORTING, 2026

Jan-Feb	Wave against a Middle East marine and energy company; one lure used dirham payroll records
Mar	Unit 42 lists the UAE among countries struck by recent campaigns

TARGETED SECTORS

Government and corporate entities; a marine and energy company in the region

SEEN IN PUBLIC REPORTING

- [S31] Unit 42 (16 Mar 2026): attribution as stated; phishing from hijacked official and corporate mail accounts; remote-management tools (Atera, ScreenConnect, SimpleHelp) in earlier campaigns; custom implants in 2025-26

OUR ASSESSMENT

The UAE-relevant risk is phishing sent from trusted, hijacked mailboxes. In earlier campaigns legitimate remote-management tools followed, blending with IT traffic; in 2025-26 the vendor reports custom implants.

CONFIDENCE **Vendor attribution; UAE targeting stated by the vendor**

Screening Serpens

UNC1549, Smoke Sandstorm, Iranian Dream Job (per Unit 42)

Espionage (state-linked per vendor)

Iran-nexus, per Unit 42 (moderate-high confidence that the campaigns are this group's)

UAE-RELEVANT REPORTING, 2026

Apr	A new variant that may have targeted an entity in the UAE
May	Unit 42 reports targeting of entities in the US, Israel and the UAE

TARGETED SECTORS

Entities in the UAE (sector not published)

SEEN IN PUBLIC REPORTING

- [S32] Unit 42 (22 May 2026): recruitment and fake meeting-invite lures; MiniUpdate and MiniJunk V2 malware; DLL side-loading and AppDomainManager hijacking

OUR ASSESSMENT

Job-offer and meeting-invite lures aimed at individual staff; detection rests on endpoint telemetry for side-loaded DLLs in user-writable paths.

CONFIDENCE **Moderate-high (vendor)**

TECHNIQUES NAMED IN THE VENDOR RESEARCH, BY TACTIC

Initial access	Command and control	Defence evasion	Persistence / defence evasion
(no ID given) Phishing sent from hijacked official and corporate mailboxes (Unit 42, MuddyWater)	T1219 Remote access software: Atera, ScreenConnect, SimpleHelp, in earlier campaigns (Unit 42, MuddyWater)	T1055.012 Process hollowing (Unit 42, MuddyWater)	T1574.001 DLL side-loading, as labelled by Unit 42 (Screening Serpens)
			T1574.014 AppDomainManager hijacking (Unit 42, Screening Serpens)

Technique IDs as linked in Unit 42's reports of 16 March and 22 May 2026. The phishing row has no ID in the source. [S12]

An unattributed intrusion into a defence company. ESET reported the compromise of a defence company in the UAE through a SmartOffice CRM server, followed by custom post-exploitation and reverse-proxy tools. ESET listed it among lesser-known and unattributed clusters [S33]. No CVE was published for the entry point.

Internet-exposed cameras were targeted. Check Point reported a sharp rise in exploitation attempts against IP cameras in the UAE and other Gulf states from 28 February, from infrastructure it attributes to Iranian actors [S58]. The flaws it highlighted include CVE-2017-7921 in Hikvision cameras and CVE-2021-33044 in Dahua devices. NVD rates both 9.8, and both are in CISA's known-exploited catalogue [S59][S60]. Affected and fixed firmware differ by model (table below) [S68][S69]. A free list of about 185,000 exposed UAE camera streams circulated on 5 March (B11), and in November the head of the

Council described attempts to hack home, farm and car cameras [S23]. Patch or remove internet exposure of camera management interfaces (§12.1 row 5).

CVE	Product series	Affected firmware	Fixed firmware
CVE-2017-7921	Hikvision DS-2CD2xx2F-I	V5.2.0 build 140721 to V5.4.0 build 160530	V5.4.5 build 170123 or later
CVE-2017-7921	Hikvision DS-2CD2xx0F-I	V5.2.0 build 140721 to V5.4.0 build 160401	V5.4.5 build 170123 or later
CVE-2017-7921	Hikvision DS-2CD2xx2FWD	V5.3.1 build 150410 to V5.4.4 build 161125	V5.4.5 build 170124 or later
CVE-2017-7921	Hikvision DS-2CD4x2xFWD	V5.2.0 build 140721 to V5.4.0 build 160414	V5.4.5 build 170228 or later
CVE-2017-7921	Hikvision DS-2CD4xx5	V5.2.0 build 140721 to V5.4.0 build 160421	V5.4.5 build 170302 or later
CVE-2017-7921	Hikvision DS-2DFx	V5.2.0 build 140805 to V5.4.5 build 160928	V5.4.9 build 170123 or later
CVE-2017-7921	Hikvision DS-2CD63xx	V5.0.9 build 140305 to V5.3.5 build 160106	V5.4.5 build 170206 or later
CVE-2021-33044	Dahua IPC-HX1XXX to HX8XXX and HUM7XXX cameras	Builds dated before June 2021	Per-model firmware dated July 2021 or later, for example V2.820.0000000.33.R.210705 (HX1XXX)
CVE-2021-33044	Dahua SD-series PTZ domes (SD1A1, SD22, SD49, SD50, SD52C, SD6AL)	Builds dated before June 2021	V2.812.0000007.0.R.210706 or later
CVE-2021-33044	Dahua TPC thermal cameras	Builds dated before June 2021	Per-model firmware dated July 2021, for example V2.630.0000000.6.R.210707 (TPC-BF1241)
CVE-2021-33044	Dahua VTO and VTH intercoms	Builds dated before June 2021	V4.300.0000003.0.R.210714 (VTO75X95X), V4.300.0000004.0.R.210715 (VTO65XXX), V4.500.0000002.0.R.210715 (VTH542XH)

Hikvision versions are those listed in the ICS-CERT advisory; devices running unauthorised firmware may not accept the update. Check the exact model against the advisory; one firmware version does not fix every model [S68][S69].

Unresolved. Victim identities, data taken and dwell time are not public for any of these cases. **Meaning.** The common entry routes are hijacked trusted mail accounts, recruitment lures and internet-facing business applications. Alert on new remote-management tools, on DLL side-loading from user-writable folders and on unusual outbound connections from CRM and mail servers (§12.1 rows 4 and 7).

7.3 Destructive hack-and-leak and hacktivist actors

Handala

Handala Hack

Hack-and-leak, destructive claims

Presents itself as pro-Palestinian; described by Security Affairs as widely seen as a front for an Iran-backed actor

2026 IN THE UAE

3 Mar	Claim of 1.3 TB from an oil company in one emirate (relayed)
12-13 Apr	Claim of wiper and theft at several public-sector bodies in one emirate: 6 PB destroyed, 149 TB stolen
4 May	Claim against an emirate's port (relayed)

CLAIMED TARGETS

State bodies, energy and a port

SEEN IN PUBLIC REPORTING

- [S26] Security Affairs (13 Apr 2026): the April claims remain unverified; describes the brand and its reported links
- [S27] A security vendor's news page (May 2026) reported the port claim, citing only the group's own claims

OUR ASSESSMENT

The most consequential claimant by stated intent. None of its 2026 UAE claims was confirmed by the named bodies by our cut-off; its posts reached our data only through relays.

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

Nasir Security

Nasir Resistance

Hack-and-leak claims

Not established; the group's own framing is political

2026 IN THE UAE

30-31 Mar	Claim of months-long access to an international airport operator, with passport images and internal documents claimed (relayed)
22 Aug	Renewed claim against the same operator
22 Aug	Claim against a customs authority, posted the same day (S66)

CLAIMED TARGETS

Aviation (airport operator); a customs authority

SEEN IN PUBLIC REPORTING

- [S28] A public breach monitor reported the March claim as alleged

OUR ASSESSMENT

A claimant focused on a few state-linked targets, whose evidence did not reach our data directly. The claim is a reason to check partner and document-management access, not to announce a breach.

CONFIDENCE **Claim relayed; unverified**

313 Team

Hacktivist (DDoS)

Self-described religious and political framing (as reported by The National); self-declared targeting of six countries including the UAE; state links not verified (CloudSEK, via The National)

2026 IN THE UAE

2 Mar	One-hour DDoS claim on two federal government websites (B21)
3 Mar	DDoS claim on an emirate's media-office site
11 Mar	DDoS claim on a federal government website, credited jointly with a DDoS-for-hire brand

CLAIMED TARGETS

Federal and emirate government websites

IN THEIR WORDS

> *"The attack will last a full hour."* B21

SEEN IN PUBLIC REPORTING

- [S29] The National (2 Mar 2026): the group publicly declared it was targeting the UAE among six countries; CloudSEK could not verify state links

OUR ASSESSMENT

A repeat DDoS claimant whose evidence is availability-check links. No claimed outage was confirmed by the named organisation or an authority.

CONFIDENCE **High that it claimed; impact unverified**

Keymous+

Hacktivist (DDoS) | Not established

2026 IN THE UAE

9 Mar	DDoS list: a federal ministry, an oil and gas company and a utility
12 Mar	Six federal sites listed with availability-check links (B22)
25 Mar	An oil and gas company and a utility in a ten-country energy list
6-8 Apr	Four further federal ministry sites

CLAIMED TARGETS

Federal ministries, energy and utility websites

IN THEIR WORDS

> *"[federal government website] Check Host"* B22

SEEN IN PUBLIC REPORTING

- No reputable public reporting on its UAE claims found in our sweep

OUR ASSESSMENT

The most frequent UAE DDoS claimant in our data (five lists). Its proof consists of probe snapshots only.

CONFIDENCE **High that it claimed; impact unverified**

DieNet

Hacktivist (DDoS)

Not established; named in press coverage among groups claiming attacks in the region

2026 IN THE UAE

1-9 Mar — Automated claim messages reposted by aligned channels: several federal government websites

CLAIMED TARGETS

Federal government websites

SEEN IN PUBLIC REPORTING

- [S29] The National (2 Mar 2026): named among groups claiming attacks in the region; claims not independently verified

OUR ASSESSMENT

Claims reached us through reposts of the group's own bot messages; none was confirmed.

CONFIDENCE **Claim relayed; unverified**

Other claimants posted less often: RipperSec claimed four UAE company databases in February, Cyber Fattah a bank website in March, coderx a facilities-management database in March and Golden Falcon an electricity intrusion in June. None of these claims was confirmed by the named organisation or an authority, and we found no reputable public reporting that corroborates them.

7.4 Ransomware and extortion

UAE ransomware listings in 2026 far exceed those of four Gulf comparators

UNITED ARAB EMIRATES

84

Accepted listings, 1 Jan-20 Nov 2026

2025	ALL TIME
48	220

GROUPS IN 2026
Krybit, The Gentlemen, INC Ransom, N0n, 0apt

SAUDI ARABIA

30

Accepted listings, 1 Jan-20 Nov 2026

2025	ALL TIME
27	94

GROUPS IN 2026
The Gentlemen, N0n, Hyflock, APT73, INC Ransom

QATAR

9

Accepted listings, 1 Jan-20 Nov 2026

2025	ALL TIME
5	24

GROUPS IN 2026
Qilin, The Gentlemen, N0n, Akira, Payload

KUWAIT

7

Accepted listings, 1 Jan-20 Nov 2026

2025	ALL TIME
6	29

GROUPS IN 2026
LockBit 5, N0n, The Gentlemen, Everest, Tengu

OMAN

9

Accepted listings, 1 Jan-20 Nov 2026

2025	ALL TIME
6	27

GROUPS IN 2026
The Gentlemen, LockBit 5, Vexy-ransomware, Cl0p, Spirals

Source: Brandefense Ransompedia accepted listings, all dates, to 20 November 2026 [S5]; ransomware.live as a cross-check [S7].

Ransomware and extortion listings are frequent and mostly name private firms. Ransompedia holds 84 accepted UAE listings dated 1 January-20 November 2026, against 48 in all of 2025 [S5]. Five of the 84 are not victim organisations or are clearly not UAE-based (for example a group's own channel announcement), and five repeat an organisation already listed, leaving 74 distinct organisations. The four Gulf comparators had far fewer in the same window: Saudi Arabia 30, Qatar 9, Oman 9 and Kuwait 7. These comparator figures are raw listing counts, not cleaned the same way.

Measure (UAE, 2026 to 20 November)	Value
Accepted listings	84 (74 distinct plausible UAE organisations)
Most active groups	Krybit 8, The Gentlemen 7, INC Ransom 7, N0n 5, 0apt 4
Most named sectors	Education 8, retail 8, construction 7, consulting 7
Busiest months	October 13 and November (to the 20th) 12

A listing is a criminal claim. One group listed three hospital groups and a conglomerate on a single day in February; we could not corroborate its listings, and none of those organisations confirmed an incident. The only 2026 listing we can set against an official statement is the retail-loyalty case (Case F, §4.6). The Council's figures put ransomware at 7.8% of 128 confirmed

incidents by mid-February [S9]. Leak-site listings and confirmed incidents measure different things, so the two figures cannot be reconciled.

A public tracker listed 70 UAE-labelled victims for the year [S7]. Several of its labels, and some of Ransompedia's, belong to companies based elsewhere. We removed entries that are clearly not UAE victim organisations; the remaining labels were not each verified.

7.5 Fraud networks and criminal personas

Criminal personas in our data are mostly sellers who name the UAE as one market among many. A smaller set posted UAE-specific offers. They include the seller of the insurer file (Case A), sellers of real-estate datasets (Case C) and two aliases behind the transport-authority listings (Case B). Others sold access and reconnaissance against government systems (Case E), and one actor offered population lists (B10). We print aliases as posted and withhold contacts. No shared concrete element links these personas to each other or to the hacktivist brands; any grouping of them would be an analytical model, not an observation.

Fraud groups outside our post data matter too. Recorded Future's reporting on the Tajin group describes abuse of UAE payment gateways for card fraud and money laundering [S34]. Police operations in April and October dismantled fraud centres and blocked thousands of bank accounts (§8.5).

KEY TAKEAWAYS

01

Vendors reported state-linked espionage against UAE entities through hijacked mail accounts and job lures.

02

Destructive hack-and-leak claims against state bodies stayed unconfirmed by them; prepare to verify before comment.

03

Ransomware listings name mostly private firms, most often in education, retail, construction and consulting.

CHAPTER 8

The fraud economy

THIS CHAPTER ANSWERS

How are UAE identities, accounts and payment channels turned into money, and what did the police report?

960+

arrests in one 30-country fraud operation led by the Ministry of Interior (July-September)

INSIDE THIS CHAPTER

8.1 Bank, wallet and payment-account trading
8.2 Card material in posts: a narrow view
8.3 Identity, KYC and SIM services
8.4 Prices in context
8.5 Official and vendor warnings

IN SHORT

The most persistent UAE-specific fraud thread in our data is a market in residents' verified accounts: bank, wallet, remittance and exchange accounts tied to an Emirates ID or residence card. Around it sit card cash-out through payment links and terminals, KYC services and impersonation scams that the police warned about all year. Treat account-opening and recovery as fraud controls, and monitor payment-link merchants as closely as cardholders.

8.1 Bank, wallet and payment-account trading

UAE accounts tied to a real identity are the commodity. Channels recruiting "loaders" (people who fund or operate accounts for fraud) asked for fresh UAE remittance and wallet accounts linked to a valid Emirates ID, quoting confirmed limits of 10,000 AED (B13). A June post sought business accounts at two UAE banks, handed over "face to face" with SIM, debit card, Emirates ID and online-banking access, for 50,000-150,000 USD of transfers (B14). Russian-language forum posts recruited handlers for personal accounts at the same two banks (B15).

EVIDENCE CARD B13 9 Feb 2026

Anonymous poster Telegram channel · Telegram · English

ORIGINAL

```
Bring UAE [remittance app] Fresh only with
emirates id 10k AED CONFIRM [...] guarantee
```

Note. Part of a January-November family of posts that recruit UAE residents to lend verified payment and wallet accounts.

HELD	Loader channels sought fresh UAE remittance-app accounts tied to a valid Emirates ID with a 10,000 AED confirmed limit.
NOT ESTABLISHED	It does not establish how many accounts were supplied or who the account holders are.

EVIDENCE CARD B14 4 Jun 2026

Anonymous poster Telegram channel · Telegram · English

ORIGINAL

```
Anybody have [UAE bank A] Business or [UAE bank B]
Business in Dubai [...] 50k-150k USD Work. *face
to face* • Sim Card • Debit Card • Emirates ID
(Phone number & account holder) • Bank logs •
Email
```

Note. The same text ran in another channel on 4 May; Russian-language drop-handler adverts named the same two banks on 22 Jun.

HELD	A buyer sought UAE business bank accounts with the holder's SIM, debit card, Emirates ID and online-banking access for USD 50k-150k in transfers.
NOT ESTABLISHED	It does not establish that any account was handed over.

EVIDENCE CARD B15 22 Jun 2026

SOQA Carding/fraud forum · Forum · Russian

ORIGINAL

```
Нужны дроповоды под физ банки [UAE bank A], [UAE
bank B] UAE. Отличные условия по работе.
```

TRANSLATION

Need drop handlers for personal accounts at [UAE bank A] and [UAE bank B], UAE. Excellent working conditions.

Note. Two further adverts (Jul, Aug) offered UAE drops able to register merchants, bank accounts and exchange accounts.

HELD	A Russian-language forum post recruited handlers of money-mule personal accounts at two named UAE banks.
NOT ESTABLISHED	It does not establish that mule accounts at these banks exist or are in use.

Card cash-out also targets UAE payment infrastructure. A November forum post claimed control of card-present terminals in Dubai and sought foreign card dumps (copied magnetic-stripe data) to run through them, saying it avoids Gulf-issued cards (B17). Telegram posts recruited "shooters" to push stolen cards through UAE payment links. Recorded Future reported that a Chinese-speaking fraud group, Tajin, used merchant accounts and payment links at UAE gateways denominated in dirhams, and assessed it "possible" that the group impersonated legitimate UAE businesses [S34].

EVIDENCE CARD B17 — 17 Nov 2026

z3fraan Carding/fraud forum · Forum · English

ORIGINAL

```
i have POS in Dubai and Oman working with swiping cards "white cards" [...] i need cards or dumps from Europe and USA or Africa and worldwide no problem [...]
```

Note. The poster says it avoids Gulf-issued cards, which points the risk at merchant acquiring and foreign issuers rather than local cardholders.

HELD	A forum user claimed control of card-present POS terminals in Dubai and sought foreign card dumps to cash out through them.
NOT ESTABLISHED	It does not establish that the terminals exist or which acquirer serves them.

Regional context: crypto fraud. A separate October post recruited traffic suppliers for a crypto approval drainer aimed broadly at Middle East merchants and individuals who accept crypto (B18). It does not establish UAE targeting or bank-card cash-out.

EVIDENCE CARD B18 — 5 Oct 2026

Moon_7thShift Carding/fraud forum · Forum · English

ORIGINAL

```
We need people who know how to generate traffic for multichain approval USDT drainer [...] Traffic is needed in the direction of invoices (crypto checks), we mainly need small entrepreneurs and individuals who accept payments in cryptocurrency; rich countries of the Middle East
```

Note. Reposted on a second forum the same day.

HELD	An operator recruited traffic suppliers for a crypto approval drainer aimed at Middle East merchants and individuals who accept crypto.
NOT ESTABLISHED	It does not establish any UAE victims or losses.

8.2 Card material in posts: a narrow view

SCOPE OF THE CARD FIGURES

These figures cover 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 that are not covered here. The figures are not a measure of card theft or fraud loss.

We counted 631 distinct UAE-associated cards in clear text in collected posts [S6]. Of these, 504 were attributed in the post to one of 14 named UAE issuers and 127 carried only a UAE country label. The two most frequent issuers account for 281 of the 504. Most appear in card-checker bot output from February and March. Because August and October were sampled and September was not read, the count is a lower bound. The report publishes issuer-level counts only.

8.3 Identity, KYC and SIM services

Residence-card KYC is a steady market. Buyers offered 5-40 USD per crypto-exchange or fintech account verified with a UAE residence card (B16). Sets of UAE ID and passport images with selfies were offered for 2.5-10 USD. Virtual or Telegram-registered +971 numbers sold for about 1.5 USD. These services connect directly to account-opening fraud and to the mule accounts in §8.1.

EVIDENCE CARD B16 — 24 Feb 2026

Anonymous poster Telegram channel · Telegram · English, Arabic

ORIGINAL

```
Wtb [crypto exchange] United Arab Emirates [...]
Price : 40$ Escrow++ You need just Residence card
تحتاج فقط بطاقة الإقامة للتوثيق
```

Note. UAE residence-card KYC was in steady demand across exchanges and fintech apps; quoted prices ran from $5 to $40 per account.

HELD	A buyer offered $40 per crypto-exchange account verified with a UAE residence card.
NOT ESTABLISHED	It does not establish how many accounts were bought or which residents took part.

EVIDENCE CARD B19 — 29 Oct 2026

RummRif Carding/fraud forum · Forum · English

ORIGINAL

```
750k Forex/Crypto Database From UAE For Use
●Recovery ●Depositors ●High Investors [...]
Sample: Email Name Phone Country Assigned To
Account Status Brand Name Original Retention Owner
FTD Currency Total Deposited In USD
```

Note. The column names look like a broker call-centre CRM; "recovery" lists are used to target people who have already lost money.

HELD	A seller listed 750,000 forex and crypto depositor records described as from the UAE, with deposit amounts, for use in recovery scams.
NOT ESTABLISHED	It does not establish the source brokers or that the depositors live in the UAE.

Leads lists are the input to call-centre fraud. A seller listed 750,000 forex and crypto depositor records described as UAE-linked, with deposit amounts, explicitly for "recovery" scams that target people who have already lost money (B19).

8.4 Prices in context

Item (UAE-related, as advertised)	Price	Card
Insurer customer file, 80,000 records	200 USD	B01
Developer customer and identity-document data	100 USD	B02
Super-administrator access to a government web system	800 USD	B08
Transport-authority dataset, 50GB claimed	5,000 USD	B03
Exchange account verified with a UAE residence card	5-40 USD	B16

Item (UAE-related, as advertised)	Price	Card
UAE ID or passport image set with selfie	2.5-10 USD	n/a
Virtual +971 number	about 1.5 USD	n/a

Prices are asking prices in posts. They say nothing about whether a sale happened or whether the goods were genuine, and sellers inflate and recycle.

8.5 Official and vendor warnings

Official and vendor warnings described the same patterns from the victim's side.

Date	Body	What was reported	Source
2026-03-02	Dubai Police	Callers posing as crisis-management staff seek UAE PASS and Emirates ID data for SIM swaps and banking-app takeover	[S49]
2026-03-09	DFSA (Dubai Financial Services Authority)	Firms impersonating authorised firms and cloned public-register domains	[S53]
2026-03-10	Netcraft (vendor)	Hundreds of "AE GOV" e-mails with the interior ministry's logo, sent from 4 March, pushed a fake registration form. A lookalike customs parcel site asked for a 20 AED fee	[S61]
2026-04-11	Dubai Police	Rise in fake calls and SMS posing as officials and bank staff seeking passwords and one-time codes	[S47]
2026-04-11	Public Prosecution	A network sent fake toll and fine SMS, some for 4 AED, to harvest card data. 35 reports, arrests including one local suspect, 22 card terminals seized	[S62]
2026-04-17	Unit 42 (vendor)	Fake payment pages using postal-service themes, and fake fine-payment flows impersonating Dubai authorities, collected card data	[S64]
2026-04-25	Abu Dhabi Police	Fake social-media accounts selling tickets, visa services, vehicles and investments, and requesting data under parcel-delivery pretexts	[S50]
2026-04-29	Dubai Police	276 arrests and nine fraud centres dismantled with US and Chinese police	[S45]
2026-04-30	ICP (the federal identity and citizenship authority)	Calls and websites used its name and logo to obtain personal data. ICP warned never to share one-time passwords or digital-identity codes	[S63]
2026-07-05	Sharjah Police	Seven arrested for impersonating officials and getting victims to install apps that gave access to their phones; bank accounts opened in other people's names	[S51]
2026-07-07	Dubai Police	Fake consumer-protection sites followed by calls pushing remote-access software during online banking	[S48]

Date	Body	What was reported	Source
2026-10-22	Ministry of Interior	More than 960 arrests and 4,126 bank accounts blocked in a 30-country operation, 1 July-30 September	[S46]
2026-10-23	Dubai Police	Six arrested over a fake shopping site that harvested card data	[S52]

Reading across both views. The posts and the police reports describe the same chain: identity data and residence cards feed account opening, mule accounts move money, and remote-access tools and fake officials take over victims' sessions. The central bank's refund duty for SMS-only fraud (§10.3) shifts part of that cost onto institutions.

KEY TAKEAWAYS

01

Verified UAE accounts tied to an Emirates ID or residence card are the core fraud commodity.

02

Payment links and card-present terminals are cash-out channels; monitor merchants, not only cardholders.

03

Police warnings and dark-web posts describe the same chain: identity data, mule accounts and remote-access takeover.

CHAPTER 9

Banking and finance deep dive

THIS CHAPTER ANSWERS

Where does the visible exposure of UAE banks sit, and which of it points to intrusion rather than to customer fraud?

12 of 23

banks in our list with a credential listed for sale on the day of the check

INSIDE THIS CHAPTER

9.1 Where the exposure sits | 9.2 What posts say about UAE banks | 9.3 What the regulator changed | 9.4 What banks should do

IN SHORT

All 23 banks in our list have infected devices associated with their domains, but 98% of those devices are outside the employee classification, and their ownership remains unverified. All 23 bank domains publish an enforcing DMARC policy. Twelve had a current credential listing, and posts name UAE banks in mule recruitment and card-checker output. Triage the listings and the 543 employee-classified devices first, then harden account opening and recovery.

This chapter uses aggregates only. The 23 banks are the central-bank-licensed banks in the 250-organisation list, including two foreign banks' UAE operations and one development bank. Payment firms, exchanges and investment bodies are in the wider banking and finance sector (Chapter 3).

24,526

infected devices associated with the 23 banks' domains (543 employee-classified)

71,616

credential records: breach databases, stealer logs and combolists

23 of 23

banks enforcing DMARC (22 reject, 1 quarantine)

9.1 Where the exposure sits

Measure (23 banks)	Value
Banks with infected-device associations	23
Banks with employee-classified devices	19
Device associations, all / employee-classified	24,526 / 543

Measure (23 banks)	Value
Share of devices (not credentials) at the two largest banks	47% (71% at the largest five)
Credential records	71,616 (44,709 breach-database, 7,335 stealer-log, 19,572 combolist)
Banks with a current credential listing	12

Most associations are outside the employee classification; ownership remains unverified. 23,983 of 24,526 bank-associated devices are not employee-classified. Many may be customers' own computers, but ownership is not established. For a bank they are a fraud signal (session theft, account takeover and recovery abuse), and they cannot be ruled out as an intrusion route. The 543 employee-classified devices are the first priority for intrusion triage.

Concentration is moderate. Two banks carry nearly half of the device associations.

9.2 What posts say about UAE banks

- **Mule accounts.** Posts sought business and personal accounts at named UAE banks with the holder's SIM, card and Emirates ID (B14, B15), and remittance and wallet accounts tied to an Emirates ID (B13).
- **Card material.** 504 of the 631 cards seen in clear text in collected posts were attributed to one of 14 UAE issuers, mostly in card-checker output in February and March (§8.2, with its scope note).
- **Cash-out infrastructure.** A forum user claimed card-present terminals in Dubai for cash-out of foreign cards (B17), and channels recruited people to push stolen cards through UAE payment links.
- **Credential lines.** Automated uploads carried online-banking login lines for UAE retail banks, which usually come from infected customer devices.

9.3 What the regulator changed

The central bank's May direction, its planned Anti-Fraud Operations Centre and the refund duty for SMS-only fraud (§10.3) aim at the same chain [S36][S38]. That is the customer-side chain the posts describe. For a bank, the cost of a weak approval method now falls on the bank. Since 14 September the central bank's operational-risk regulation also covers central-bank-licensed financial institutions, not only banks. It requires notice within four hours of an event that has, or is likely to have, a significant impact on critical operations, and independent penetration tests of critical functions [S57].

9.4 What banks should do

1. **Contain privileged, remote-access or no-MFA accounts the same day; validate other current listings within five working days and employee devices within 30 days.** They are the most direct intrusion signals in this chapter (§12.1 rows 2-3).
2. **Treat the other device associations as fraud intelligence too.** Feed them into session-risk scoring and step-up authentication, and escalate any linked to staff or administrative access (§12.1 row 11).
3. **Harden account opening against residence-card KYC and mule recruitment.** Test with synthetic cases; watch for accounts that receive many small inbound transfers and pay out quickly (§12.1 row 18).
4. **Watch merchants as well as cardholders.** Payment links and terminals are cash-out channels (§8.1; §12.1 row 19).

KEY TAKEAWAYS

01

Most bank-associated devices are outside the employee classification, and their ownership is unverified; triage the 543 employee-classified devices and 12 current listings first.

02

All assessed bank domains publish an enforcing DMARC policy; keep testing email authentication and defences against phishing from hijacked mailboxes.

03

Mule accounts, residence-card KYC and payment-link cash-out are the fraud chain to break.

CHAPTER 10

Regulatory and national response

THIS CHAPTER ANSWERS

Which rules and official measures changed for UAE organisations in 2026, and what should a CISO do about them now?

4 h

for central-bank-licensed financial institutions to notify the central bank of a significant operational event, under a regulation in force since 14 September 2026

INSIDE THIS CHAPTER

10.1 Who sets the rules | 10.2 What the texts say | 10.3 The central bank's authentication shift | 10.4 What the police and the Council did | 10.5 What CISOs should do now

IN SHORT

The UAE's cyber rules are layered: federal law, emirate-level standards and the separate regimes of the two financial free zones. The clearest 2026 changes came from the central bank: a four-hour incident-notification rule for central-bank-licensed financial institutions, and a push beyond SMS one-time passwords with refund duties for SMS-only fraud. Map which regime applies to each entity, then rehearse breach notification against the shortest clock.

This chapter is not legal advice. We list only provisions we read in an official text or in a named secondary source; where we could not retrieve an official text, we say so.

10.1 Who sets the rules

Layer	Body	What it covers
Federal policy	UAE Cybersecurity Council	National strategy, policies and incident coordination [S54][S43]
Federal banking	Central Bank of the UAE (CBUAE)	Licensed banks, insurers and payment firms [S36] [S42]
Federal data and digital government	Federal Authority for Artificial Intelligence and Data (announced 14 June 2026)	AI oversight, digital government and data regulation, per a law-firm analysis [S41]
Emirate (Dubai)	Dubai Electronic Security Center (DESC)	Dubai government and semi-government entities [S44]

Layer	Body	What it covers
Financial free zone	DIFC Commissioner of Data Protection	Firms in the Dubai International Financial Centre [S39]
Financial free zone	ADGM Office of Data Protection	Firms in Abu Dhabi Global Market [S40]

10.2 What the texts say

Instrument	Provision we read	Source
DIFC Data Protection Law No. 5 of 2020, as amended (incl. Amendment Law No. 1 of 2025)	Article 41: notify the Commissioner of a personal-data breach "as soon as practicable in the circumstances"; Article 42: notify data subjects of high-risk breaches; Schedule 2: a fine of up to 50,000 USD for failing to report under either article	[S39]
ADGM Data Protection Regulations 2021	Article 32: notify the Office of Data Protection without undue delay and, where feasible, not later than 72 hours after becoming aware	[S40]
Federal Decree-Law No. 34 of 2021 on countering rumours and cybercrimes	Article 2: hacking a system, imprisonment and/or a fine of 100,000-300,000 AED, rising where data is acquired or damage results; Article 3: government systems, temporary imprisonment and a fine of 200,000-500,000 AED, at least 5 years where damage or a cyberattack is involved; Article 5: harm to government or critical-facility systems, temporary imprisonment and a fine of 500,000-3,000,000 AED, with a cyberattack an aggravating circumstance; Article 40: internet fraud, at least one year and/or 250,000-1,000,000 AED. In force since 2 January 2022	[S56]
CBUAE Operational Risk Management Regulation No. C 1/2026 (in force 14 September 2026)	Applies to central-bank-licensed financial institutions, not only banks (press report of the regulation). Notify the central bank within 4 hours of an event that has, or is likely to have, a significant impact on critical operations; a brief report within 24 hours; notification within 72 hours of any high-severity incident; independent external penetration tests for critical functions	[S57]
Federal Decree-Law No. 45 of 2021 (PDPL)	In force; implementing regulations still not issued and no private-sector supervisory authority clearly designated as of June 2026, per a law-firm analysis	[S41]
Federal Decree-Law No. 6 of 2025 (central bank law)	Article 149, as summarised by a practice guide: fraud prevention and detection, and prompt reporting of verified fraud and security breaches to the central bank	[S42]
Dubai Information Security Regulation	Issued under Resolution No. 13 of 2012 and maintained under Dubai Law No. 11 of 2014, with further DESC standards for IoT and other areas	[S44]
National Cybersecurity Strategy	Approved by the Cabinet on 3 February 2025; five pillars	[S43]

We read Federal Decree-Law No. 34 of 2021 in an English text hosted by ADGM; the official portal could not be retrieved, and later amendments were not checked. We could not retrieve the official PDPL text, so we do not quote its notification wording.

10.3 The central bank's authentication shift

Banks are moving card and login approval from SMS codes to their apps. Several major banks stopped sending SMS one-time passwords for online card purchases from 6 January 2026 and moved approval into the bank's app [S37]. On 21 May the central bank told licensed institutions to strengthen anti-fraud consumer protection and reduce reliance on single-factor verification such as SMS one-time passwords. It also said it had begun setting up a central Anti-Fraud Operations Centre for real-time fraud monitoring; no deadline was published [S36].

In July, Emarat Al Youm reported a central-bank disclosure on SMS-only fraud. Institutions must refund the full amount where fraud used a one-time password sent only by SMS, once the customer reports it promptly and the report is verified [S38]. For banks, that moves the cost of weak authentication onto the institution.

10.4 What the police and the Council did

Enforcement in 2026 targeted fraud at scale. Dubai Police reported 276 arrests and nine fraud centres dismantled in a joint operation with US and Chinese police announced on 29 April [S45]. The Ministry of Interior reported more than 960 arrests and 4,126 bank accounts blocked in a 30-country operation from 1 July to 30 September [S46]. The Council issued public advisories, including a wiper-malware warning on 4 April [S11].

10.5 What CISOs should do now

1. **Map each legal entity to its regime.** A group with a DIFC subsidiary, an ADGM fund and an onshore bank faces three breach-notification rules. Keep the map in the incident plan (§12.1 row 12).
2. **Rehearse against the shortest clock.** For central-bank-licensed financial institutions that is now four hours to the regulator [S57]. Elsewhere use ADGM's 72-hour outer limit where it applies, and "as soon as practicable" in the DIFC (§12.1 row 12).
3. **Finish the move off SMS codes.** For banks and payment firms, the central bank's direction and the refund duty make SMS-only approval a direct cost [S36][S38] (§12.1 row 10).
4. **Track the PDPL regulations.** Prepare data inventories and breach logs now; the implementing rules may arrive with the new federal authority [S41] (§12.1 row 13).

KEY TAKEAWAYS

01

Central-bank-licensed financial institutions now face a four-hour notification clock, and DIFC and ADGM entities have their own rules; map them before an incident.

02

The central bank's authentication direction and refund duty make SMS-only codes a liability.

03

Federal data-protection rules are still awaiting implementing regulations; prepare inventories now.

CHAPTER 11

Outlook

THIS CHAPTER ANSWERS

What should UAE organisations plan for in 2027, how confident are we, and what would change the plan?

3

conditional scenarios, each with the signal that would change it

INSIDE THIS CHAPTER

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

IN SHORT

Our judgements are about exposure and claims, not about intentions of states. Identity exposure and account fraud are likely to persist whatever happens regionally. Observed destructive and hacktivist claims clustered in the March-April 2026 heightened period, and our coverage is incomplete; plan for recurrence if similar conditions return. Plan for both: keep listing and device triage running all year, and keep wiper recovery and DDoS readiness tested for the next heightened period.

11.1 Key judgements

Judgement	Confidence	Basis	Limit
Credential and infected-device exposure will remain the most common measured exposure for leading UAE organisations	High	Chapter 3 counts; the year-round KYC and account trade (Chapter 8)	Association counts, not verified compromise
Hacktivist DDoS and destructive claims will cluster around periods of regional tension	Medium	2026 pattern: claims concentrated in March-April (Chapter 6); official statements on the heightened period [S22]	One year of data; claimants change names; September posts not available
Real-estate customer data will remain the most frequently advertised UAE-specific dataset; insurance and transport will see recurring single-organisation claims	Medium	Chapter 4 cases; at least nine real-estate sellers; buyer demand preceding supply	Sellers recycle; claims unverified
Ransomware listings of UAE firms will stay well above Gulf comparators	Medium	84 listings to 20 November against 7-30 for comparators [S5]	Listings are claims and include mislabels
Payment-authentication changes will shift fraud toward mule accounts, remote-access takeover and payment links	Medium	Central-bank direction and refund duty (§10.3); police warnings (§8.5)	Fraud-loss data is not public

11.2 What would change the assessment

- **A confirmed destructive incident at a named state body or critical operator** would move destructive risk from a claim-driven to an evidenced judgement and justify stronger recovery investment across sectors.
- **A sustained fall in current credential listings** across the 250 organisations at a repeat check would be an observation to interpret, not proof that controls work. Listings also move with market supply, seller behaviour and coverage. Response is better measured by validated-account dispositions, response times, session-revocation evidence and recurrence among remediated accounts.
- **Publication of the PDPL implementing regulations** would create a breach-notification baseline and more public incident data.
- **A vendor or official report tying a leak-site listing to a confirmed UAE incident** would let us calibrate how many listings reflect real intrusions.

11.3 Conditional scenarios

These are planning assumptions, not forecasts.

1. **Renewed regional tension.** If official statements again report a heightened period, expect DDoS claims against federal and emirate portals within days, relayed hack-and-leak claims against energy, ports and aviation, and wiper attempts. Signal: hacktivist channels publishing UAE target lists.
2. **Steady state.** If no heightened period occurs, expect the fraud economy to dominate: account trading, residence-card KYC, real-estate leads and ransomware listings at the 2026 pace. Signal: listing and KYC prices staying low.
3. **Authentication gap closes.** If banks finish moving approval into apps, expect a shift to remote-access scams and payment-link cash-out rather than SMS-code theft. Signal: police warnings focusing on remote-access apps.

KEY TAKEAWAYS

01

Identity exposure and account fraud are likely to persist regardless of regional events.

02

Observed destructive claims clustered during the heightened period; plan for recurrence if similar conditions return.

03

Watch for confirmed incidents behind listings; they would show how far listings reflect real intrusions.

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 a trigger, 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 credential-listing and infected-device alerts, then act on what is specific to you: current listings, employee devices and internet-facing systems. Then close the authentication, email and backup gaps, rehearse wiper, DDoS and identity-fraud scenarios, and report each row's completion evidence to the board.

12.1 30/60/90 days

This is a sequence, not a waiting period. A current material threat should enter your incident process immediately; the trigger column says when a row starts again.

Row	When	Trigger	Action	Owner	Completion evidence
1	Days 1-30	Start of the plan	Confirm that you receive credential-listing and infected-device alerts for your primary domains; if not, arrange them	CISO and threat intelligence	Alert source named; first alert received
2	Days 1-30	Each new credential-listing alert	Validate the account and its MFA status. Contain privileged, remote-access or no-MFA accounts the same day; record a disposition for the rest within 5 working days	Identity team	Each listing has a disposition: reset, already remediated, or not ours
3	Days 1-30	Each new employee-device alert	Validate employee-classified device associations; revoke sessions and tokens where active	Identity and endpoint teams	Device list reconciled with asset inventory; revocations logged

Row	When	Trigger	Action	Owner	Completion evidence
4	Days 1-30	Start of the plan; each new edge-system advisory	Inventory internet-facing VPN, mail, CRM, CMS and AI-orchestration endpoints; patch or isolate end-of-life systems; enforce single sign-on and MFA on CMS and administrator interfaces and remove local administrator accounts	Infrastructure	External re-test passes; exceptions signed off
5	Days 1-30	Start of the plan; each new camera advisory	Patch or remove internet exposure of IP cameras and recorders, including CVE-2017-7921 and CVE-2021-33044, using the affected and fixed firmware by model in §7.2	Facilities and infrastructure	Camera inventory; external re-test shows no exposed management interfaces
6	Days 1-30	Start of the plan; each wiper advisory	Restore a critical system from offline backup within the promised recovery time	Infrastructure and business continuity	Timed restore record
7	Days 31-60	Start of the plan	Alert on new remote-management tools, DLL side-loading from user-writable paths and unusual outbound connections from CRM and mail servers	SOC	Detection live; test alert fired
8	Days 31-60	Start of the plan	Enforce DMARC reject or quarantine on every sending domain	Email and DNS owners	DMARC policy per domain
9	Days 31-60	Start of the plan; renew when the Council or police announce a heightened period	Contract upstream DDoS mitigation for public portals	Infrastructure and network	Mitigation contract in place; failover tested
10	Days 31-60	Start of the plan	Move remaining customer and staff approvals off SMS one-time codes	Digital channels and fraud	Share of approvals by method, before and after
11	Days 31-60	Each new customer-device alert (banks and payment firms)	Feed non-employee device associations into session-risk scoring and step-up authentication	Fraud and digital channels	Signal live in risk scoring; first review

Row	When	Trigger	Action	Owner	Completion evidence
12	Days 31-60	Start of the plan; any new legal entity or rule	Map each legal entity to its notification regime (central bank four-hour rule, onshore, DIFC, ADGM) and rehearse against the shortest clock	Legal and privacy	Map in the incident plan; drill timings
13	Days 31-60	Start of the plan; update when the PDPL implementing regulations are issued	Prepare data inventories and breach logs; update the notification map	Privacy	Inventory and breach log in place; map updated
14	Days 31-60	Start of the plan; each new data-sale claim naming you	Review CRM and loyalty-platform exports and partner access	Data owners	Export log review signed off
15	Days 61-90, or at once when triggered	A data-sale or leak claim naming your customers, once a sample or field list is assessed as credible, or a confirmed incident	Warn customers about impersonation using leaked property, policy or loyalty data, as an awareness notice that does not confirm a breach	Customer communications	Notice published
16	Days 61-90	Start of the plan; each claim naming you	Rehearse a hacktivist DDoS and leak claim, including who confirms status publicly; verify each real claim against telemetry and the system owner	Communications and SOC	Exercise report with timings
17	Days 61-90	Start of the plan; each wiper advisory	Rehearse a wiper scenario across IT and OT	CISO and OT owners	Exercise report; gaps assigned
18	Days 61-90	Start of the plan; new KYC or SIM-swap pattern in warnings	Test account-opening and recovery against residence-card and SIM-swap fraud with synthetic cases; telecoms tighten SIM-swap and number-port checks	Fraud and identity	Test results; controls changed
19	Days 61-90	Start of the plan	Monitor merchants and payment links for cash-out patterns	Acquiring and fraud	Rules live; first review
20	Days 61-90	Day 90, then each quarter	Report validated-account dispositions, response times, session revocations and recurrence among remediated accounts; show listing and device counts as context only	CISO	Board paper with response measures and before-and-after context

12.2 By role

- **Boards and executives.** Ask for the listing disposition rate and the timed backup restore. Both are measurable within 30 days.
- **CISOs.** Treat a current credential listing as an incident trigger; fund wiper recovery and upstream DDoS mitigation before the next heightened period.
- **SOC and threat intelligence.** Hunt side-loaded DLLs, remote-management tools and unusual outbound traffic from mail and CRM servers; verify every hacktivist claim against telemetry before escalation.
- **Fraud teams.** Focus on account opening, recovery, mule accounts and payment links; SMS codes are no longer a defensible single factor.
- **Communications and legal.** Prepare holding statements for unverified claims; keep the notification map current.

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

KEY TAKEAWAYS

01

Start with alerts, listings and employee devices; they are specific and measurable.

02

Test backup restores and DDoS readiness before the next heightened period.

03

Measure progress by completion evidence, not by plans.

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 are Brandefense's own data and have no public address; every external source in Appendix C carries a link and the date it was verified.

A.2 Blackhole posts

Item	Value
Posts with the UAE country tag	130,477 counted
Coverage	Relevant-post ranges for January–July and November; August and October covered only in part; September posts not available
Forum posts	Forum posts mentioning the UAE; 1,271 distinct posts
Relevant (cleaned) posts, January–July and November	23,663–24,456 of 65,544, given as a range

Of 30 random relevant posts, 27 were crime-related and 10 named the UAE specifically, so cleaned counts are an upper bound for UAE-specific criminal activity.

Two limits shape every trend in this report. Family counts are not compared across June 2026. September posts were not available; September appears only in monthly counts and in the forum posts mentioning the UAE.

A.3 The 250 organisations

Selection, verification and limits are in §3.1. For each primary domain we read the exposure signals that Atlas uses for its ratings. They are infected devices, employee devices, credential records, dark-chat and dark-web mentions, new lookalike domains, documents that reference the domain, and current and past credential-market listings. Data were read on 21 November 2026.

A.4 Atlas ratings

Each organisation received an Atlas exposure rating from these signals. The national headline is reported as Atlas gives it; sector results are given as signal counts. Treat a current credential-market listing as a reason to validate accounts, not as proof of a breach.

205 organisations had candidate lookalike matches; those matches were not all validated.

A.5 DNS, TLS and web checks

We checked public DNS records for mail, email authentication and DNSSEC, and checked TLS and the homepage of each 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 checks on a scale of 0–100; a higher value means weaker hygiene. It is a model, not an Atlas rating. A sector value is the index's summary for that sector, not an average of its organisations.

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. The report publishes issuer-level counts only.

A.7 Ransomware

We used Ransompedia accepted listings for the UAE, Saudi Arabia, Qatar, Kuwait and Oman, all dates, dated by publication. Rejected and duplicate listings are excluded. A public tracker and relayed Blackhole posts are used only as cross-checks.

A.8 Incident coverage

Incident coverage draws on our post data for the 250 organisations, public reporting in English, Arabic and Russian, and official UAE pages for the window, with a final check to 20 November 2026.

Remaining coverage limits. Our view is partial:

- Public reporting was not equally deep for every organisation.
- For some official texts, including federal legislation and the central bank's rulebook, we relied on copies hosted elsewhere or on named secondary sources, as cited.
- Tor ransomware leak sites are covered only through Ransompedia.
- Closed forums, private groups and sales arranged in direct messages are outside our collection.
- 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 body or company is named only where the incident was officially confirmed and widely reported. Attributions to states are reported only as the source states them; the authors make none. Actor aliases are printed; links, contacts, indicators and personal data are withheld.

Appendix B. Evidence register

Every post quoted in this report appears as a redacted post card in the chapter shown. Excerpts are short; omissions are marked [...]; identifiers, contacts, links and victim organisations are replaced with labels in brackets, under the policy in A.9. Political and religious statements in actor posts are left out. Translations are ours unless the post carried the actor's own English. Posting dates are not intrusion dates.

Card	Posted	Venue	Alias as shown	Language	Shown in
B01	2026-01-30	Breach forum	Insurer-data seller (alias withheld)	English	§4.6
B02	2026-04-02	Breach forum	Seller of B01 (alias withheld)	English	§4.4
B03	2026-11-15	Breach forum	databreach000	English	§4.6
B04	2026-04-13	Breach forum	ksa901	English	§4.4
B05	2026-09-10	Leak aggregator forum	Aggregator account (actor handle withheld)	English	§6.3
B06	2026-05-06	Breach forum	attackercompany	English	§4.4
B07	2026-01-26	Breach forum	Retrogade	English	§4.5
B08	2026-04-26	Breach forum	Crimson	English	§4.5
B09	2026-03-23	Breach forum	rSosa	English	§4.5
B10	2026-02-24	Breach forum	TheAshborn	English	§4.5
B11	2026-03-05	Breach forum	CVDEAD	English	§4.5
B12	2026-08-11	Leak aggregator forum	X Forum Bot	English	§4.5
B13	2026-02-09	Telegram channel	Anonymous poster	English	§8.1
B14	2026-06-04	Telegram channel	Anonymous poster	English	§8.1
B15	2026-06-22	Carding/fraud forum	SOQA	Russian	§8.1
B16	2026-02-24	Telegram channel	Anonymous poster	English, Arabic	§8.3
B17	2026-11-17	Carding/fraud forum	z3fraan	English	§8.1
B18	2026-10-05	Carding/fraud forum	Moon_7thShift	English	§8.1
B19	2026-10-29	Carding/fraud forum	RummRif	English	§8.3
B20	2026-02-18	Breach forum	Anonymous buyer	English	§4.4
B21	2026-03-02	Actor channel	313 Team	Arabic, English	§6.2

Card	Posted	Venue	Alias as shown	Language	Shown in
B22	2026-03-12	Actor channel	Keymous+	English	§6.2
B23	2026-03-27	Breach forum	coderx	English	§6.3
B24	2026-06-01	Actor channel	Golden Falcon	English	§6.3

Appendix C. Sources

S1 Brandefense Blackhole post corpus, UAE country tag and forum posts mentioning the UAE, post dates 1 January-20 November 2026, extracted 21 November 2026.

S2 Brandefense Blackhole infected-device, breach-database, stealer-log and combolist associations for 250 domains, read 21 November 2026.

S3 Brandefense Atlas exposure ratings for the 250 domains, 21 November 2026, including credential-market listings, lookalike domains, exposed documents and mentions.

S4 Brandefense public DNS, TLS and homepage checks of the 250 domains, 21 November 2026.

S5 Brandefense Ransompedia, accepted listings for the UAE, Saudi Arabia, Qatar, Kuwait and Oman, all dates, extracted 21 November 2026.

S6 Brandefense Blackhole extraction of UAE-associated cards seen in clear text in collected posts, 21 November 2026.

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

S8 DataReportal, "Digital 2026: the United Arab Emirates". https://datareportal.com/reports/digital-2026-united-arab-emirates. Verified on 21 November 2026.

S9 Khaleej Times (WAM), "Over 70% of cyber threats targeting UAE are state-sponsored, authority says", 18 February 2026. https://www.khaleejtimes.com/uae/over-70-of-cyber-threats-targeting-uae-are-state-sponsored-authority-says. Verified on 21 November 2026.

S10 The National, "UAE foils AI-powered 'terrorist cyber attacks' on vital sectors", 22 February 2026. https://www.thenationalnews.com/news/uae/2026/02/22/uae-foils-ai-powered-terrorist-cyberattacks-on-vital-sectors. Verified on 21 November 2026.

S11 UAE Cybersecurity Council, advisory "Wiper Malware Campaign Targeting Multiple Sectors" (TLP:WHITE), 4 April 2026, hosted by ADGM. https://assets.adgm.com/download/assets/432318719+-+Wiper+Malware+Campaign+Targeting+Multiple+Sectors.pdf/af059afe318811f1b18b0634db0fb850. Verified on 21 November 2026.

S12 Gulf News, "UAE Cyber Security Council warns against wiper malware threat", updated 19 March 2026. https://gulfnews.com/uae/uae-cyber-security-council-warns-against-wiper-malware-threat-1.500480274. Verified on 21 November 2026.

S13 Khaleej Times, report on remarks by the head of the UAE Cybersecurity Council at the SAMENA summit, 1 April 2026. https://www.khaleejtimes.com/business/uae-cyberattacks-triple-to-600000-amid-iran-conflict-says-cybersecurity-chief. Verified on 21 November 2026.

S14 Emarat Al Youm, report on remarks by the head of the UAE Cybersecurity Council in Fujairah (Arabic), 20 April 2026. https://www.emaratalyoum.com/local-section/other/2026-04-20-1.2037698. Verified on 21 November 2026.

S15 Khaleej Times (WAM), "UAE authority foils sophisticated cyberattacks on entities in financial sector", 3 July 2026. https://www.khaleejtimes.com/uae/foils-cyberattacks-entities-financial-sector. Verified on 21 November 2026.

S16 Gulf News (WAM), "UAE foils advanced cyberattacks targeting vital sectors", 10 August 2026. https://gulfnews.com/amp/story/uae%2Fuae-foils-advanced-cyberattacks-targeting-vital-sectors-1.500636064. Verified on 21 November 2026.

S17 Khaleej Times, "$5 million ransom: UAE official recalls how country responded to major cyberattack", 15 September 2026 (updated 16 September). https://www.khaleejtimes.com/uae/records-640000-cyberattacks-a-day-chief-reveals. Verified on 21 November 2026.

S18 The National, report of a CNN interview with the head of the UAE Cybersecurity Council, 16 September 2026. https://www.thenationalnews.com/news/uae/2026/09/16/irans-irgc-behind-many-cyberattacks-on-uae-says-security-chief/. Verified on 21 November 2026.

S19 Euronews, interview with the head of the UAE Cybersecurity Council at the Arab Media Summit, 17 September 2026. https://www.euronews.com/2026/09/17/every-iranian-strike-came-with-a-cyberattack-uae-cyber-chief-says. Verified on 21 November 2026.

S20 Khaleej Times (WAM), "UAE foils around 750,000 cyberattacks targeting sectors including energy, education", 21 October 2026. https://www.khaleejtimes.com/uae/thwarts-750000-cyberattack-attempts. Verified on 21 November 2026.

S21 Emarat Al Youm, report on remarks by the head of the UAE Cybersecurity Council at Dubai Municipality's cyber security week (Arabic), 28 October 2026. https://www.emaratalyoum.com/local-section/other/2026-10-28-1.2096890. Verified on 21 November 2026.

S22 Khaleej Times, "Over 40 cyber groups tried to attack UAE infrastructure amid regional crisis, official says", 18 November 2026. https://www.khaleejtimes.com/uae/over-40-cyber-groups-tried-to-attack-uae-infrastructure-amid-regional-crisis-official-says. Verified on 21 November 2026.

S23 Emarat Al Youm, report on remarks by the head of the UAE Cybersecurity Council at the World Police Summit (Arabic), 19 November 2026. https://emaratalyoum.com/local-section/accidents/2026-11-19-1.2104340. Verified on 21 November 2026.

S24 The National, "UAE's Landmark Group probes data breach in Shukran loyalty programme", 11 November 2026. https://www.thenationalnews.com/business/money/2026/11/11/uaes-landmark-group-probes-data-breach-for-its-shukran-loyalty-programme/. Verified on 21 November 2026.

S25 Khaleej Times, "Shukran members' personal data accessed in data breach, but card details safe", 11 November 2026. https://www.khaleejtimes.com/business/shukran-members-personal-data-accessed-in-data-breach-but-card-details-safe. Verified on 21 November 2026.

S26 Security Affairs, "Iran-linked group Handala claims to have breached three major UAE organizations", 13 April 2026. https://securityaffairs.com/190716/hacking/iran-linked-group-handala-claims-to-have-breached-three-major-uae-organizations.html. Verified on 21 November 2026.

S27 UpGuard news page on a claim against a UAE port operator, May 2026. https://www.upguard.com/ (article URL withheld). Verified on 21 November 2026.

S28 Daily Dark Web, report of an alleged claim against a UAE airport operator, 31 March 2026. https://dailydarkweb.net/ (article URL withheld). Verified on 21 November 2026.

S29 The National, "Missile attacks and cyber hacks: Dual threats of modern warfare", 2 March 2026. https://www.thenationalnews.com/future/technology/2026/03/02/cyberwar-and-military-escalation-converge-as-middle-east-digital-infrastructure-is-attacked. Verified on 21 November 2026.

S30 StormWall, "DDoS Threat Landscape in MENA: Q1 2026 Report" (undated page). https://stormwall.network/resources/blog/q1-2026-ddos-report-mena. Verified on 21 November 2026.

S31 Palo Alto Networks Unit 42, "Boggy Serpens threat assessment", 16 March 2026. https://unit42.paloaltonetworks.com/boggy-serpens-threat-assessment/. Verified on 21 November 2026.

S32 Palo Alto Networks Unit 42, "Tracking Iranian APT Screening Serpens' 2026 Espionage Campaigns", 22 May 2026. https://unit42.paloaltonetworks.com/tracking-iran-apt-screening-serpens/. Verified on 21 November 2026.

S33 ESET, "ESET APT Activity Report Q4 2025-Q1 2026", 28 May 2026. https://www.welivesecurity.com/en/eset-research/eset-apt-activity-report-q4-2025-q1-2026/. Verified on 21 November 2026.

S34 Recorded Future Insikt Group, "Inside Tajin Group's Phishing and Money Laundering Network" (undated page; data to July 2026). https://www.recordedfuture.com/research/tajin-group-gurantee-marketplace. Verified on 21 November 2026.

S35 Khaleej Times, "91% of UAE DDoS attacks are low-volume as threats turn stealthier", 22 September 2026 (Help AG data). https://www.khaleejtimes.com/business/91-of-uae-ddos-attacks-are-low-volume-as-threats-turn-stealthier. Verified on 21 November 2026.

S36 Gulf News, "UAE banks ordered to tighten anti-fraud security beyond OTPs", 21 May 2026. https://gulfnews.com/business/banking/uae-banks-ordered-to-tighten-anti-fraud-security-beyond-otps-1.500548327. Verified on 21 November 2026.

S37 Gulf News, "UAE banks to end SMS OTPs for online card payments from January 6", updated 2 January 2026. https://gulfnews.com/business/banking/uae-banks-to-end-sms-otps-for-online-card-payments-from-january-6-1.500396452. Verified on 21 November 2026.

S38 Emarat Al Youm, report on a central-bank disclosure on refunds for SMS-only fraud (Arabic), 16 July 2026. https://www.emaratalyoum.com/business/local/2026-07-16-1.2065407. Verified on 21 November 2026.

S39 DIFC, Data Protection Law, DIFC Law No. 5 of 2020, as amended (incl. DIFC Laws Amendment Law No. 1 of 2025). https://www.difc.com/business/laws-and-regulations/legal-database/difc-laws/data-protection-law-difc-law-no-5-2020. Amendment law: https://assets.difc.com/v1/media/edge/images/dubaiintern0078-difcexperie96c5-production-3253/media/project/difcexperiences/difc/difcwebsite/documents/laws--regulations/amendment-law-no-1-of-2025.pdf. Verified on 21 November 2026.

S40 ADGM Office of Data Protection, "Personal Data Breach Notifications". https://www.adgm.com/operating-in-adgm/office-of-data-protection/data-breach-notifications. Verified on 21 November 2026.

S41 Morgan Lewis, "UAE establishes Federal Authority for Artificial Intelligence and Data", June 2026. https://www.morganlewis.com/pubs/2026/06/uae-establishes-federal-authority-for-artificial-intelligence-and-data. Verified on 21 November 2026.

S42 Chambers and Partners, "Cybersecurity 2026: UAE, trends and developments" (Ankura authors; undated). https://chambers.com/practice-guides/guides/cybersecurity-2026/uae/trends-and-developments. Verified on 21 November 2026.

S43 Government of Dubai Media Office, UAE Cabinet meeting approving the National Cybersecurity Strategy, 3 February 2025. https://mediaoffice.ae/en/news/2025/february/03-02/mohammed-bin-rashid-chairs-cabinet-meeting. Verified on 21 November 2026.

S44 Dubai Electronic Security Center, "Standards and policies". https://www.desc.gov.ae/regulations/standards-policies/. Verified on 21 November 2026.

S45 The National, "Almost 300 arrested in joint UAE, US, Chinese crackdown on financial crime", 29 April 2026. https://www.thenationalnews.com/news/uae/2026/04/29/almost-300-arrested-in-joint-uae-us-chinese-crackdown-on-financial-crime/. Verified on 21 November 2026.

S46 The National, "UAE leads 39 billion USD global digital fraud crackdown with more than 900 arrests", 22 October 2026. https://thenationalnews.com/news/uae/2026/10/22/uae-leads-39-billion-global-digital-fraud-crackdown-with-more-than-900-arrests. Verified on 21 November 2026.

S47 Gulf News, "Dubai Police warn of rise in fake calls posing as officials and banks", 11 April 2026. https://gulfnews.com/uae/crime/dubai-police-warn-of-rise-in-fake-calls-posing-as-officials-and-banks-1.500503458. Verified on 21 November 2026.

S48 Khaleej Times, Dubai Police warning on fake consumer-protection links, 7 July 2026. https://www.khaleejtimes.com/uae/dubai-police-fake-consumer-protection-links-banking-scam-warning. Verified on 21 November 2026.

S49 Emarat Al Youm, Dubai Police warning on callers posing as crisis-management staff (Arabic), 2 March 2026. https://www.emaratalyoum.com/local-section/accidents/2026-03-02-1.2020925. Verified on 21 November 2026.

S50 Khaleej Times, Abu Dhabi Police warning on fake social-media accounts, 25 April 2026. https://www.khaleejtimes.com/uae/fake-social-media-accounts-visa-concert-ticket-property-scam. Verified on 21 November 2026.

S51 Sharjah24, Sharjah Police arrests in a remote-access impersonation scam, 5 July 2026. https://sharjah24.ae/en/Articles/2026/07/05/mm07. Verified on 21 November 2026.

S52 Khaleej Times, "Dubai Police arrest gang over shopping website scam", 23 October 2026. https://www.khaleejtimes.com/crime/dubai-police-arrest-gang-shopping-website-scam-steal-bank-details. Verified on 21 November 2026.

S53 Khaleej Times, DFSA warning on fresh online scams and fake firms, 9 March 2026 (DFSA alert of 5 March). https://www.khaleejtimes.com/uae/dubai-regulator-warns-fresh-online-scams-fake-firms-dfsa-permit. Verified on 21 November 2026.

S54 Sharjah24, UAE Cabinet approves the UAE Cybersecurity Council, 29 November 2020. https://sharjah24.ae/en/Articles/2020/11/29/VP-approves-UAE-Environment-Policy-UAE-Cybersecurity-Council-and-UAE-National-Media-Team. Verified on 21 November 2026.

S55 Zawya (WAM), "World Economic Forum recognises UAE PASS as global digital government model" (undated page). https://www.zawya.com/en/business/world-economic-forum-recognises-uae-pass-as-global-digital-government-model-402881. Verified on 21 November 2026.

S56 Federal Decree-Law No. (34) of 2021 on Countering Rumors and Cybercrimes, English text hosted by ADGM (issued 20 September 2021; in force 2 January 2022). https://assets.adgm.com/download/assets/Federal%2BDecreeLaw%2BNo%2B34%2Bof%2B2021%2BOn%2BCountering%2BRumors%2Band%2BCybercrimes.pdf/7b3c845c864f11ef8ccdca0b2c1f6c13. Verified on 21 November 2026.

S57 Gulf News, "UAE overhauls bank risk rules: 4-hour reporting, cyber tests and tougher penalties", updated 15 September 2026. https://gulfnews.com/business/banking/uae-overhauls-bank-risk-rules-4-hour-reporting-cyber-tests-and-tougher-penalties-1.500675080. Verified on 21 November 2026.

S58 Check Point Research, "Interplay between Iranian targeting of IP cameras and physical warfare in the Middle East", 4 March 2026. https://research.checkpoint.com/2026/interplay-between-iranian-targeting-of-ip-cameras-and-physical-warfare-in-the-middle-east/. Verified on 21 November 2026.

S59 NIST NVD, CVE-2017-7921 (Hikvision cameras, improper authentication; CVSS 3.1 9.8; added to CISA KEV 5 March 2026). https://nvd.nist.gov/vuln/detail/CVE-2017-7921. Verified on 21 November 2026.

S60 NIST NVD, CVE-2021-33044 (Dahua devices, authentication bypass; CVSS 3.1 9.8; added to CISA KEV 21 August 2024). https://nvd.nist.gov/vuln/detail/CVE-2021-33044. Verified on 21 November 2026.

S61 Netcraft, "Middle East crisis: opportunistic fraud", 10 March 2026. https://netcraft.com/blog/middle-east-crisis-opportunistic-fraud. Verified on 21 November 2026.

S62 Khaleej Times, report on a cross-emirate fake traffic-fine SMS network, 11 April 2026. https://www.khaleejtimes.com/uae/crime/dh4-traffic-fine-cross-emirate-fraud-network-busted-over-fake-sms-scam. Verified on 21 November 2026.

S63 Gulf News, "UAE warns against phone scams, fake websites impersonating ICP logo", 30 April 2026. https://gulfnews.com/uae/government/uae-warns-against-phone-scams-fake-websites-impersonating-icp-logo-1.500524560. Verified on 21 November 2026.

S64 Palo Alto Networks Unit 42, threat brief on Iranian cyber activity in 2026, 17 April 2026. https://unit42.paloaltonetworks.com/iranian-cyberattacks-2026/. Verified on 21 November 2026.

S65 The National, report on a finance conference's attendee-document exposure, 18 February 2026. https://www.thenationalnews.com/ (article URL withheld). Verified on 21 November 2026.

S66 DeXpose, report of a claim against a UAE customs authority, 22 August 2026. https://www.dexpose.io/ (article URL withheld). Verified on 21 November 2026.

S67 Gulf News, "A hacker accessed sensitive UAE-linked systems then demanded $5m", 15 September 2026. https://gulfnews.com/living-in-uae/safety-security/a-hacker-accessed-sensitive-uae-linked-systems-then-demanded-5m-1.500675569. Verified on 21 November 2026.

S68 CISA (ICS-CERT), advisory ICSA-17-124-01, Hikvision IP cameras (CVE-2017-7921), 4 May 2017. https://www.cisa.gov/news-events/ics-advisories/icsa-17-124-01. Verified on 21 November 2026.

S69 Dahua, security advisory DHCC-SA-202106-001, identity authentication bypass in some Dahua products (CVE-2021-33044), 1 September 2021, updated 15 November 2021. https://www.dahuasecurity.com/about-dahua/trust-center/dahua-psirt/dhcc-sa-202106-001:security-advisory---identity-authentication-bypass-vulnerability-found-in-some-dahua-products. 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 with information-stealing malware that Brandefense associates with the organisation's domain; "employee" is Brandefense's classification, not verified employment.
- **Credential-market listing:** a credential tied to the domain offered on a monitored market at the time of the check.
- **Combolist:** a list of login and password pairs assembled from various sources; age and validity vary.
- **Stealer log:** data captured by information-stealing malware from a device.
- **Checker bot:** a bot that tests stolen cards against payment gateways and prints the result.
- **Wiper:** malware that destroys data rather than encrypting it for ransom.
- **Mule account:** a bank or wallet account lent or sold to move proceeds of fraud.
- **KYC (know your customer):** identity checks at account opening; "KYC services" sell accounts that have already passed them.
- **Availability-check link:** a link to a public service that tests whether a site answers from a few locations; it captures a moment, not an outage.
- **Hack-and-leak:** an operation that publishes stolen material to cause damage or pressure, sometimes with destructive claims.
- **Post card:** a redacted reproduction of one dark-web post, with venue, date, alias, language and what it does and does not establish.

- **Relay:** a third-party channel or bot that reposts another actor's claim; a relay is weaker evidence than the actor's own post.
- **DMARC / SPF / DKIM:** email-authentication standards; DMARC tells receivers what to do with mail that fails.
- **DNSSEC:** signatures that let resolvers verify DNS answers.
- **TLP:CLEAR:** may be shared without restriction; other legal duties still apply.
- **Lookalike domain:** a newly observed domain that resembles an organisation's own; a candidate for phishing, not a confirmed phishing site.
- **Card dumps:** copied magnetic-stripe data used to clone cards for card-present cash-out.
- **Accepted listing:** a Ransompedia leak-site listing kept after rejected and duplicate entries are removed.
- **OT (operational technology):** systems that run physical processes, such as power, water and industrial control.
- **HSTS:** a web header that tells browsers to use HTTPS only.
- **End-of-life:** software no longer receiving security updates from its vendor.

About this report

Prepared by Odin by Brandefense. Version 1.0 was completed on 21 November 2026. Research cutoff: 20 November 2026 for posts, ransomware listings and public reporting; exposure data were read on 21 November 2026. 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 the UAE. The authors take no position on the policies of any government; attributions are reported as their sources state them. Recommendations describe what organisations could do; they do not state that any organisation has or has not done them. An Arabic edition is available; where the editions differ, the English edition prevails.

© 2026 Brandefense. All rights reserved.