TJDEED TECHNOLOGY

REGIONAL INTELLIGENCE BRIEF

Identity Under Fire

How the 2025–2026 Middle East Conflict Reshaped the Identity Threat Landscape — and What Organizations Must Do Now During the Ceasefire Window

Classification:	**Restricted — Client Use Only**
Published:	April 2026
Prepared by:	TJDEED Threat Intelligence Unit

Executive Summary

> *The 2025-2026 Middle East conflict has produced the highest concentration of identity-targeted cyberattacks ever recorded in the MENA region. A 2-week ceasefire agreement reached in April 2026 has created a temporary pause — but this window is not a signal of reduced risk. It is the most critical 14 days your organization will have to harden your defenses before operations resume.*

During the active conflict period (October 2023 – April 2026), TJDEED's threat intelligence unit monitored over 4,200 cyber incidents affecting organizations across Jordan, the UAE, Saudi Arabia, Egypt, Qatar, and Bahrain. Of these, identity-related attacks — credential theft, account compromise, unauthorized access, and privilege escalation — accounted for the single largest category of successful breaches.

This report presents our findings, the specific threat actor groups active in the region, the attack vectors they favor, and a concrete readiness checklist organizations can act on immediately.

Key Findings at a Glance

68% of breaches	Of confirmed breaches in the MENA region during the conflict period began with a compromised identity — credential theft, phishing, or unauthorized access escalation.
4.45M avg. breach cost (USD)	IBM Cost of a Data Breach 2025: average total cost of a breach in the Middle East — second highest globally after the United States.
197 days avg. dwell time	The average time between initial identity compromise and detection in regional organizations — nearly 6.5 months of undetected attacker presence.
70+ active threat groups	Hacktivist and state-affiliated threat groups documented as operating in or targeting the MENA region during the conflict escalation in 2025–2026.
3x phishing increase	Phishing attempt volume against regional organizations in Q1 2026 compared to Q1 2024, driven by conflict-linked social engineering campaigns.

The Identity Threat Landscape

Identity has become the primary battlefield in the region's hybrid warfare environment. Unlike traditional network intrusion, identity attacks are harder to detect, easier to scale, and devastatingly effective — because a compromised credential looks exactly like a legitimate user.

The Four Identity Attack Vectors in Active Use

1. Spear Phishing — Conflict-Themed Lures

The conflict provided attackers with an unprecedented supply of credible lures. TJDEED observed campaigns using fake emergency evacuation notices, spoofed government security advisories, and fraudulent "missile alert" applications to harvest credentials. These campaigns targeted employees at financial institutions, logistics companies, and government contractors across Jordan, the UAE, and Saudi Arabia.

- Impersonation of official government cybersecurity bodies (CERT Jordan, UAE NCSC, Saudi NCA)
- Fake HR communications about emergency work-from-home policy updates
- Fraudulent banking security alerts tied to conflict-period system maintenance
- LinkedIn-based impersonation targeting C-suite executives and IT administrators

2. Credential Stuffing at Scale

Iranian-linked threat actors, including groups affiliated with Charming Kitten (APT35) and MuddyWater, operated large-scale credential stuffing infrastructure targeting regional organizations. Using credentials from previous global breaches, attackers systematically tested access against VPN portals, email systems, and SaaS applications.

- Focus on organizations with known legacy VPN deployments (no MFA)
- Targeting of Microsoft 365 and Google Workspace tenants
- After-hours access attempts timed to reduce detection likelihood

3. Privilege Escalation via Misconfigured Active Directory

Once initial access was established through compromised credentials, attackers consistently exploited Active Directory misconfigurations to escalate privileges. TJDEED's incident response team documented identical lateral movement patterns across multiple regional organizations — indicating coordinated or tool-shared attack playbooks.

- Exploitation of default or weak service account passwords
- Kerberoasting attacks against AD environments with SPNs on user accounts
- Pass-the-hash and pass-the-ticket techniques for lateral movement

- Targeting of Domain Admins through delegation attack paths

4. SIM Swapping and SMS MFA Bypass

Several high-profile breaches in the Gulf involved SIM swapping attacks against executives and IT administrators — bypassing SMS-based MFA by compromising mobile numbers. This vector specifically targets organizations that rely on SMS as their only MFA method.

- Coordinated campaigns against telecom providers in 3 GCC countries
- Targeting of executives whose mobile numbers were exposed in public directories
- Exploitation of telecom-level vulnerabilities (SS7 protocol weaknesses)

Active Threat Actor Profiles

The following threat actors were specifically documented by TJDEED intelligence as conducting identity-targeted operations against regional organizations during the conflict period.

Threat Actor	Origin	Primary Targets	Primary Identity Method
Charming Kitten (APT35)	Iran-affiliated	Finance, Gov, Tech — UAE, Jordan, KSA	Spear phishing, credential harvesting portals, MFA bypass
MuddyWater (APT34)	Iran-affiliated	Telecom, Energy, Government — Gulf	VPN credential stuffing, RAT deployment post-access
Cyber Fattah	Hacktivist	Corporate & Media — Israel, Jordan	Mass phishing, data leak via compromised accounts
DieNet	Hacktivist	Banking, Infrastructure — Regional	Credential dumps, defacement via CMS account takeover
Shadow Unit	Multi-origin	Universities, NGOs — Egypt, Jordan	Account compromise, credential theft, data publication
Pioneer Kitten	Iran-affiliated	Critical Infrastructure — Broad MENA	VPN exploitation, AD privilege escalation, ransomware staging

Ceasefire Period: Why Threat Activity Does Not Stop

The 2-week ceasefire agreement reached in April 2026 should not be misread as a reduction in cyber threat activity. TJDEED's analysis of previous ceasefire and de-escalation periods in the region's conflict cycle shows a consistent pattern:

- Threat actors use ceasefire periods to consolidate existing access rather than stand down
- Previously compromised credentials and backdoors remain active and exploitable
- The period immediately following a ceasefire historically shows a spike in ransomware deployment — attackers who gained access during active conflict activate their payloads
- Geopolitical uncertainty increases insider threat risk, as employees face pressure from external actors

> Recommendation: Treat the ceasefire window as the most urgent 14 days for security hardening, not a period of reduced vigilance. Any attacker who has established identity-level access during the conflict period now has time to move laterally, escalate privileges, and stage their payload without the noise of ongoing conflict operations masking their activity.

Sectoral Impact Analysis

Identity attacks were not evenly distributed across sectors. The following sectors experienced the highest concentration of identity-related breaches and credential-targeting campaigns during the conflict period.

Financial Services

Banks and financial institutions were the single most targeted sector, representing 31% of all documented identity incidents. The combination of high-value access credentials, strict regulatory environments that create compliance pressure, and the strategic value of financial disruption made financial organizations priority targets.

- Corporate banking portal credentials harvested via executive phishing
- SWIFT operator accounts targeted through social engineering
- API credentials for fintech integrations compromised via third-party suppliers

Government & Public Sector

Government agencies and public sector organizations faced persistent, sophisticated campaigns. The strategic value of government credentials — both for espionage and for disruption — drove targeted, patient attack campaigns rather than opportunistic phishing.

- Ministry-level Active Directory accounts targeted for privilege escalation
- Contractor and vendor credentials used as initial access vectors into government networks
- Citizen data portals compromised through administrator credential theft

Logistics & Transportation

Regional logistics and transportation companies faced a surge in identity attacks linked to supply chain intelligence gathering. Attackers specifically targeted operations systems and tracking platforms to monitor supply movements.

Healthcare

Healthcare organizations became a significant new target vector during the conflict, with attackers recognizing that healthcare institutions often run legacy identity infrastructure with minimal MFA enforcement and high staff turnover creating credential management gaps.

The 14-Day Ceasefire Window: A Readiness Checklist

The following checklist reflects the minimum hardening steps TJDEED recommends every regional organization complete during the current ceasefire window. Items are prioritized by impact and speed of implementation.

CRITICAL — Complete Within 48 Hours

!	Audit all privileged accounts (Domain Admin, Local Admin, Service Accounts) — identify any created in the last 6 months without formal change control
!	Force password reset for all accounts with administrative privileges
!	Disable all dormant accounts inactive for 90+ days
!	Enforce MFA on all VPN and remote access portals — SMS-based MFA is NOT sufficient; use authenticator apps or hardware tokens
!	Review all SIEM alerts from the past 30 days for unaddressed identity anomalies — after-hours logins, impossible travel, bulk data access

HIGH PRIORITY — Complete Within 7 Days

H	Implement Privileged Access Management (PAM) for all privileged accounts — session recording and just-in-time access are minimum requirements
H	Conduct AD health check — identify Kerberoastable accounts, accounts with unconstrained delegation, and stale SPNs
H	Review all third-party and vendor access — remove access for inactive vendors, force MFA for all active vendor accounts
H	Enable conditional access policies — block authentication from high-risk countries and anonymizing proxies
H	Deploy Security Awareness training focused specifically on current conflict-themed phishing lures

IMPORTANT — Complete Within 14 Days

I	Implement Identity and Access Management (IAM) with role-based access control — ensure least-privilege principle is enforced across all systems
I	Deploy Single Sign-On (SSO) to centralize authentication and reduce credential sprawl

I	Implement SIEM correlation rules specific to the attack patterns documented in this report — PAM session anomalies, AD privilege escalation, credential stuffing patterns
I	Conduct a simulated phishing exercise using conflict-themed lures to assess employee susceptibility baseline

How TJDEED's Identity Hardening Pack Addresses These Threats

TJDEED's Identity Hardening Pack was designed specifically in response to the threat landscape documented in this report. It bundles four critical solutions that address the full identity attack chain — from initial access through privilege escalation and detection.

IAM	Identity & Access Management — centralized control over who can access what, with role-based enforcement and automated provisioning/de-provisioning. Addresses: credential sprawl, over-permissioned accounts, dormant account risk.
MFA	Multi-Factor Authentication — TOTP and hardware token-based MFA that eliminates SMS-based bypass vulnerabilities. Addresses: SIM swapping, credential stuffing, VPN brute force.
PAM	Privileged Access Management — session recording, just-in-time access, and privilege vaulting for all administrative accounts. Addresses: AD privilege escalation, lateral movement, insider threat.
SIEM	Security Information & Event Management — real-time correlation of identity events across all systems, with pre-built detection rules for the attack patterns in this report. Addresses: long dwell times, undetected lateral movement, privilege abuse.

Deployment Timeline

TJDEED's Identity Hardening Pack is designed for rapid deployment in the context of an urgent threat environment:

- Week 1–2: MFA enforcement across all remote access and privileged accounts
- Week 3–4: PAM deployment and privileged account vaulting
- Week 5–6: IAM role-based access review and remediation
- Week 7–8: SIEM correlation rules tuned to regional threat patterns

Next Steps

TJDEED is offering a complimentary 30-minute Identity Readiness Assessment for organizations in the MENA region during the ceasefire period. In this session, our threat intelligence team will review your current identity posture against the attack patterns documented in this report and identify your highest-priority remediation actions.

Book your Identity Readiness Assessment: info@tjdeed.com | tjdeed.com/identity-assessment

DISCLAIMER & SOURCES

This report is based on threat intelligence gathered by TJDEED Technology's security operations team, combined with publicly available intelligence from Check Point Research, Group-IB, Resecurity, Cyble, the World Economic Forum Cybersecurity Centre, and IBM's Cost of a Data Breach 2025 report. Specific incident data has been anonymized to protect client confidentiality. Statistical claims reflect regional observations and publicly reported figures and should be considered indicative rather than exhaustive. TJDEED Technology makes no warranty as to the completeness of this intelligence. Organizations should conduct their own threat assessments. This report may not be redistributed without written permission from TJDEED Technology.