Event Report

CloudSEK

Middle East Cyber Threat Landscape 2025-2026

Comprehensive Regional Threat Intelligence Assessment · April 2025 – August 2026

CATEGORY
Threat Intelligence

REGION
Middle East

REPORTING PERIOD
April 2025 – August 2026

Contents

Executive Summary

17
month reporting window, April 2025 – August 2026

2,245
feeds in March 2026, the single highest month

7,112
feeds referencing Israel, the most targeted country

357
ransomware feeds in June 2026, the period peak

CloudSEK recorded extensive threat intelligence coverage of activity related to the Middle East region across all monitored modules, ransomware, hacktivism, dark web, adversary intelligence, malware, and vulnerability intelligence, during the period April 2025 through August 31, 2026. This represents a persistently elevated and in several months sharply escalating threat environment, with notable peaks in June 2025, October 2025, and March 2026.

The Middle East cyber threat landscape in the reporting period was shaped by three converging forces: sustained hacktivist campaigns driven by the ongoing regional geopolitical conflict (particularly targeting Israel), accelerating ransomware operations against industrial and government organisations, and intensified Iranian and Israeli state-linked APT campaigns targeting critical infrastructure, defence, and telecommunication sectors across the region.

Israel was the most targeted country by a wide margin, followed by Turkey, Iran, the United Arab Emirates, Saudi Arabia, and Egypt. Government and Financial Services were the most impacted sectors. Hacktivism was the numerically dominant attack category, mainly anti-Israel operations - but ransomware activity showed a striking upward trajectory, peaking in June 2026. Ideological motivation and direct financial motivation together accounted for the majority of threat actor activity in the region.

Key threat actors across the reporting period include: hacktivist group **Handala** conducting wiper, phishing, and disruptive operations against Israel; ransomware operator **Nova** the single most prolific ransomware actor targeting the region; **MuddyWater** (IRGC-linked), deploying the RustyWater/Phoenix backdoors against UAE and Israel; **Charming Kitten/APT35/Mint Sandstorm** conducting espionage against defence, research, and government targets; and **Predatory Sparrow** (Gonjeshke Darande), conducting destructive attacks against Iranian financial infrastructure.

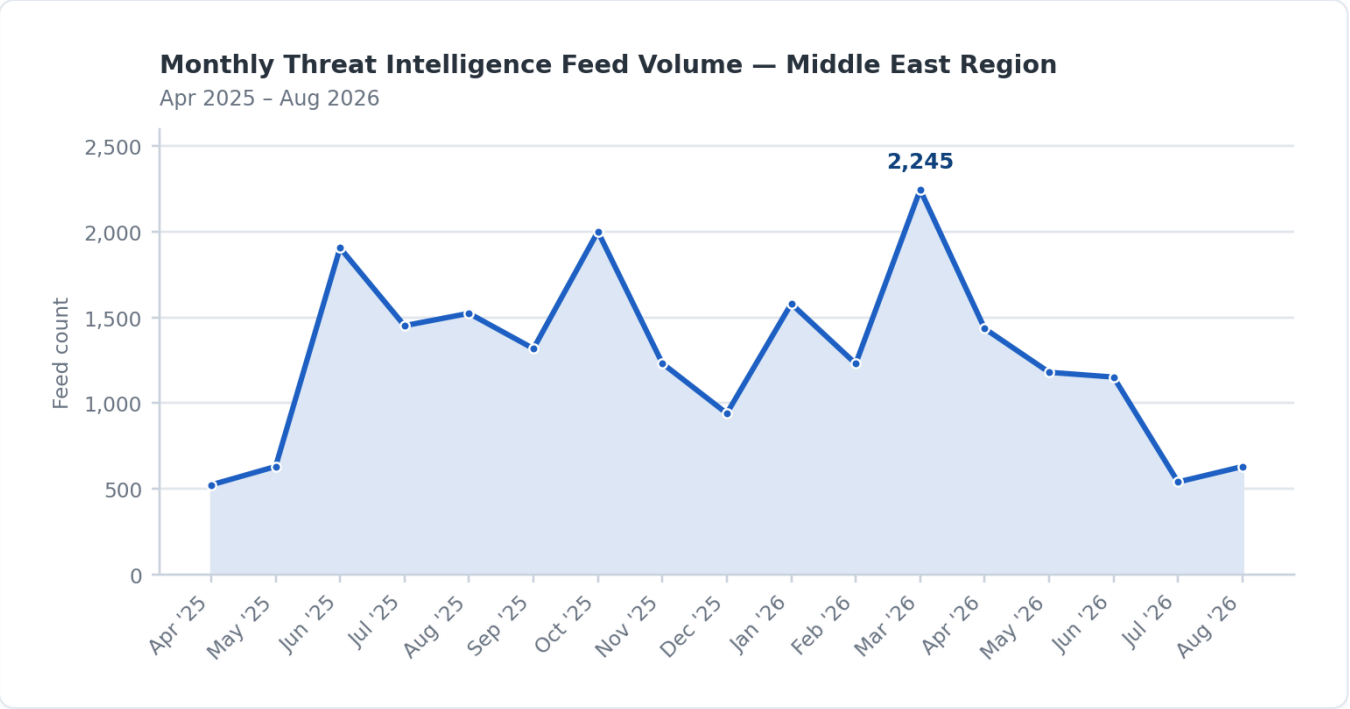
Vulnerability exploitation was a critical initial-access vector throughout the period. The most impactful CVEs include **CVE-2025-55182** (React Server Components pre-auth RCE, CVSS 10.0, KEV-listed, EPSS 0.998), **CVE-2024-55591** and **CVE-2025-24472** (Fortinet FortiOS/FortiProxy authentication bypass, both KEV-listed, exploited by The Gentlemen and Gunra ransomware), **CVE-2025-0282** and **CVE-2025-22457** (Ivanti Connect Secure RCE, both CVSS 9.0, KEV-listed, exploited by China-nexus UNC5221), and **CVE-2025-29824** (Windows CLFS privilege escalation, CVSS 7.8, exploited as a zero-day by Play ransomware). Stealth Falcon APT exploited a zero-day (CVE-2025-33053, Microsoft WEBDAV RCE) specifically targeting high-profile defence entities in the Middle East.

Threat Landscape Overview

Reporting Period Coverage

This report encompasses incidents that occurred within the 17-month reporting period. The attacks and incidents were not uniformly distributed:

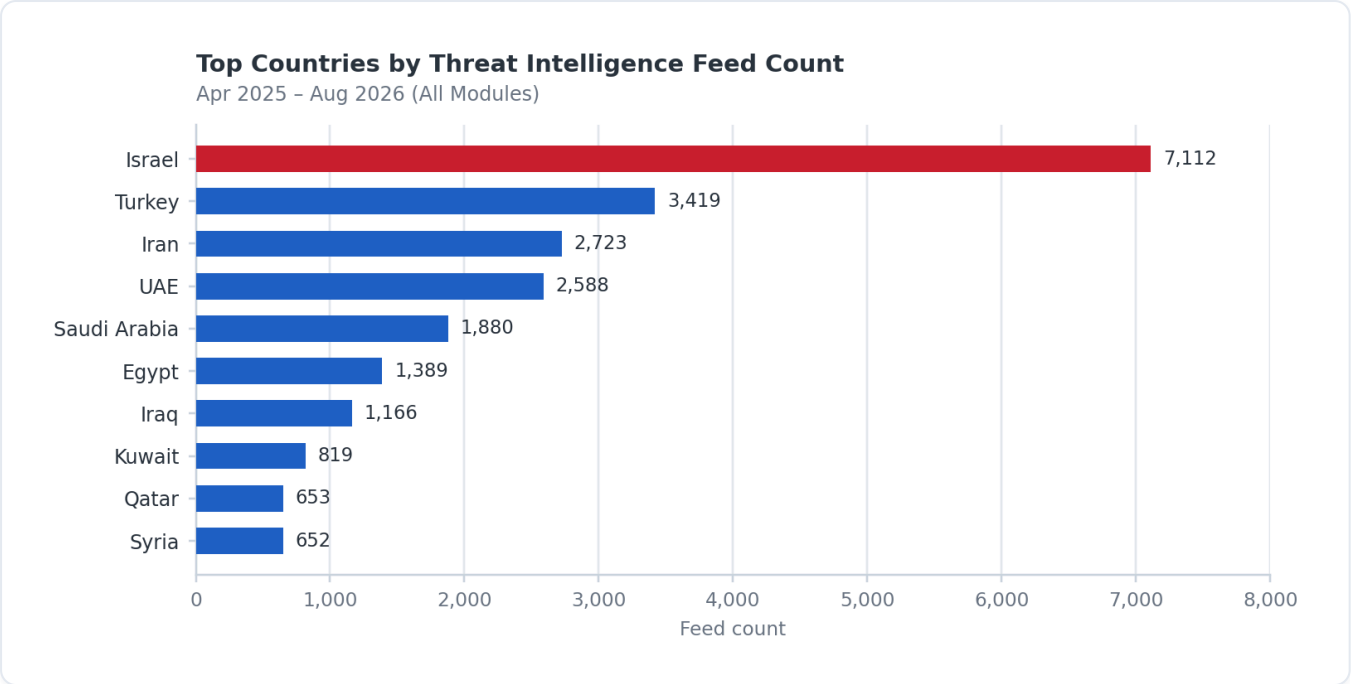
The first half of 2025 showed a sharp escalation starting in June 2025 (1,906 feeds, 3.6× the April baseline of 523), driven by hacktivism surges. A second major peak occurred in October 2025 (2,001) and a third, the highest in the period, in March 2026 (2,245). Feed volumes moderated in the second quarter of 2026, with July and August 2026 showing lower aggregate counts, partially attributable to reporting lag near the data cut-off rather than an actual reduction in threat activity.



Monthly activity volume, Middle East region, April 2025 – August 2026 (all threat categories combined)

Geographic Distribution

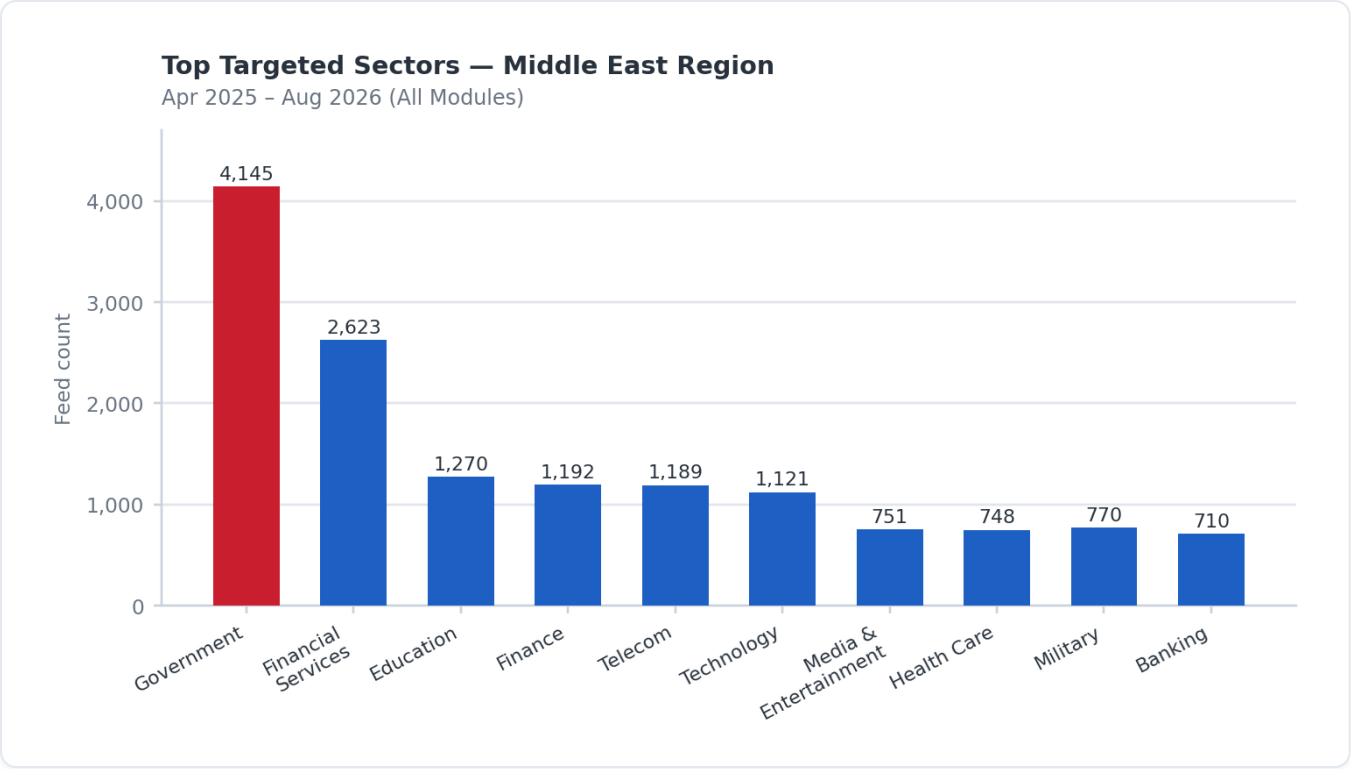
Israel dominated as the most-targeted country, reflecting both its position as the primary target of anti-Israel hacktivist campaigns and sustained APT operations. Turkey ranked second (3,419), driven by ransomware activity against its industrial and manufacturing sectors. Iran featured prominently as both a source and target of cyber operations, Iranian state-linked APTs operated offensively while Iran itself was targeted by **Predatory Sparrow**/Gonjeshke Darande and anti-regime hacktivist groups. UAE (2,588) and Saudi Arabia faced significant dark web, ransomware, and espionage activity. Among smaller Gulf states, Kuwait (819) and Qatar (653) saw notable attention.



Top countries by threat activity, Middle East region, April 2025 – August 2026 (all threat categories)

Sector Targeting

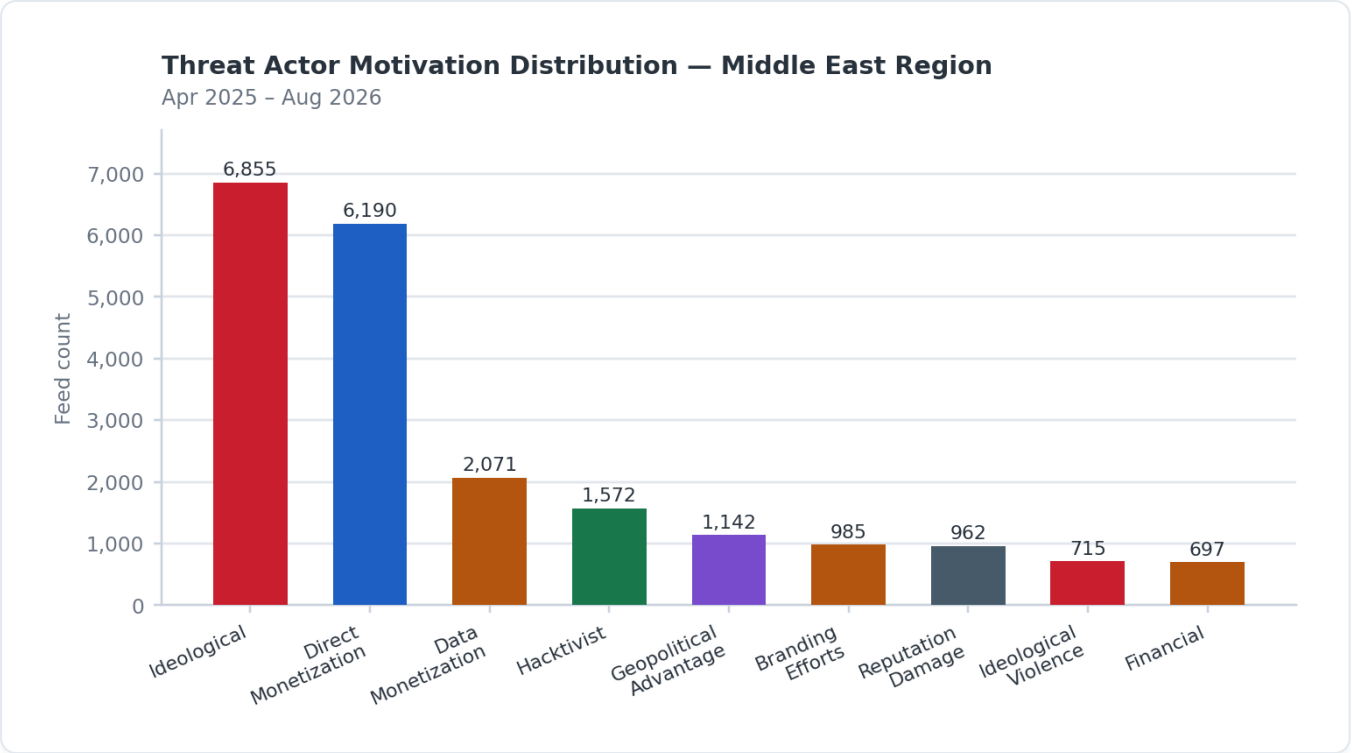
Government and Financial Services were by far the most targeted sectors across the entire reporting period, consistent with their status as high-value targets for both hacktivists seeking to demonstrate disruptive impact and ransomware actors seeking large ransom payments. Education (1,270), Finance (1,192), and Telecommunications (1,189) followed. Energy and critical infrastructure, while lower in count, attracted disproportionate attention from state-sponsored actors. Ransomware specifically targeted Facility Management, Industrial, and Infrastructure sectors at higher rates relative to their economy-wide share.



Top targeted sectors, Middle East region, April 2025 – August 2026 (all threat categories)

Attack Motivation Profile

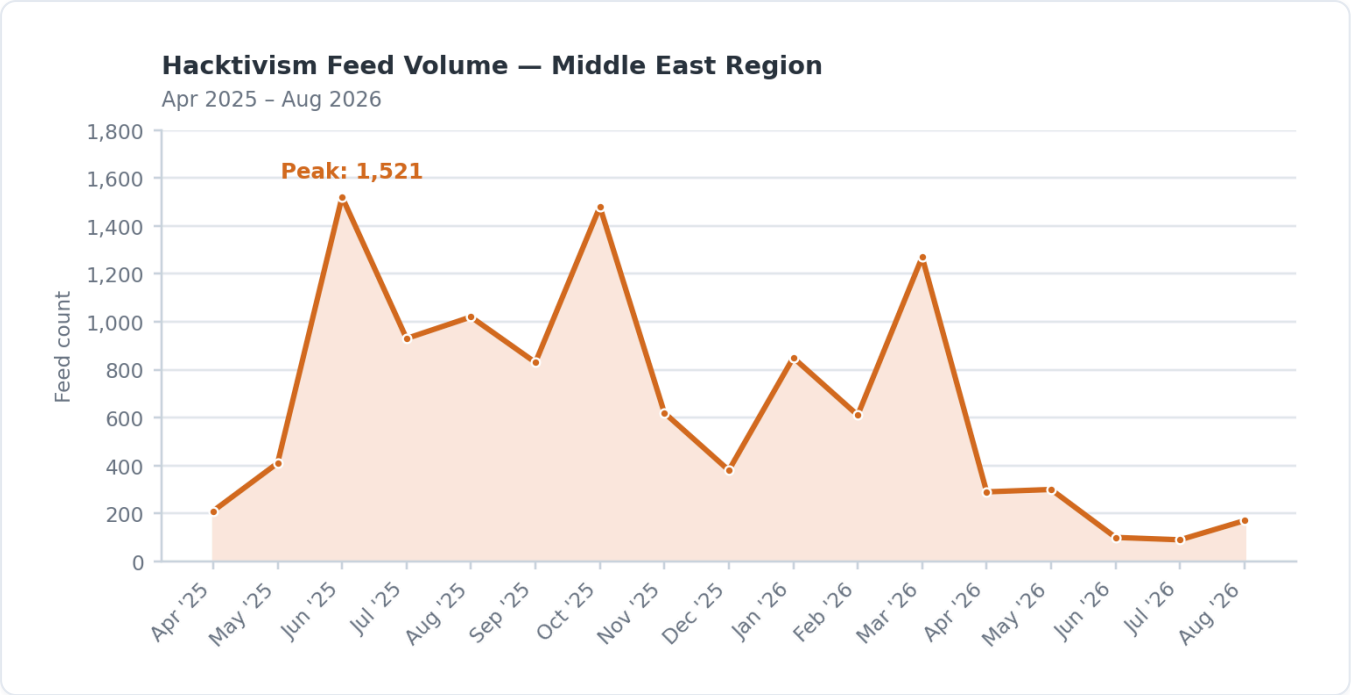
Ideological motivation narrowly exceeded direct financial motivation over the full period, confirming that the Middle East threat environment is jointly shaped by politically-driven actors and cybercriminal operators. Hacktivist motivation and geopolitical advantage reinforce that state-directed and state-adjacent activity constitutes a substantial share. Intelligence gathering and disruptive intent represent smaller but strategically significant clusters, mainly attributable to APT campaigns.



Threat actor motivation distribution, Middle East region, April 2025 – August 2026

Hacktivism Activity

Threat intelligence data captured extensive hacktivism activity related to the Middle East during the reporting period, making it the single largest threat category by volume. Activity peaked in June 2025 (with the highest recorded hacktivism activity), declined through the second half of 2025, resurged in October 2025 and March 2026, then markedly declined from mid-2026 onwards. The sharp deceleration from June 2026 onwards is notable and may reflect both operational fatigue among hacktivist groups and a shift to longer-dwell targeted operations.

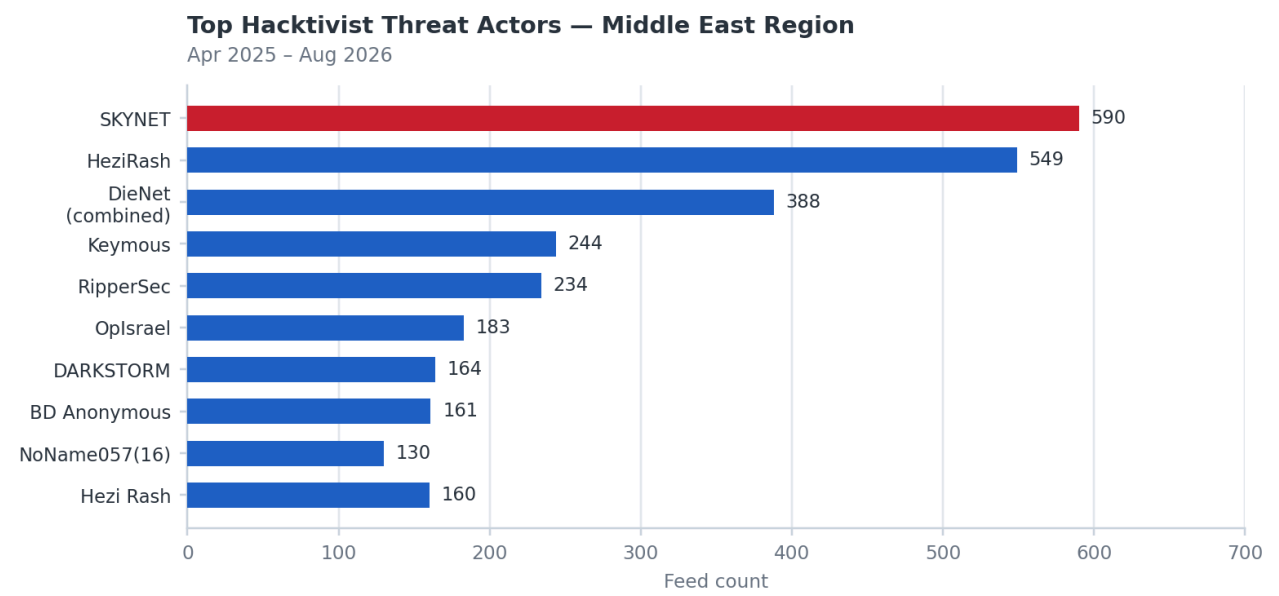


Hacktivism activity volume, Middle East region, April 2025 – August 2026

Top Hacktivist Countries Targeted

Israel was the overwhelming primary target of hacktivism in the region, accounting for **37.8%** of hacktivism activity. Iran ranked second, primarily as a target of anti-regime and pro-Israel hacktivist groups. Turkey (1,107), UAE (700), Iraq (506), Saudi Arabia (496), and Egypt (439) followed. Jordan (199), Kuwait (189), Syria (327), and Azerbaijan (236) also featured. Cyprus (220) appeared frequently, likely due to its geographic and network proximity to Middle East operations.

Top Hacktivist Threat Actors



Top hacktivist threat actors, Middle East region, April 2025 – August 2026 (by activity level)

Actor	Activity Level	Primary Targets	Motivation	TTPs
SKYNET	High	Israel, Turkey, UAE	Ideological / Geopolitical	DDoS, defacement, data leaks
HeziRash	High	Israel, Turkey	Ideological / Hacktivism	DDoS, web defacement
DieNet / DieNet_Network	Moderate	Israel, US, Iraq	Ideological, anti-Israel	DDoS, SQL injection, defacement
Keymous	Moderate	Israel, UAE, Saudi Arabia	Hacktivism / Ideological	DDoS, defacement
RipperSec	Moderate	Government, Retail, Education	Hacktivism / Ideological	DDoS, web attacks
OpIsrael	Moderate	Israel (coordinated campaign)	Ideological / Anti-Israel	DDoS, defacement, leaks
DARKSTORM	Moderate	Israel, Turkey, UAE	Ideological / Geopolitical	DDoS, data leaks
BD Anonymous	Moderate	Israel, India, Turkey	Hacktivism	DDoS, defacement
NoName057(16)	Moderate	Israel, US, European pro-Israel targets	Ideological / Geopolitical	DDoS via DDoSia tool
Handala	Moderate	Israel (Gov, Health, Tech)	Ideological / Hacktivism / Geopolitical	Wiper, phishing, data leak, defacement

Handala: Featured Actor Profile

Key incidents in **Handala**'s escalating campaign:

- January 2025, **Handala** claimed to have accessed the public address systems of around 20 Israeli kindergartens, broadcasting fake rocket warning sounds and threatening audio
- February 2025, the group claimed to have obtained **2.1 terabytes** of data from Israeli National Police systems including officer psychological records and classified case files
- December 2025, **Handala** published names and personal details of Israeli air defense engineers, offering $30,000 rewards for additional information
- February 2026, the group claimed access to Clalit Health Services (approximately 4.8 million patients), leaking over 10,000 patient records.

Handala (also known as **Handala** Hacking Group, **Handala** Hack) is an ideologically motivated hacktivist group, active from December 2023 through August 25, 2026. The group primarily targets Israeli government, health care, technology, and education entities, with secondary targeting of UAE and US organizations.

Handala employs a diverse and advanced TTP set: phishing (T1566), web defacement (T1491), data encryption for impact (T1486), PowerShell abuse (T1086), proxy infrastructure (T1090), resource hijacking (T1496), and data manipulation (T1565).

Notably, CloudSEK intelligence records that **Handala** launched a cyberattack on UAE critical infrastructure on April 15, 2026, demonstrating geographic expansion beyond Israel. Its motivations are recorded as ideological, hacktivist, geopolitical advantage, and extremist promotion.

Notable Hacktivist Incidents & Campaigns

Cyber Fattah: Saudi Games 2024 Platform Breach (June 2025)

In June 2025, an Iran-linked group called **Cyber Fattah**, operating as part of a broader coalition known as the 'Holy League', reportedly breached the registration platform for the Saudi Games 2024 through a poorly secured database tool. The stolen data allegedly included passport and ID scans, bank account numbers, medical certificates, and login credentials of athletes, visitors, and officials. The data was later posted on dark web forums. Security researchers linked the attack to broader Iranian-aligned efforts targeting Saudi Arabia's international image.

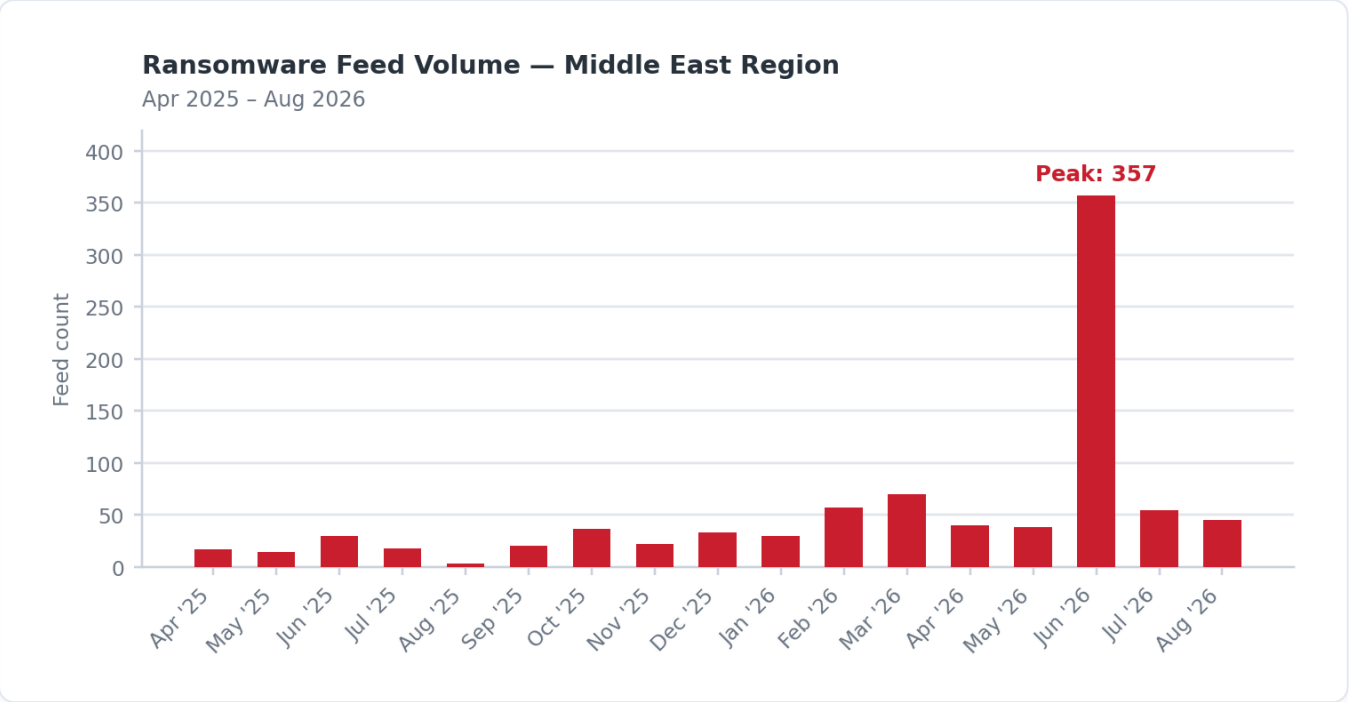
Date	Actor(s)	Target / Country	Sector	Type
Aug 31, 2026	Khilafah Hackers	Multiple Israeli websites	Various	Web defacement
Aug 31, 2026	Moroccan Soldiers / Elite Squad	Israeli Digital Library Platform	Education/Media	Data breach claim
Aug 31, 2026	Multiple hacktivist groups	eFAWATEERcom Bank / Jordan	Financial Services	DDoS / service disruption
Aug 30, 2026	Khilafah Hackers	Five Israeli websites	Various	Web defacement
Aug 24, 2026	Nation of Saviors	Oron Group / Israel	Business Services	Alleged breach
Aug 23, 2026	Cyber Islamic Resistance	Oron Group / Israel	Business Services	Penetration claim
Mar 2026	Multiple coalitions	Middle East (broad escalation)	Government, Finance, Telecom	DDoS, defacement, leaks
Feb 27 – Mar 5, 2026	Multiple	Middle East (regional escalation)	Various	Multi-vector hacktivist surge

Date	Actor(s)	Target / Country	Sector	Type
Oct 2025	SKYNET, HeziRash, DieNet, OpIsrael	Israel, Turkey, UAE (peak month)	Government, Finance, Telecom	DDoS, defacement, data leaks
Jun 2025	Multiple anti-Israel groups	Israel, Iran (peak month)	Government, Finance, Military	DDoS, defacement, wiper, leaks

It is important to note

Ransomware Activity

Threat intelligence feeds from CloudSEK show sustained ransomware activity targeting the Middle East region during the reporting period. Ransomware activity followed a distinct upward trend across the 17 months: after a slow start (17 feeds in April 2025, 14 in May), monthly volumes grew steadily, reaching a sustained elevated plateau from October 2025 (37) through mid-2026. The most dramatic spike occurred in June 2026 (357), representing a nearly 10× surge relative to the prior month and more than 20× the April 2025 baseline, the most significant single-month escalation recorded in the reporting window.



Ransomware activity volume, Middle East region, April 2025 – August 2026

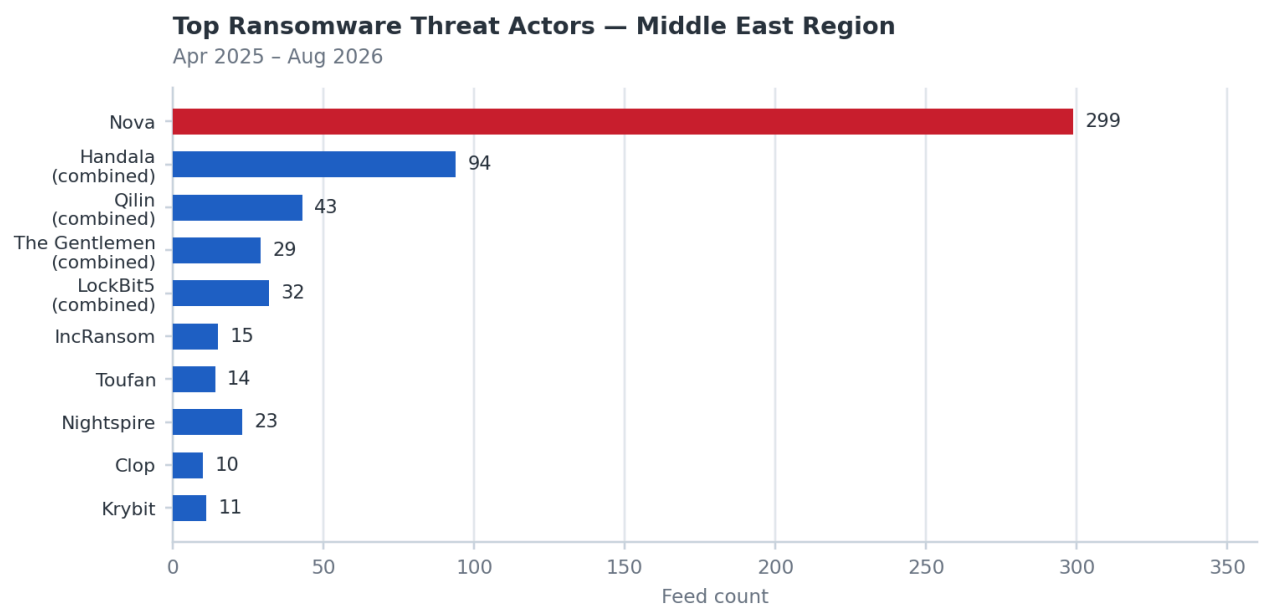
Ransomware by Country

Turkey was the most ransomware-targeted country in the region, followed by Israel, the UAE, Egypt, and Saudi Arabia. Gulf states Kuwait, Qatar, Jordan (14), and Oman (12) saw increasing attention. Bahrain (6) and Lebanon (6) appeared in lower volumes. Iran (14) featured in ransomware feeds mainly as a source of ransomware actors with externally directed operations rather than as a victim of ransomware campaigns.

Ransomware by Sector

Facility Management was the most targeted sector in ransomware operations, followed by Industrial, Property Management, Infrastructure, and Manufacturing. These figures reflect a deliberate targeting pattern by ransomware groups, particularly **Nova**, **The Gentlemen**, and **DragonForce**, against asset-heavy sectors with operational technology and high operational disruption potential. Government (34) and Financial Services (33) ranked lower in ransomware-specific targeting relative to their overall threat intelligence footprint, consistent with higher security maturity in those sectors.

Top Ransomware Threat Actors



Top ransomware threat actors, Middle East region, April 2025 – August 2026 (activity level, duplicates consolidated)

Actor	ME Activity Level	First Seen	Last Active	Motivation	Known TTPs
Nova	Moderate	Apr 2025	Aug 2026	Data & Financial Profit-making	Ransomware, Botnet, payment card theft, phishing
Handala (ransomware ops)	Low	Feb 2024	Aug 2026	Ideological / Hacktivist	Data encryption, phishing, wiper
Qilin	Low	Late 2022	Aug 2026	Financial / Extortion	Phishing, CAPTCHA-based cred theft, CVE exploitation
The Gentlemen	Low	2025	Aug 2026	Financial / Cybercrime	CVE-2024-55591 exploitation, VPN brute-force, Rclone
LockBit5 / LockBit	Low	Mar 2021	Aug 2026	Financial / Profit-making	Phishing, valid accounts, external remote services
Nightspire	Low	2025	Aug 2026	Financial / Cybercrime	Encryption, data data theft
IncRansom	Low	2023	Aug 2026	Financial / Extortion	Double extortion, data theft
Toufan	Low	2025	Aug 2026	Ideological / Financial	Ransomware, data leak
DragonForce	Low	Oct 2022	Aug 2026	Financial / Cybercrime	RaaS cartel, SimpleHelp vuln, social engineering, MSP supply chain

Notable Ransomware Incidents

Date	Title	Threat Actors	Countries
2026-08-31	**The Gentlemen** Ransomware Targets Saudi Consulting Services SAUD CONSULT	**The Gentlemen**	Saudi Arabia

Date	Title	Threat Actors	Countries
2026-08-22	**NasirSecurity** Claims 'Most Massive Hack Operation in UAE History', Targeting Dubai Airport, UAE Customs, Kuwait Ministry of Interior, Yad Vashem, Rumaila Operating Organisation, Oman CC Energy	**NasirSecurity**	United Arab Emirates, Kuwait, Israel, Iraq, Oman
2026-08-21	TheGentlemen Ransomware Targets AWJ Holding Company and Almeer General Contracting Establishment (Saudi Arabia)	**The Gentlemen**	Saudi Arabia
2026-08-19	**Deadlock** Ransomware Targets Global Terminal Services	**Deadlock**	Middle East
2026-08-13	**LockBit5** Ransomware Targets Towell Holding (Oman), Data Listed on Leak Site	**LockBit5**	Oman
2026-08-13	**LockBit5** Ransomware Targets soeuae.ae (UAE)	**LockBit5**	United Arab Emirates
2026-08-30	**Qilin** Ransomware Targets Black Cat Engineering & Construction WLL (Kuwait/Bahrain)	**Qilin**	Kuwait
2026-08-26	**Krybit** Ransomware Targets Mima Foods, Egyptian Global Food Exporter	**Krybit**	Egypt
2026-08-13	**Payload** Ransomware Targets Zara Investment Holding	**Payload**	Middle East
2026-08-13	LockBit Ransomware Targets Turkish Mining Company Gümüştaş Madencilik	LockBit	Turkey
Feb 2025	**DragonForce** Ransomware Targets Al Bawani (Saudi Arabia): ~**6.96 TB** stolen including building plans for military-related sites; data published after ransom deadline passed.	**DragonForce**	Saudi Arabia
Jul 2025	**Everest** Ransomware Targets Rezayat Group (Saudi Arabia): ~**10 GB** taken including engineering drawings and financial records. Rezayat operates 25 companies across 13 countries.	**Everest**	Saudi Arabia

The Gentlemen: Emerging Ransomware Group

The Gentlemen (led by 'Hastalamuerte', a former **Qilin** affiliate) emerged as a significant new ransomware operator in the reporting period, with confirmed targeting of Saudi Arabian organisations.

The group's TTPs: initial access via exploitation of **CVE-2024-55591** (Fortinet FortiOS/FortiProxy auth bypass, CVSS 9.8) and brute-forcing of VPN credentials; lateral movement using NetExec and PowerShell; data data theft via Rclone; and multi-platform ransomware execution (Windows, Linux, ESXi). The group had at that point impacted approximately 94 organisations globally, demonstrating high technical sophistication.

APT & Cyber Espionage Operations

BladedFeline (OilRig Subgroup): Iraq and Kurdistan Espionage (June 2025)

Security researchers at ESET disclosed in June 2025 that **BladedFeline**, connected to the Iran-linked **OilRig** cluster, had been conducting long-running espionage against **KRG** (Kurdistan Regional Government) officials, Iraqi central government entities, and a telecom company in Uzbekistan. The group used two custom backdoor programs called Whisper and PrimeCache. Whisper hides its communications inside the victim's own Microsoft Exchange mail server, making it very difficult to detect. The campaign has been active since 2017.

Politically motivated threat actors, state-sponsored APTs and their proxies, accounted for around 153 activity indicators under explicit geopolitical and intelligence-gathering motivation tags when filtered for Middle East targeting. The dominant APT nexuses in the region were Iranian state-linked groups (**MuddyWater**, Charming Kitten/**APT35**/Mint Sandstorm, **APT42**, **Nimbus Manticore**/**UNC1549**, **OilRig**), Israeli-linked operators (**Predatory Sparrow**, **Stealth Falcon**), and Chinese-nexus groups (UNC5221/UNC5337) exploiting network edge devices with global reach including Middle East targets.

Iranian-Nexus APT Activity

Actor	Activity Level	Primary Targets (ME)	Motivation	Key TTPs	Key Malware / Tools
MuddyWater (Mango Sandstorm / TA450)	Low	Israel, UAE, US diplomatic targets	Geopolitical, Espionage, Disruptive	Spearphishing, RMM abuse, VPN-based phishing, PowerShell, code obfuscation (Gemini AI)	Phoenix backdoor, RustyWater implant, fake AirArabia lure documents
Charming Kitten (APT35 / Mint Sandstorm / TA453)	Low	Defence, Research, Media (Israel, US, Iran)	Intelligence Gathering, Espionage, Geopolitical	Spearphishing (email, WhatsApp), LNK abuse, PowerShell backdoors, data theft over C2	AnvilEcho PowerShell implant, NokNok-like tooling
APT42	Low	Middle East, US (research, media)	Intelligence Gathering, Espionage	Spearphishing, credential harvesting	Not specified in CloudSEK data
Nimbus Manticore (UNC1549)	Low	Aviation, Defence, Telecom, Software Dev (Saudi Arabia, ME, US)	Geopolitical, Espionage	Phishing, trojanised software installers (Zoom, SQL Developer), SEO poisoning, AI-assisted malware development	MiniFast backdoor, MiniJunk framework
OilRig	Low	Government, Energy (ME region)	Espionage, Geopolitical	Spearphishing, exploitation of public-facing applications	Toolset not specified in current CloudSEK data
Predatory Sparrow (Gonjeshke Darande)	Low	Iranian financial infrastructure, state media	Geopolitical, Ideological, Destructive	DDoS, external defacement, financial theft, data data theft	Wiper malware, custom destructive payloads

MuddyWater: Expanded UAE Targeting

In early 2026, MuddyWater was documented using Microsoft Teams to conduct social engineering attacks, posing as IT support staff and asking employees to share their screens to capture passwords and MFA codes in real time. In the

background, they deployed Chaos ransomware as a false flag to disguise their actual espionage goals. Command-and-control traffic was routed through Starlink. This was documented by Rapid7.

CloudSEK intelligence also documented MuddyWater's expanded targeting of UAE organisations in early 2026, including phishing campaigns using regional airline-themed lures and corporate document decoys techniques consistent with the group's established pattern of region-specific social engineering. A separate campaign targeted UAE maritime and industrial firms using a multi-stage Remcos RAT delivery chain. CloudSEK also confirmed MuddyWater evolving its toolchain from BugSleep/MuddyRot to a Rust-based implant called RustyWater, underscoring the group's continued investment in detection evasion.

Nimbus Manticore (UNC1549): Wartime Cyber Operations

A significant CloudSEK cyber news intelligence report (June 1, 2026) documented that **Nimbus Manticore** (**UNC1549**, **IRGC**-linked) significantly expanded wartime cyber operations during the 2026 Middle East conflict. The group introduced a new modular backdoor, MiniFast, and continued deploying the MiniJunk malware framework. Initial access methods included phishing, distribution of trojanised software installers (including Zoom and SQL Developer), and SEO poisoning. Targeted sectors encompassed Aviation, Defence, Telecommunications, Software Development, and Government, with regional coverage spanning the US, Europe, Middle East, Africa, Saudi Arabia, and Australia. Notably, evidence suggests AI-assisted malware development practices to accelerate tooling adaptation and operational tempo.

APT35 / Charming Kitten:

CloudSEK intelligence provided an insider assessment of IRGC-linked APT35 operations which can be found here, covering their malware arsenal and victimology across the Middle East and international targets. Charming Kitten (also known as Mint Sandstorm and TA453) remained active through August 2026, confirming its sustained operational tempo. The group's targeting of the Education, Media and Entertainment, Research and Development, and Technology sectors in Israel, Iran, India, and the US reflects a broad intelligence collection mandate.

Stealth Falcon (UAE-attributed): Zero-Day Exploitation in Middle East Defence

Stealth Falcon APT, a UAE government-attributed group, was documented exploiting a zero-day vulnerability (CVE-2025-33053, Microsoft WEBDAV RCE) to specifically target high-profile defence entities in the Middle East. The group deployed deceptive URL files and custom spyware including the Horus Agent implant, designed to fingerprint victim machines and deploy next-stage payloads including keyloggers and credential dumpers. Microsoft patched CVE-2025-33053 in June 2025. This operation confirms that UAE-linked APT capability continues to evolve with zero-day acquisition and deployment against regional defence targets.

> **Note: Stealth Falcon is a UAE government-attributed group targeting entities in other regional countries**

Predatory Sparrow: Destructive Operations Against Iran

Predatory Sparrow (also known as Gonjeshke Darande) recorded sustained destructive activity during the reporting period. The group targets Iranian financial infrastructure including Bank Sepah and the Nobitex cryptocurrency exchange, as well as Iranian state media (IRIB). Its methods include direct network floods, external defacement, financial theft via cryptocurrency wallet manipulation, and data theft. The group's broader targeting pattern indicates geopolitical motivation rather than purely anti Iran objectives.

RedAlert Trojan: Weaponised Emergency Alert App

A RedAlert Trojan campaign was documented distributing a fake emergency alert application spread via SMS messages spoofing the Israeli Home Front Command. The malicious app harvested SMS messages, contact lists, and GPS location data from infected devices. This attack vector, exploiting civilian wartime anxiety to deliver mobile malware, represents a distinct social engineering category that increased during periods of conflict escalation.

Dark Web & Underground Activity

Threat intelligence data shows extensive dark web activity linked to Middle East countries during the reporting period. Turkey was the most-targeted country in dark web activity, followed by UAE, Israel (1,391), Saudi Arabia, and Egypt (858). This differs from the overall ranking (where Israel leads) because dark web activity captures criminal marketplace listings, data breach advertisements, access broker listings, and leaked credential sets, which correlate more with market size and enterprise IT footprint than with hacktivist targeting patterns.

Dark Web Sector Targeting

Financial Services and Government were the top sectors in dark web activity, followed by Finance, E-Commerce, Investments, Retail, Banking, Education (363), and Telecommunications (360). This profile is consistent with criminal market demand, financial sector data commands premium prices on underground forums, and government entity breaches attract both criminal buyers and nation-state-sponsored actors.

Notable Dark Web Events

A significant dark web event during the period:

- A threat actor known as the **Belsen Group** leaked configuration data and VPN credentials for over 15,000 Fortinet devices on the dark web (January 17, 2025, reported in CloudSEK cyber news), with the data reportedly stolen via **CVE-2022-40684** (authentication bypass) and released publicly in January 2025. The leak exposed device configurations, firewall rules, usernames, passwords, and SSL-VPN credentials for devices globally, including numerous Middle East deployments.
- The Salesforce Experience Cloud misconfiguration abuse campaign involving threat actor xpl0itrs (TeamPCP) included Middle East government and financial services targets, with access prices ranging from $2,000 to $40,000 per victim.

> Threat intelligence data shows a heavy concentration of credential theft, initial access broker listings, and leaked corporate data relating to UAE, Saudi Arabia, and Kuwait entities, reflecting sustained criminal marketplace interest in Gulf state enterprise infrastructure.

Vulnerability Exploitation & CVE Landscape

Network edge devices (VPNs, firewalls, SSL gateways), widely-deployed web frameworks (React, Apache), and cloud-native platforms (Kubernetes, Erlang/OTP for telecom/IoT) were the primary exploitation targets across the reporting period. Multiple critical vulnerabilities were added to CISA's Known Exploited Vulnerabilities (KEV) catalog and confirmed in active use. The following CVE table summarises the most significant vulnerabilities relevant to Middle East-operating organisations.

CVE	Vendor / Product	Vulnerability Class	CVSS	Observations
CVE-2025-55182	Meta / React Server Components (react-server-dom-webpack, -turbopack, -parcel) v19.0–19.2	Pre-authentication RCE via unsafe deserialization (CWE-502)	10	CVSS 10.0 Critical, EPSS 0.998 (99.96th percentile). KEV-listed 2025-12-05, due 2025-12-12. Known ransomware use confirmed. Over 77,000 IPs found vulnerable; 30+ organisations breached. Exploitation linked to Chinese state-associated threat actors. Exploit code publicly available. First disclosed Dec 3, 2025.
CVE-2025-32433	Erlang/OTP SSH server (versions prior to OTP-27.3.3 / OTP-26.2.5.11 / OTP-25.3.2.20); also affects Cisco telecom products (ConfD, NSO, Smart Phy, StarOS, Ultra Packet Core)	Pre-authentication RCE via SSH protocol message handling flaw (CWE-306, missing authentication)	10	CVSS 10.0 Critical, EPSS 0.986 (99.92nd percentile). KEV-listed 2025-06-09. Particularly impactful for Middle East telecoms and industrial IoT using Cisco telecom stacks. 10+ public PoC exploits available on GitHub. Ranked in GTI's 'Top 20 Most Exploited Vulnerabilities of 2025'.
CVE-2025-22457	Ivanti Connect Secure (pre-22.7R2.6) / Policy Secure (pre-22.7R1.4) / ZTA Gateways (pre-22.8R2.2)	Stack-based buffer overflow enabling unauthenticated RCE (CWE-121 / CWE-787)	9	CVSS 9.0 Critical, EPSS 0.9998 (99.98th percentile). KEV-listed 2025-04-04, due 2025-04-11. Known ransomware use confirmed. Exploited in-the-wild by UNC5221 (China-nexus) deploying TRAILBLAZE, BRUSHFIRE, and SPAWN malware suite. Obfuscation network used: compromised Cyberoam, QNAP, and ASUS devices.
CVE-2025-0282	Ivanti Connect Secure (pre-22.7R2.5) / Policy Secure (pre-22.7R1.2) / Neurons ZTA Gateways (pre-22.7R2.3)	Stack-based buffer overflow enabling unauthenticated RCE (CWE-121 / CWE-787)	9	CVSS 9.0 Critical, EPSS 0.9998 (99.98th percentile). KEV-listed 2025-01-08, due 2025-01-15. Known ransomware use confirmed. Exploited by UNC5337 (China, Mandiant attribution) using Dryhook, Phasejam, and SPAWN toolkits; credential and session data exfiltrated. Patching is strongly recommended. 10+ public exploits available.
CVE-2024-55591	Fortinet FortiOS 7.0.0–7.0.16 / FortiProxy 7.0.0–7.0.19 and 7.2.0–7.2.12	Authentication bypass via Node.js WebSocket module enabling super-admin privilege escalation (CWE-288)	9.8	CVSS 9.8 Critical, EPSS 0.983 (99.91st percentile). KEV-listed 2025-01-14, due 2025-01-21. Known ransomware use confirmed. Actively exploited: config and VPN credentials for 15,000+ Fortinet devices leaked by **Belsen Group** (Jan 2025). Exploited by **The Gentlemen** ransomware for initial access. Active exploitation confirmed by GTI. 10+ public exploits.
CVE-2025-24472	Fortinet FortiOS 7.0.0–7.0.16 / FortiProxy 7.0.0–7.0.19 and 7.2.0–7.2.12 (Security Fabric enabled)	Authentication bypass via alternate channel enabling super-admin escalation (CWE-288)	8.1	CVSS 8.1 High, EPSS 0.070 (93.7th percentile). KEV-listed 2025-03-18, due 2025-04-08. Known ransomware use confirmed. Exploited by Gunra ransomware (Conti-derived **RaaS**) in combination with **CVE-2024-55591**. Active exploitation confirmed.

CVE	Vendor / Product	Vulnerability Class	CVSS	Observations
CVE-2025-29824	Microsoft Windows Common Log File System (CLFS) Driver, Windows 10/11 and Windows Server 2008/2012	Use-after-free enabling local privilege escalation (CWE-416)	7.8	CVSS 7.8 High, EPSS 0.138 (96.2nd percentile). KEV-listed 2025-04-08. Known ransomware use confirmed. Exploited as a zero-day by Play ransomware in attacks on a US organisation. **Stealth Falcon** APT also exploited related Windows zero-day (**CVE-2025-33053**, WEBDAV RCE) against Middle East defence targets in June 2025.
CVE-2025-1974	Kubernetes ingress-nginx controller (widely deployed in cloud-native and enterprise environments)	Unauthenticated RCE via improper isolation in pod network (CWE-653); cluster-wide Secrets exposure	9.8	CVSS 9.8 Critical, EPSS 0.995 (99.94th percentile). KEV-listed status not confirmed in data. Named 'IngressNightmare'. 10+ public exploits. High risk for cloud-first Middle East organisations (UAE fintech, Saudi Vision 2030 digital infrastructure). No active exploitation in the Middle East confirmed by GTI, PLAUSIBLE risk.
CVE-2025-30065	Apache Parquet Java (parquet-avro module, versions ≤1.15.0)	Unauthenticated RCE via deserialization during schema parsing (CWE-502)	9.8	CVSS 9.8 Critical, EPSS 0.433 (98.6th percentile). Not KEV-listed. 9 public PoC exploits. Risk is primarily for data engineering pipelines processing Parquet files from external sources, relevant to Middle East banking and analytics platforms. No confirmed active exploitation.

Exploitation Trends

Three key trends characterise vulnerability exploitation relevant to the Middle East during the reporting period. First, network edge devices (Fortinet, Ivanti) continued to be the primary vector for initial access by both ransomware and APT actors, vulnerabilities in these products were the most frequently weaponised, with multiple KEV additions and confirmed ransomware use. Second, deserialization vulnerabilities in widely-deployed web and data frameworks (React, Apache Parquet, Apache Tomcat) achieved critical CVSS scores and near-universal EPSS scores, with React Server Components (**CVE-2025-55182**) becoming one of the most-discussed vulnerabilities of the entire reporting period (2,223 total mentions across social media, Telegram, and dark web sources). Third, cloud-native and container infrastructure (Kubernetes IngressNightmare) introduced a new class of cluster-wide compromise risk directly relevant to Middle East organisations undergoing cloud digitalisation. The average CVSS score of the nine most significant CVEs above is 9.2, all falling in the Critical or High severity bands.

Country-by-Country Assessment

Israel

Israel was the most targeted country in the Middle East region with the highest overall activity indicators and 5,447 hacktivism-specific entries. Sustained anti-Israel hacktivist campaigns by groups including **SKYNET**, **HeziRash**, **Handala**, **DieNet**, **OpIsrael**, and numerous coalition actors drove the high volume. APT operations by **MuddyWater** and **Charming Kitten/APT35** against Israeli government, health care, and technology entities added a high-stakes espionage dimension. Ransomware operators (**Nova**, **NasirSecurity**, nasirsecurity) also claimed incidents against Israeli targets, including the Yad Vashem Museum (Aug 2026). **Predatory Sparrow**'s operations were primarily outbound from an Israeli context, targeting Iranian infrastructure. The RedAlert Trojan campaign (March 2026) exploiting civilian emergency alert infrastructure demonstrated advanced exploitation of conflict-driven psychological vectors.

United Arab Emirates

The UAE recorded 2,588 total activity indicators and significant dark web mentions, the highest dark web volume of any Middle East country. UAE Critical infrastructure was targeted by **Handala** in a documented April 15, 2026 cyberattack. **MuddyWater** conducted multi-stage campaigns against UAE maritime and industrial firms (January 2026) and UAE businesses using fake AirArabia lures (February 2026). Ransomware incidents included **NasirSecurity** claiming 'the most massive hack in UAE history' (August 22, 2026), targeting Dubai Airport, UAE Customs (Federal Customs Authority), and other entities. **LockBit5** targeted soeuae.ae (August 2026). The Salesforce Experience Cloud misconfiguration abuse campaign (July 2026) included UAE government and financial services entities.

Saudi Arabia

Saudi Arabia recorded 1,880 total activity indicators and sustained dark web mentions. The kingdom was increasingly targeted by ransomware operators, particularly **The Gentlemen** (SAUD CONSULT, AWJ Holding, Almeer General Contracting) and **NasirSecurity**. Dark web criminal marketplace interest in Saudi entities (financial services, e-commerce, retail) remained persistently elevated. **Nimbus Manticore** (**UNC1549**, **IRGC**-linked) specifically named Saudi Arabia as a target region in expanded wartime cyber operations (June 2026). **Predatory Sparrow** targeted Saudi Games infrastructure, while Israeli conglomerate Shlomo's breach with Saudi dimensions. Saudi Arabia's Vision 2030 digitalisation agenda continues to expand the country's attack surface.

Turkey

Turkey recorded 3,419 total activity indicators, second only to Israel overall, and led all Middle East countries in ransomware-specific targeting. Turkey's large industrial, manufacturing, and logistics sectors made it an attractive ransomware target for **Nova**, **DragonForce**, Doommageddon, and **Deadlock**. Dark web activity for Turkey was the highest in the region, indicating high criminal marketplace interest in Turkish enterprise data. Turkey's strategic geographic position and NATO membership also makes it a target of politically-motivated actors, including **NoName057**(16) and regional hacktivist coalitions.

Egypt

Egypt recorded 1,389 total activity indicators, driven primarily by hacktivism (439 entries) and dark web activity (858 entries). Ransomware targeting of Egyptian organisations was documented, including the **Krybit** attack on Mima Foods (August 2026). Egypt's large banking and government sectors, along with its significant e-commerce and retail footprint, sustained elevated criminal interest.

Iraq, Kuwait, and Gulf States

Iraq (significant activity) faced significant hacktivist attention (506 entries), with government and media entities frequently targeted. Kuwait (notable activity) saw incidents including **NasirSecurity** targeting the Kuwait Ministry of Interior and **Qilin** ransomware targeting Black Cat Engineering & Construction WLL. Qatar and Jordan (652 feeds, primarily hacktivism 199 entries including eFAWATEERcom Bank DDoS) also featured. Oman (12 ransomware feeds) saw **LockBit5** target Towell Holding and **NasirSecurity** target Oman CC Energy Development. Bahrain (6 ransomware feeds) had the lowest direct ransomware exposure among Gulf states but remains part of the region-wide threat surface.

Iran

Iran (elevated activity levels) occupied a dual role: a major source of offensive cyber capability and a significant target of adversarial operations. Iranian state-linked threat actors, **MuddyWater** (Mango Sandstorm / TA450), **Charming Kitten** (Mint Sandstorm / **APT35** / TA453), **APT42**, **Nimbus Manticore** (**UNC1549**), Homeland Justice, **OilRig**, collectively account for 28+ active CloudSEK-tracked campaigns in the region. Iran was simultaneously targeted by hacktivists (1,884 hacktivist feeds, the second-highest in the region), including pro-Israel groups, anti-regime actors, and Predatory Sparrow. GTI's threat actor database identified 74 Iran-search-tagged entities active in the reporting period. The ongoing **IRGC** cyber programme continues to expand in scope, with documented AI-assisted tool development (**Nimbus Manticore**, June 2026).

Attack Technique Analysis

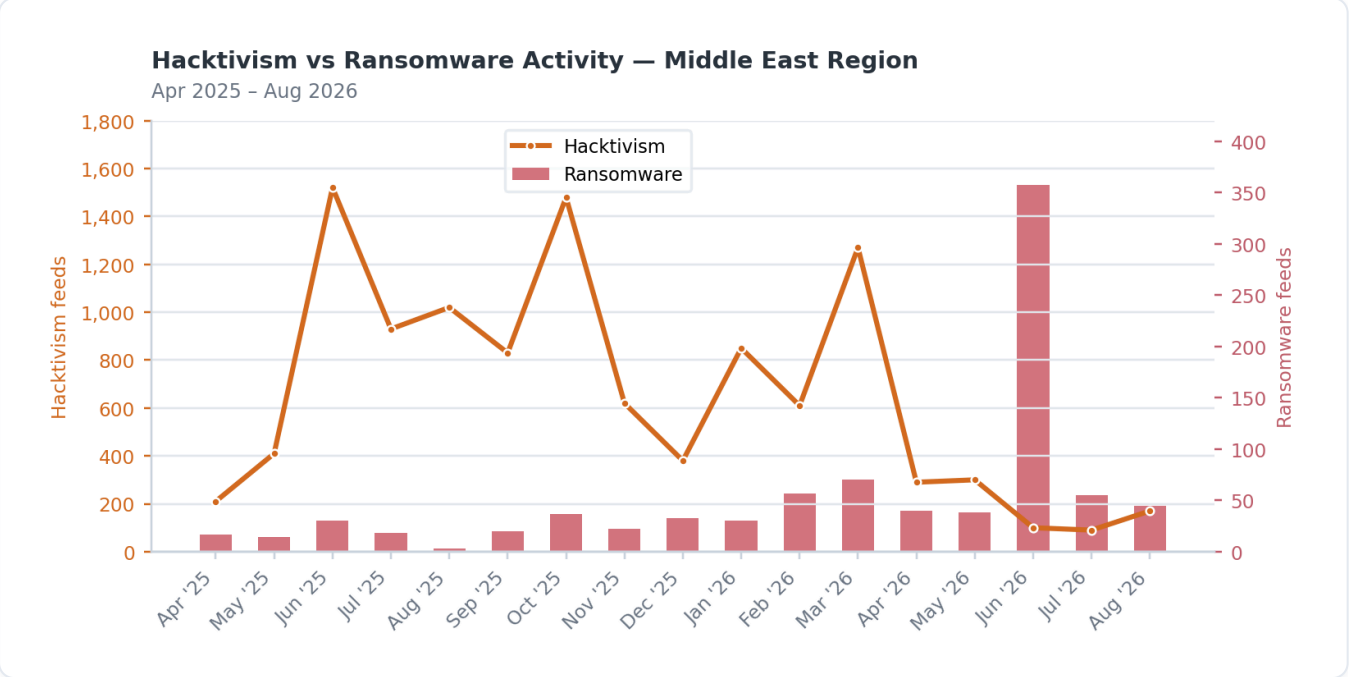
Dominant Attack Vectors

Attack Category	Volume Signal	Primary Actors (ME Context)	Primary Sectors Targeted	Key TTPs
DDoS / Denial of Service	High, dominant in hacktivism (extensive feeds)	SKYNET, HeziRash, DieNet, OpIsrael, Keymous, RipperSec, NoName057(16)	Government, Finance, Telecom, Media, Military	Direct Network Flood (T1498.001), Service Exhaustion (T1499.002), DDoSia tool, crowdsourced attack platforms
Ransomware / Data Encryption	Rising, sustained feeds, peaked in June 2026	Nova, The Gentlemen, Qilin, LockBit5, DragonForce, IncRansom, Handala	Industrial, Facility Mgmt, Manufacturing, Government, Finance	Phishing (T1566), VPN exploitation, valid accounts (T1078), data encryption (T1486), double extortion
Web Defacement	High, embedded in hacktivism volume	Khilafah Hackers, Moroccan Soldiers, multiple coalition groups	Government, Education, Media, Business Services	External defacement (T1491.002), SQL injection
Spearphishing / Social Engineering	Significant, APT & cybercrime primary vector	MuddyWater, Charming Kitten, APT35, Handala, DragonForce	Government, Defence, Diplomacy, Technology	Spearphishing attachment (T1566.001), spearphishing link (T1566.002), voice phishing (T1566.004), fake software installers
Vulnerability Exploitation	Critical, network edge & web frameworks	UNC5221, UNC5337, The Gentlemen, Gunra, Play ransomware, Stealth Falcon	All sectors (edge device exposure)	Exploit public-facing application (T1190), privilege escalation (T1068) via CVE-2024-55591, -2025-22457, -2025-0282, -2025-29824
Data theft / Leak	Significant, ransomware + APT + hacktivism	Qilin, DragonForce, MuddyWater, Charming Kitten, Nimbus Manticore, Handala	Government, Defence, Finance, Industrial	Data theft over C2 (T1041), Rclone, cloud storage abuse
Credential Theft / Account Compromise	High, dark web focused	Dark web actors, cybercrime syndicates, Initial Access Brokers	Financial Services, Banking, E-Commerce	Credential stuffing, stealer malware, phishing, exposed admin interfaces
Supply Chain Attack	Emerging, DragonForce MSP targeting	DragonForce (MSP cartel model)	IT Services, MSPs, enterprise customers	Trusted relationship (T1199), RMM tool abuse, white-label ransomware model
Wiper / Destructive Attack	Targeted, APT and hacktivist specific	Handala, Predatory Sparrow, Iranian actors	Government, Infrastructure, Finance	Data encrypted/wiped for impact (T1486), system shutdown/reboot (T1529)
Mobile Malware / Trojanised Apps	Targeted, conflict-context exploitation	Unknown actors (RedAlert Trojan campaign)	Civilian population, military-adjacent	Fake emergency alert app via SMS spoofing of Israeli Home Front Command

AI-Assisted Threat Actor Operations

Two documented instances of AI-assisted threat actor operations emerged in the reporting period. First, **MuddyWater** was observed using Google's Gemini AI model to obfuscate PowerShell code and impede static analysis of malicious payloads. Second, **Nimbus Manticore** (**UNC1549**) demonstrated evidence of AI-assisted malware development practices to accelerate tooling adaptation and operational tempo. These are the first instances of AI-facilitated offensive capability enhancement by Iranian-nexus actors targeting the Middle East.

Hacktivism vs. Ransomware: Diverging Trajectories



Hacktivism vs ransomware activity volumes, Middle East region, April 2025 – August 2026 (dual-axis overlay)

The dual-axis chart above illustrates a key structural divergence:

- Hacktivism (amber line) dominated early-to-mid 2025 and resurged in October 2025 and March 2026 before sharply declining from April 2026 onward.
- Ransomware (rose bars) followed a slower but more sustained upward trajectory, culminating in the June 2026 spike.
- The two activity types are largely anti-correlated in their monthly patterns, when hacktivism surged in June 2025 and October 2025, ransomware remained relatively subdued. The June 2026 ransomware peak occurred during the sharpest hacktivism decline of the entire period, suggesting that criminal ransomware operators and ideologically-motivated hacktivist groups operate largely independently and do not compete for the same operational windows.

Major Campaigns & Emerging Threats

Operation Roaring Lion: Israel-Iran Cyber-Kinetic Operation (February 2026)

On February 28, 2026, alongside military strikes on Iran, Israel carried out what has been widely described as one of the largest cyber operations on record against a country's digital infrastructure. Iran's internet connectivity reportedly dropped to below **4%** of normal levels. State news agencies including IRNA and the **IRGC**-linked Tasnim were taken offline. A widely used prayer app (BadeSaba, approximately 5 million users) was reportedly hacked to send push notifications urging Iranian soldiers to stop fighting. State TV satellite feeds were replaced with different content, and traffic cameras in Tehran were reportedly accessed for intelligence purposes.

Operation Anti-Israel Hacktivist Surge (June 2025 / October 2025 / March 2026)

Three distinct hacktivist surge events drove the regional hacktivism peaks: June 2025, October 2025, and March 2026. The March 2026 events are ('Regional Escalation of Hacktivist Activity in the Middle East, February 27–1st March 2026' and 'Regional Escalation of Hacktivist Activity in the Middle East, 2nd–5th March 2026'), indicating a coordinated multi-group campaign. **SKYNET**, **HeziRash**, **DieNet**, **OpIsrael**, **Keymous**, **DARKSTORM**, and **NoName057**(16) were consistently the most active actors across these surge events.

NasirSecurity Multi-Country Claimed Breach Campaign (August 2026)

In August 22, 2026, the CloudSEK ransomware feed recorded a cluster of events from threat actor **NasirSecurity** (also nasirsecurity, Nasir Security) claiming simultaneous breaches of multiple high-profile entities across five countries: Dubai Airport (UAE), UAE Customs / Federal Customs Authority (UAE), Kuwait Ministry of Interior (Kuwait), Yad Vashem Museum (Israel), Rumaila Operating Organisation (Iraq), and Oman CC Energy Development (Oman). The actor claimed this represented 'the most massive hack operation in UAE history. CloudSEK data records these as claims, independent verification of breach depth and authenticity is not confirmed by CloudSEK data alone.

Salesforce Experience Cloud Misconfiguration Abuse: Regional IAV Campaign

A threat actor xpl0itrs (linked to TeamPCP) selling unauthorized access to Salesforce Experience Cloud systems on dark web forums and Telegram, including Middle East government and financial services targets. Access was achieved by exploiting a known Salesforce Experience Cloud / Aura API misconfiguration, not a novel zero-day, allowing Guest User schema enumeration and object manipulation. Access prices ranged from $2,000 to $40,000. This campaign represents a structural risk for Middle East organisations that have deployed Salesforce Experience Cloud (including government portals and banking self-service platforms) without enforcing proper Guest User permission hardening.

RondoDox Botnet: React2Shell Weaponisation

RondoDox botnet weaponising **CVE-2025-55182** (React2Shell, the critical React Server Components RCE, CVSS 10.0) within weeks of its public disclosure. This rapid weaponisation-to-botnet timeline (public Dec 3, KEV Dec 5, botnet Dec 23) illustrates the accelerating exploit commercialisation cycle and its direct relevance to Middle East entities operating React-based web infrastructure.

Iranian Hacktivism Infrastructure: SKYNET & Proxy Network

Threat intelligence data revealed a significant Iranian-linked infrastructure element: the second highest-volume actor in the combined hacktivism feed for the period is a Telegram channel dedicated to distributing Iran-based proxy and VPN configuration tools (V2ray, Hiddify, Nekobox, Segaro, described in Persian). With 386 activity records, this channel

appeared alongside **SKYNET** (590), **HeziRash** (549), and **Keymous** (244) in the hacktivist actor feed aggregate. This suggests that a substantial portion of the 'hacktivist' activity volume is driven by Iranian technical infrastructure distribution rather than direct offensive action, indicating the breadth of Iran's cyber-support ecosystem.

Key Shifts in Threat Actor Behaviour

- **MuddyWater** evolved its toolchain from established implants to RustyWater (Rust-based), and began using AI (Gemini) for code obfuscation, indicating deliberate investment in detection evasion.
- **Nova** ransomware emerged in April 2025 and rapidly became one of the most active groups observed in the Middle East, with sustained operations through August 2026.
- **The Gentlemen** ransomware established a new, technically advanced **RaaS** operation exploiting Fortinet vulnerabilities, directly targeting Saudi Arabian businesses.
- **Handala** expanded its geographic scope from Israel-only targeting to include UAE critical infrastructure (April 2026), reflecting the geopolitical broadening of the conflict's cyber dimension.
- Iranian APT groups (**Nimbus Manticore** / **UNC1549**) documented AI-assisted malware development by June 2026, the first GTI-recorded instance of AI-facilitated offensive tooling acceleration for this actor.
- Hacktivist coalitions showed cyclical surge-and-decline patterns with three distinct peaks (Jun 2025, Oct 2025, Mar 2026), suggesting coordinated or event-triggered mobilisation rather than continuous baseline operations.
- Criminal initial access broker (IAB) activity, particularly around Salesforce, Fortinet, and Ivanti vulnerabilities, increased significantly throughout 2026, monetising vulnerabilities at speed.

Recommendations

PRIORITY 1 Patch Critical Network Edge Vulnerabilities Immediately

- Upgrade Fortinet FortiOS to versions ≥7.0.17 and FortiProxy to ≥7.0.20 / ≥7.2.13 to remediate **CVE-2024-55591** (CVSS 9.8) and **CVE-2025-24472** (CVSS 8.1), both KEV-listed and actively exploited by ransomware groups in the region.
- Upgrade Ivanti Connect Secure to ≥22.7R2.6, Policy Secure to ≥22.7R1.4, and ZTA Gateways to ≥22.8R2.2 to remediate **CVE-2025-22457** (CVSS 9.0, KEV) and **CVE-2025-0282** (CVSS 9.0, KEV), both actively exploited by China-nexus UNC5221/UNC5337.
- Review and rotate all FortiGate/FortiProxy admin credentials and SSL-VPN credentials in light of the **Belsen Group** dark web dump (January 2025) exposing 15,000+ device configurations.
- Audit Kubernetes ingress-nginx deployments for **CVE-2025-1974** (IngressNightmare, CVSS 9.8, EPSS 0.995), restrict pod network access to the ingress controller and apply the vendor patch immediately.

PRIORITY 2 Harden Web Application and API Surfaces

- Upgrade React Server Components to versions ≥19.0.1 / ≥19.1.2 / ≥19.2.1 to remediate **CVE-2025-55182** (CVSS 10.0, KEV-listed, ransomware-used, EPSS 0.998). This is the highest-priority web framework patch in the reporting period.
- Audit all Salesforce Experience Cloud / Aura API deployments for Guest User permission exposure. Enforce Field-Level Security, disable Guest User record creation, and restrict Aura API access to authenticated sessions only.
- Inventory Apache Parquet Java usage in data pipelines and upgrade to ≥1.15.1 to remediate **CVE-2025-30065** (CVSS 9.8). Apply 'org.apache.parquet.avro.SERIALIZABLE_PACKAGES' configuration restrictions.
- Apply Erlang/OTP SSH patches (OTP-27.3.3 / OTP-26.2.5.11 / OTP-25.3.2.20) for **CVE-2025-32433** (CVSS 10.0, KEV-listed), particularly critical for Middle East telecoms operators using Cisco ConfD, NSO, or OTP-based IoT infrastructure.

PRIORITY 3 Anti-Phishing and Social Engineering Defences

- Deploy advanced email security with **MuddyWater**-specific lure theme detection, particularly regional airline booking themes and corporate document decoys. **MuddyWater**'s use of NordVPN as a phishing credibility prop should be blocked at URL filtering.
- Implement **FIDO2**/hardware MFA for all government, defence, and financial services personnel to counter **Charming Kitten**'s spearphishing credential-harvest campaigns.
- Alert mobile users to verify emergency alert app sources, the RedAlert Trojan campaign (March 2026) demonstrates that wartime stress creates effective social engineering conditions for mobile malware.
- Configure Conditional Access policies blocking RMM tool abuse, **MuddyWater** and **DragonForce** both extensively abuse legitimate remote management tools (T1219) for persistence.

PRIORITY 4 **Ransomware Resilience**

- Implement immutable, offline backups for all critical industrial, infrastructure, and government systems, ransomware groups operating in the region (**Nova**, **The Gentlemen**, **DragonForce**) routinely delete accessible backups as a pre-encryption step.
- Restrict Rclone, MEGAsync, and other cloud sync tools at the perimeter, **The Gentlemen** and **DragonForce** use these for pre-encryption data data theft enabling double-extortion.
- Segment operational technology (OT) networks from IT networks, the high ransomware targeting of Facility Management, Industrial, and Infrastructure sectors indicates ransomware actors are prioritising OT-adjacent targets for maximum operational disruption.
- Monitor for anomalous NetExec, PowerShell remoting, and lateral movement patterns, **The Gentlemen**'s documented TTPs include extensive NetExec use for lateral movement post-initial-access.

PRIORITY 5 **DDoS and Hacktivism Preparedness**

- Ensure DDoS scrubbing and traffic diversion services are contractually active and tested for government, financial services, and telecom entities in Israel, UAE, Saudi Arabia, and Turkey, these are the most consistently targeted countries in hacktivist surge events.
- Pre-position incident response playbooks for coordinated hacktivist surge events (historically June, October, and March have been peak months) to enable faster response and communication.
- Harden web application firewalls against SQL injection (used by **DieNet**) and volumetric application-layer floods (T1499.002, used by **NoName057**, **DieNet**, **SKYNET**).
- Monitor Telegram channels and dark web forums for advance coordination of **OpIsrael**, **DieNet_**Network, **SKYNET**, and **DARKSTORM** operations, threat intelligence data provide early warning signals for coordinated attacks.

Conclusion

The Middle East cyber threat landscape from April 2025 through August 31, 2026 was characterised by an unusually high density of concurrent threat types: politically-motivated hacktivism at industrial scale, accelerating ransomware operations against critical sectors, sustained and evolving APT campaigns by Iranian and Israeli-linked state actors, and active exploitation of multiple critical vulnerabilities with Middle East-relevant attack surfaces. The extensive activity indicators recorded over the 17-month window, with the single highest month reaching 2,245 in March 2026, demonstrate that the region's threat environment is not merely elevated but structurally complex.

The most critical risk trend entering the post-reporting window is the sustained growth of ransomware targeting, which accelerated dramatically in June 2026 (the period's ransomware peak) and showed no signs of reverting to baseline by August 2026. The combination of new advanced ransomware operators (**Nova**, **The Gentlemen**), active exploitation of Fortinet and Ivanti vulnerabilities, and AI-assisted dark web activity creates conditions for continued escalation. Simultaneously, Iranian APT groups documented AI-assisted malware development in June 2026, signalling an acceleration of offensive capability enhancement that will likely manifest in more advanced campaigns in the near term.

The combination of criminal ransomware activity (primarily financially motivated) and state-sponsored cyber operations (politically motivated) at the same regional targets, government, financial services, and critical infrastructure, means that Middle East organisations face a uniquely compressed threat environment. A successful state-actor compromise of a financial institution can create pathways exploited by criminal actors and vice versa. Defenders must adopt threat-informed architecture that addresses both high-volume hacktivist noise and low-signal, long-dwell APT operations simultaneously.

> CloudSEK assesses the Middle East cyber threat environment as ELEVATED-HIGH for the period immediately following this report. The risk is highest for: (1) Israeli government, health care, and defence entities facing sustained multi-vector attacks; (2) UAE and Saudi critical infrastructure organisations facing ransomware escalation and APT interest; (3) Turkish industrial and manufacturing firms facing the highest ransomware targeting volume in the region; and (4) organisations across the region operating unpatched Fortinet, Ivanti, React, or Kubernetes infrastructure.

Despite the overall elevated threat picture, the data also shows patterns of restraint and cyclicality in hacktivist operations, the sharp post-March 2026 decline in hacktivism may indicate operational fatigue, command-and-control disruption of key hacktivist infrastructure, or a deliberate strategic shift to more targeted operations. Organisations should not interpret reduced hacktivist noise as reduced overall risk, given the inverse trend in ransomware and APT activity over the same period.

CloudSEK

Predict ◆ Protect ◆ Quantify

We **Predict** Cyber Threats **Before They Strike**

Registered Office:

CloudSEK Research Pte. Ltd.
160 Robinson Road, #20-03, Singapore Business Federation Center, Singapore - 068914

Regional Office : India

CloudSEK Information Security Pvt Ltd.
16/1, Cambridge Rd, Halasuru, Cambridge Layout, Jogupalya, Bengaluru, Karnataka - 560008

Regional Office : United States

CloudSEK Inc.
8 The Green, Ste A, Dover, DE - 19901, United States

Regional Office : United Kingdom

CloudSEK, 2 Kingdom Street,
6th Floor London, W2 6BD - United Kingdom

CloudSEK

info@cloudsek.com www.cloudsek.com

Scan for a free Demo of CloudSEK platform