Executive summary
Current cyberthreats in the Middle East

This study focuses on the Middle Eastern cyberthreat landscape considering two waves of conflict escalation involving Iran in June 2025 and Q1 2026 (with the start of the U.S. and Israeli military operation launched on February 28). This report offers a comprehensive analysis of the threat landscapes of the most targeted countries in the region, identifying how they correlate with geopolitical conflicts, as well as industrial profiles and economic situation. Forecast of future regional cyberthreats and actionable defense recommendations are given.

Regional growth drivers

Oil- and gas-producing countries in the Middle East (Qatar, the UAE, and Saudi Arabia) are aimed to diversify their economies to reduce reliance on oil exports. The shift toward high-tech industries specifically biotechnology, quantum computing, and nuclear energy is aimed at achieving this goal.

The drive for digital sovereignty, the need for national security amidst complex geopolitics, and the demand for massive data and computing power for AI solutions have led to a trend in the Middle East to reduce reliance on cross-border digital architectures. This applies not only to data hosting but also to the localization of critical hardware capabilities.

Currently, this sector faces a number of constraints:

- shortage of qualified AI-specialists;
- risks associated with the data center's geographical location and the periodic escalation of conflicts;
- need for Middle Eastern countries to balance between Chinese and US technology companies.

Leading regional economies

The region's growth drivers are shaped by its strongest economies and their development trajectories. Typically, these same countries lead in the number of cyberattacks they face due to their highly digitized infrastructure and attackers' interest in financial gain and confidential data theft.

According to the International Monetary Fund's 2026 forecast, the leading Arab nations are **Qatar, the UAE, and Saudi Arabia**.

- Qatar's economy is based on oil and gas extraction;
- the UAE is investing in service sectors as it seeks to diversify its economy;
- Saudi Arabia is investing in non-oil economic sectors to digitize its industrial infrastructure.

Cybersecurity threatscape in the Middle East

The reporting period (Q2 2025–Q1 2026) saw two acute phases of the conflict surrounding Iran: **June 13–24, 2025** (though some attacks were discovered in July, affecting Q2 and Q3 data) and **February–March 2026**. This significantly impacted the region's cyberthreat landscape.

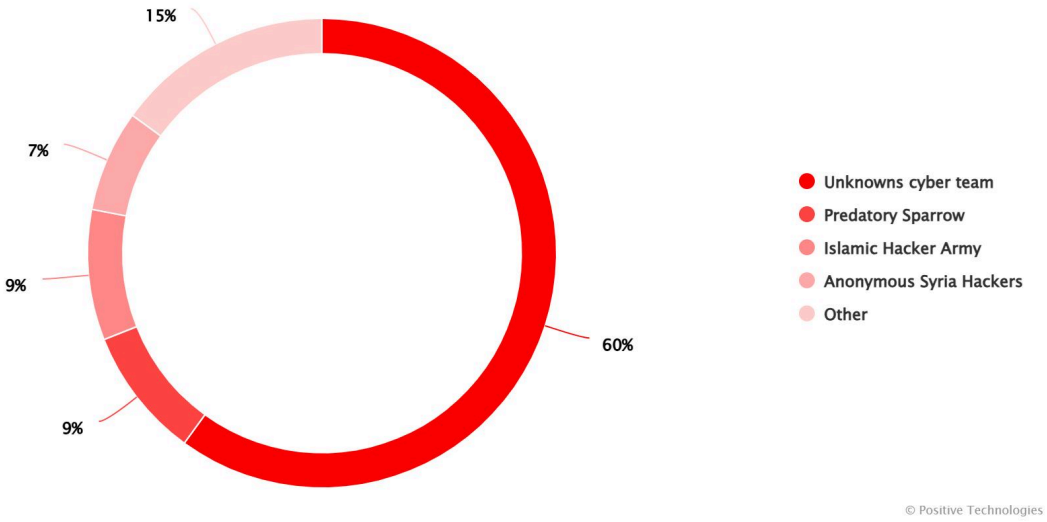
The June incidents primarily affected Iran and Israel, while the incidents that took place in Q1 2026 accompanied the U.S. and Israeli military operation launched on February 28, impacted other Middle Eastern countries involved in the conflict. The cyberattacks were mostly aimed at halting critical infrastructure operations and shaping public opinion through attacks on the media, spreading disinformation on social networks, and demonstrating the vulnerability of major state institutions.

June and July, 2025

During the conflict's acute phase (June 13–20), over 250 hacktivist attacks, including DDoS, data leaks, and website defacements, targeted the Middle East, primarily hitting Iran and Israel. Elsewhere in the region, financially motivated ransomware groups dominated.

Analysis of dark web forums and Telegram channels reveals that most hacktivist attacks on Iran were carried out by the cybergroup **The Unknowns** (accounting for 60% of listings related to breaches of Iranian companies on underground forums), followed by **Predatory Sparrow** and the **Islamic Hacker Army** (9% each).

Figure 1. Groups that attacked Iran in June 2025



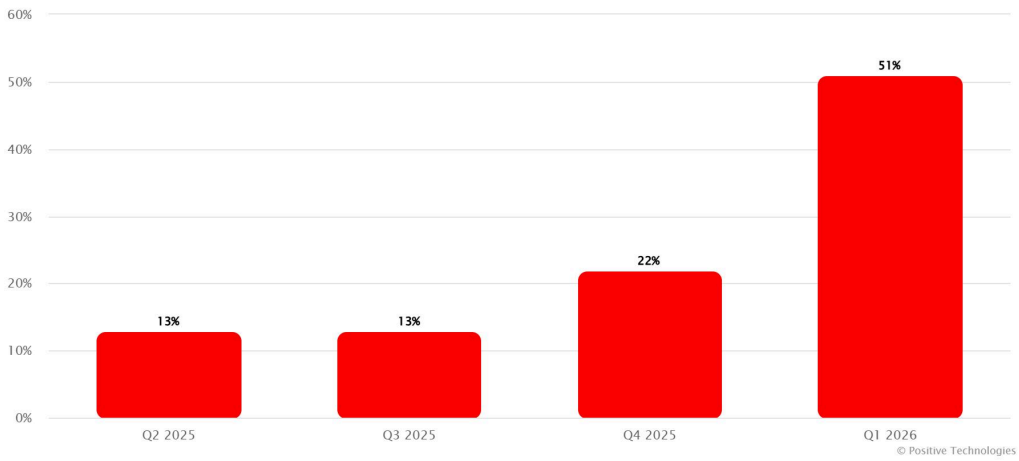
In Israel, the **Handala Hack Team** operated alongside state-sponsored groups **APT35 and APT42**. Handala Hack Team, an alleged hacktivist group, targeted Israeli industrial and medical organizations using phishing, data theft, extortion, and destructive wiper attacks, successfully seizing infrastructure and stealing confidential data.

Researchers assess that both APT35 and APT42 act in Iran's interests. APT35 carries out long-term, resource-intensive cyberespionage campaigns. They target military personnel, diplomats, and government officials in the Middle East and the U.S., along with the media, energy, defense, and telecom sectors. APT42 also focuses on cyberespionage, targeting organizations and individuals primarily in the Middle East.

February and March 2026

Due to geographic expansion, Q1 2026 accounted for 51% of all attacks during the reporting period. At the same time, **the geographic expansion drove a sharp increase in cyberattacks** in Kuwait, Qatar, and Cyprus. The relatively low number of attacks in Q2 2025 is due to the brief nature of the conflict escalation. Furthermore, because incidents were discovered across both June and July, the data is split between the second and third quarters.

Figure 2. Distribution of attacks by quarter over the entire reporting period

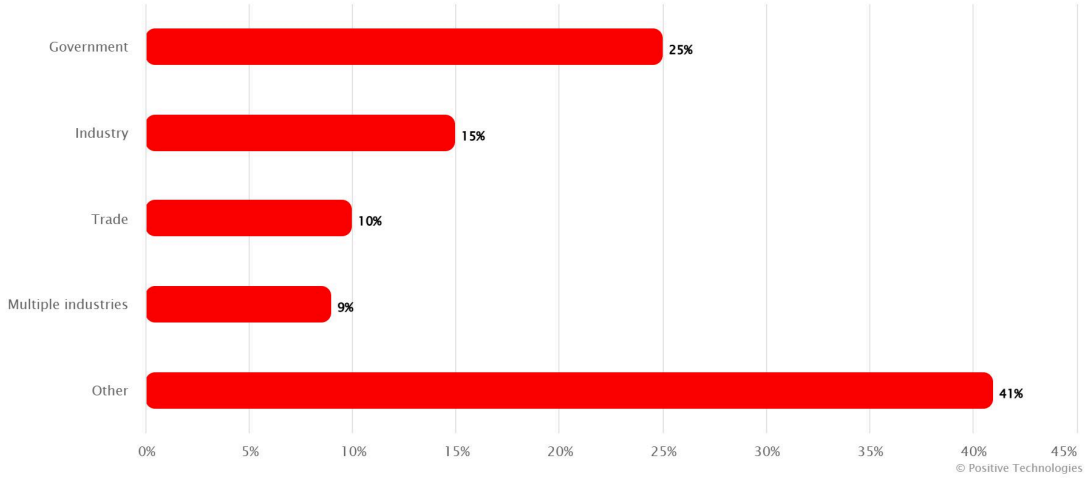


Industry data shows that during escalations, attackers prioritized the government and transport sectors. This indicates a strategy of targeting critical information infrastructure to inflict national damage and demoralize the public by exposing vulnerabilities. **Successful attacks on media organizations also spiked during both conflict periods.**

Government institutions from Qatar, Kuwait, and Israel accounted for 45% of targeted national-level organizations in Q1 2026. In Iran attackers focused on manipulating public opinion. Major Iranian news agencies also suffered website outages. Furthermore, Q1 2026 saw attacks spread to previously untouched sectors, with incidents in educational and scientific institutions rising to 5%.

The region's industry breakdown reflects two main trends: conflict-driven attacks on government institutions (25% of all attacks) and attacks on industry (15%) and retail (10%) during de-escalation phases.

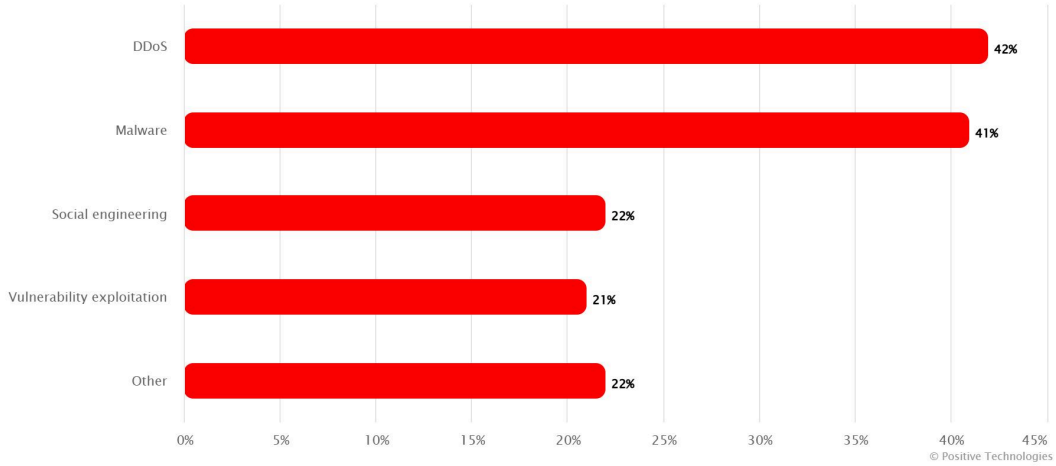
Figure 3. Distribution of victim categories over the entire reporting period



Cyberattack methods

The Iran-Israel conflict altered cyberattack trends, making DDoS attacks the most prevalent threat, accounting for 42% of successful attacks. These attacks are a common tactic among hacktivists due to their high visibility, scalability, and impact on public sentiment.

Figure 4. Distribution of cyberattack methods over the analyzed period



Malware (41%) remains one of the most prominent global threats because it is versatile and highly effective at every stage of the kill chain. During the period analyzed, the most common malware types were:

- ransomware (30%);
- remote access trojans/tools (RATs) (27%);
- spyware (19%).

Social engineering (22%) is often used as the initial access vector for malware attacks.

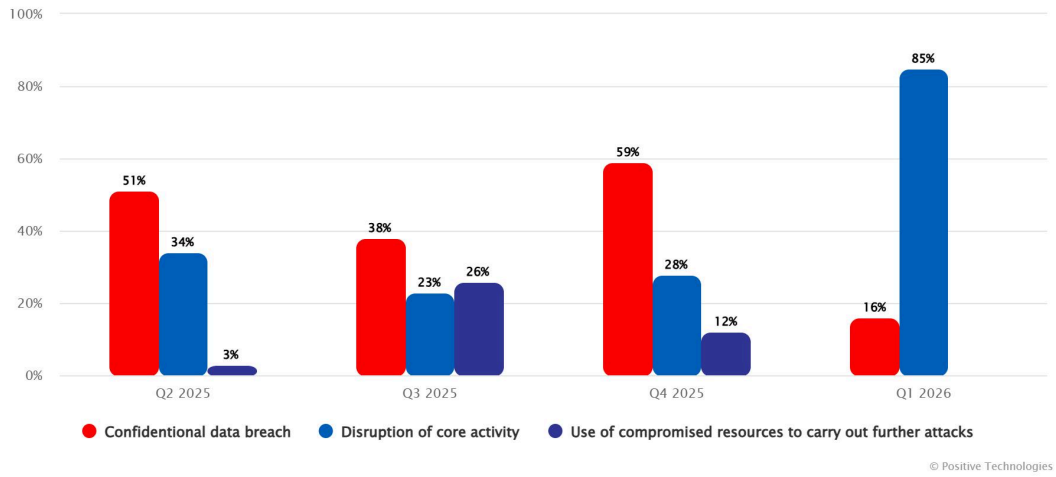
Exploitation of vulnerabilities (21%) remains successful in the region. Despite the Middle East's rapid digitalization, many sectors still rely on legacy security systems, giving attackers opportunities to exploit long-known vulnerabilities in outdated infrastructure. The spread of IoT devices, which are often the weakest point in network security, further expands the attack surface.

Consequences of cyberattacks

The most common consequence of cyberattacks against Middle Eastern organizations during this period was business disruption (60%).

Unsurprisingly, this was largely driven by attacks during active phases of conflict, particularly in Q1 2026. Business disruption incidents increased by 57 percentage points compared with Q4 2025.

Figure 5. Quarterly distribution of cyberattack consequences



Data leaks ranked second (44%), driven partly by aggressive ransomware activity and partly by poor cyberhygiene.

The use of compromised resources to carry out further attacks ranked third (10%), largely because of mass compromises and device infections by large-scale botnets with multinational command-and-control (C2) infrastructure.

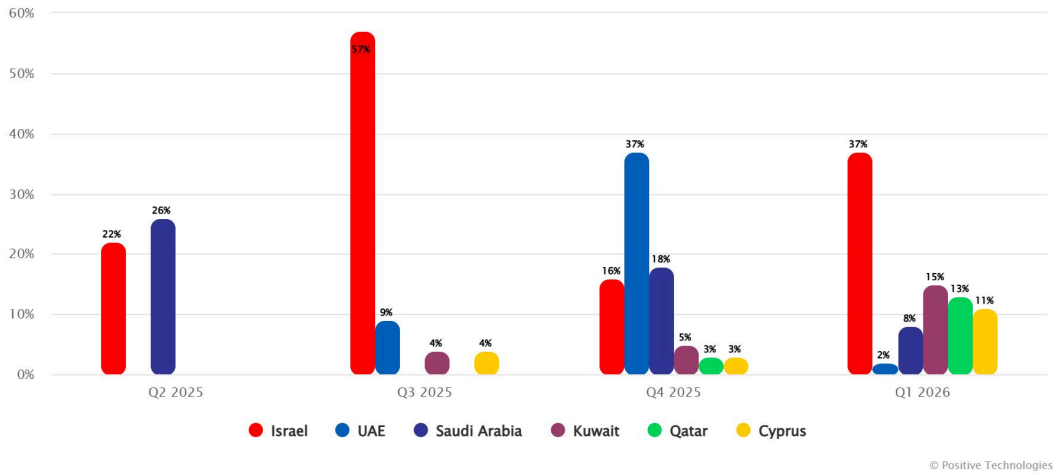
Cyberthreat landscape differs across the most targeted countries.

During the analyzed period, the most frequently targeted countries in the Middle East were:

- Israel (33%);
- Saudi Arabia (12%)ж
- the UAE (11%).

The number of successful attacks on Qatar, Kuwait, and Cyprus only began to approach the leading countries in Q1 2026, driven by escalating regional geopolitics.

Figure 6. Quarterly distribution of targeted countries



The cyber threat landscape varies across countries. The top three most targeted industries over the entire period under review were:

- in Israel: manufacturing and industry (22%), government agencies (16%), and IT and transport, each at 9%;
- in Saudi Arabia: government agencies (35%), manufacturing and industry (20%), retail and service sector companies, each at 10%;
- in the UAE: retail companies (61%), manufacturing and industry (11%), financial organizations, IT companies, and companies in the service sector, each as 6%.

DDoS, malware, and vulnerability exploitation were topped the list for both Israel and Saudi Arabia, though their distribution differed. Due to the conflict, DDoS attacks took center stage in Israel (51%), while malware accounted for 29% and vulnerability exploitation for 27%. In Saudi Arabia, malware-based attacks predominated (55%), followed by vulnerability exploitation (40%), with DDoS and social engineering sharing third place (30% each).

The UAE shows a somewhat unusual pattern in the cyberattack methods. In more than half of cases (56%), attackers managed to compromise supply chains or trusted communication channels. This choice may be linked to the high level of business digitalization in the UAE, where mature companies typically rely on automated internal processes, close integration between suppliers, contractors, partners, and corporate IT systems, and, in some cases, privileged access to IT systems for trusted suppliers and partners. Nevertheless, malware and social engineering were also common due to the activity of ransomware groups, accounting for 44% and 28% of attacks, respectively.

In Iran (considered as a key player in the conflict) top targeted industries were strategically important financial institutions (38%), media outlets (25%), and organizations in the industrial and telecommunications sectors (13% each). This pattern is characteristic of an escalating geopolitical conflict, marked by a concentration of attacks on critical infrastructure and media organizations.

Regional forecast and recommendation

It is anticipated that, **as the conflict de-escalates**, malicious actors will focus their attention on key sectors of each country's economy:

- IT in Israel;
- manufacturing and services in Saudi Arabia;
- retail, services, and manufacturing in the UAE.

Facilities in emerging sectors such as energy infrastructure and sovereign AI infrastructure are also under threat. For attacks on individuals, the use of generative AI will likely increase.

If the conflict escalates, the number of sophisticated attacks on critical infrastructure and satellite systems is expected to rise.

Regardless of how the conflict unfolds, cybersecurity strategies must address both global trends and regional specifics:

1. Protect critical information infrastructure (CII). Focus on assets vital to national security, public safety, and the economy. These require continuous threat monitoring and proactive defense, such as SIEM solutions.
2. To protect critical and industrial infrastructure, organizations must secure their network perimeters and strictly filter primary malware delivery vectors, most notably corporate email.
3. Given the region's rapid digital transformation, threat prevention must begin at the software development stage. Application security testing (AST) tools, like static code analysis, help detect vulnerabilities before deployment. Meanwhile, dynamic analysis ensures any remaining flaws are fixed during testing and delivery.
4. Deploy early-detection systems for OT networks. Solutions based on industrial protocol network traffic analysis (NTA) can drastically enhance the defense of critical facilities, which is especially vital given the high degree of industrial digitalization in the region.
5. Countering AI-driven threats. The escalating use of GenAI in cyberattacks necessitates the development of deepfake detection tools and updated security awareness training for the general public.
6. Adopt zero-trust architectures in industrial environments. The digitalization of industrial infrastructure has vastly expanded the attack surface, requiring a shift toward zero-trust architectures and solutions for protecting CII. A technical challenge is integrating modern security tools with legacy systems and the existing OT environments. To address this, organizations should conduct regular cybersecurity exercises with qualified specialists to identify and mitigate common threats.

Current cyberthreats in the Middle East

Learn more about Positive Technologies researches