everbridge

Cybersecurity Threat Assessment

Conflict-Driven Cyber Threats Continue to Target UAE, Signal Elevated Risk Across the Gulf

April 2, 2026

Bottom Line Up Front

- As of April 2, cyberattacks across the Gulf region have sharply increased in connection with the ongoing US/Israel-Iran conflict, with daily volumes in the United Arab Emirates (UAE) reportedly tripling from pre-conflict levels to as many as 700,000 attacks per day.
- While most observed activity remains high-volume and often low-impact, the threat landscape includes distributed denial of service (DDoS), ransomware, data breaches, data leaks, wiper malware, and website defacement, which can still cause meaningful disruption for inadequately protected organizations.
- Although the UAE is experiencing the most visible surge in cyber activity, the threat environment spans the wider Gulf and conflict-linked geographies, and is likely to persist beyond a ceasefire, positioning UAE-based organizations as sustained high-value targets and increasing pressure on firms to demonstrate resilience and continuity under ongoing cyber stress.
- The increasing use of artificial intelligence is accelerating the scale, speed, and sophistication of cyber threats, enabling more effective phishing, automation, and intrusion techniques, while creating an urgent requirement for organizations to adopt AI-enabled defenses, workforce training, and resilience strategies to maintain operational security and credibility.

Risks and Vulnerabilities Summary

- **Credential compromise and identity risk**: The surge in phishing, social engineering, token theft, and session hijacking increases the likelihood of unauthorized access, employee error, and insider compromise.
- **Data integrity and destructive risk:** Reported activity includes ransomware, data leaks, and wiper malware, increasing risk to business continuity, recovery timelines, and the integrity of internal and customer data.
- **Operational continuity**: Dependence on regional cloud, hosting, and customer-facing platforms increases exposure to service degradation, failover strain, and outages if shared infrastructure is targeted.
- **Critical infrastructure interdependency**: Highly digitized and interconnected sectors such as energy, aviation, ports, and smart city systems increase the risk of cascading disruption across transport, utilities, and communications.
- **Incident response saturation**: Sustained attack volumes risk overwhelming security operations centers, increasing alert fatigue, and the likelihood that targeted intrusions go undetected.
- **Regulatory and compliance exposure**: Increased incident frequency raises scrutiny from UAE regulators and international partners, elevating the risk of penalties, reporting obligations, and contractual liabilities.

Contact: GlobalInsightsTeam@everbridge.com

everbridge

Outlook and Assessment

- The UAE is likely to remain in a sustained elevated cyber-threat posture in the near term, with high-volume activity continuing even if most incidents are disrupted before causing major damage.
    - **Confidence: High.** The UAE remains one of the most persistently exposed Gulf states, hosts critical infrastructure and US-linked firms, and is a frequent target, making sustained elevated activity highly likely.
- Corporate exposure is greatest for finance, government-adjacent services, logistics, aviation, energy, and cloud-dependent firms in the UAE, especially those with cross-border vendors or customer-facing portals.
    - **Confidence: Moderate.** These sectors are high-value and central to UAE operations and its role as a regional hub, but specific targeting priorities remain unclear.
- Spillover into neighboring Gulf states and shared service providers is likely to continue, so organizations with operations in or ties to the UAE should expect indirect disruption even when their own networks are not directly targeted.
    - **Confidence: Moderate**. Regional interconnectivity and alliance with the US increase spillover risk, but the scale and timing remain uncertain.
- The most likely tactics over the next several weeks are AI-enabled phishing, fraud, disinformation, DDoS, and credential theft, with destructive activity such as wiper attacks remaining lower-frequency but material.
    - **Confidence: Moderate.** AI is increasing the scale and effectiveness of social engineering and intrusion attempts, though the frequency of destructive attacks remains uncertain.

- **Potential indicators of escalation:** increased volume and frequency of malicious cyber activity, successful ransomware or wiper attacks, prolonged service outages, confirmed compromise of government or financial platforms, and new warnings from UAE or regional authorities identifying targeted sectors or infrastructure.
- **Potential indicators of de-escalation:** a sustained reduction and normalization in attack volume, fewer UAE- or Gulf Cooperation Council (GCC)-targeted claims, shorter recovery times, no new destructive malware activity, and a shift in official messaging from active defense to routine monitoring.
- **Business implications:** Organizations with operations in the UAE and across the broader Gulf and Eastern Mediterranean should maintain elevated monitoring, strengthen phishing and payment-verification controls, and conduct regular employee training and simulated attack exercises to reduce human-factor risk. Firms should also validate incident response and business continuity plans, test cloud and vendor failover capabilities, and ensure rapid containment procedures are in place to mitigate disruption to digital services and operations.

Global Insights Confidence Levels

High	Moderate	Low
This judgment is based on strong, credible, and typically corroborated reporting, supported by a clear analytic basis and relevant precedent or observable indicators. Some uncertainty may remain, but it is unlikely to change the core assessment.	This judgment is based on a reasonable body of reporting and sound analytic reasoning, but important gaps, conflicting information, or a fluid environment leave meaningful uncertainty. New information could materially refine or alter the assessment.	This judgment is based on limited, fragmentary, weakly corroborated, or highly uncertain reporting, or on a scenario with several unresolved variables. The assessment is plausible, but it should be treated with caution because new information could significantly change it.

Contact: GlobalInsightsTeam@everbridge.com