StormWall

stormwall.network
sales@stormwall.network
+44 20 3695 6722

DDoS Attacks in MENA in Q2 2025

a StormWall Report

StormWall

stormwall.network sales@stormwall.network

+44 20 3695 6722

In terms of DDoS attacks, the second quarter of 2025 was a record breaker for the MENA region, with traffic volumes far exceeding previous maximums.

StormWall operates dedicated scrubbing centers in the Middle East, and our network has over 5 Tbit/s of combined filtering capacity. Processing attack traffic daily allows us to track trends in the MENA DDoS threat landscape.

The following analysis examines the attack patterns and changes observed in MENA during Q2 of 2025.

The Big Picture

In the second quarter of 2025, DDoS attacks in MENA increased by 236% year-over-year, marking an absolute record. The geopolitical situation in the Middle East escalated significantly with two serious conflicts: Israel-Palestine and Iran-Israel. The Iran-Israel conflict caused a sharp spike in DDoS attacks in both nations, while extortion and blackmail attacks were also detected targeting companies in the UAE and Saudi Arabia.

- Geopolitical tensions were the primary driver of attack activity.
- The majority of attacks were concentrated in Saudi Arabia, Israel, and Iran.
- In the Middle East and North Africa region, hackers heavily targeted finance, the public sector and telecommunications industries.
- Attacks targeting APIs carried over the HTTP/HTTPS protocol increased by 162% year over year.
- Hackers adopted a new attack method—probing. The number of probing attacks increased by nine times. Hackers are using low-volume DDoS to find weak points.

Let's break down these trends in more detail:

DDoS attacks up 236% year-over-year

In the second quarter of 2025, StormWall recorded unprecedented DDoS activity in the MENA region. Attacks targeting the public sector increased by 53% in Q2 of 2025, while attacks on financial services increased by 26%. Most campaigns tracked by StormWall analysts were politically motivated.

About 73% of malicious traffic in MENA in Q2 2025 could be attributed to hacktivists, while the remaining 27%—to for profit hackers and extortionists.

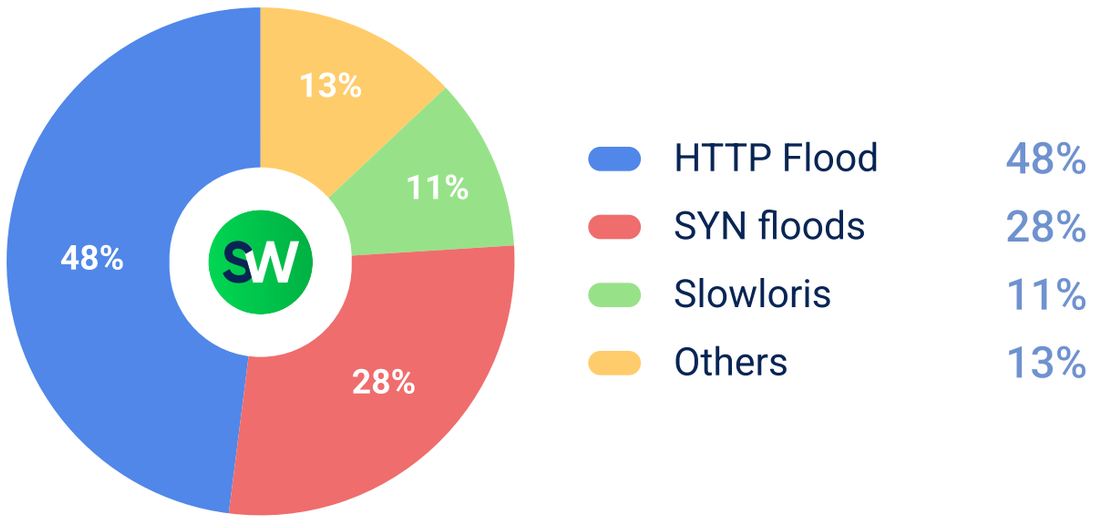
API Attacks Up 162%

Attacks targeting APIs jumped 162% in Q2 of 2025. These attacks are particularly challenging to defend against because they can mimic legitimate traffic patterns, making detection and mitigation more complex.

Attackers botnets to target API endpoints, with over 80% of API attacks involving hacked device networks. The average botnet size tracked in the region has grown to about 140,000 devices. Traditional DDoS methods send a lot of traffic to websites, but API attacks take advantage of the way APIs work to cause problems in important systems.

On average, an API attack generated 4.7 Gbps of traffic, which is much lower than the traffic generated by traditional volumetric campaigns. However, in API attacks, a target can be brought down using only 12% of the traffic volume needed for a generic flood.

Most Common API Attack Methods in **MENA Q2 2025:**

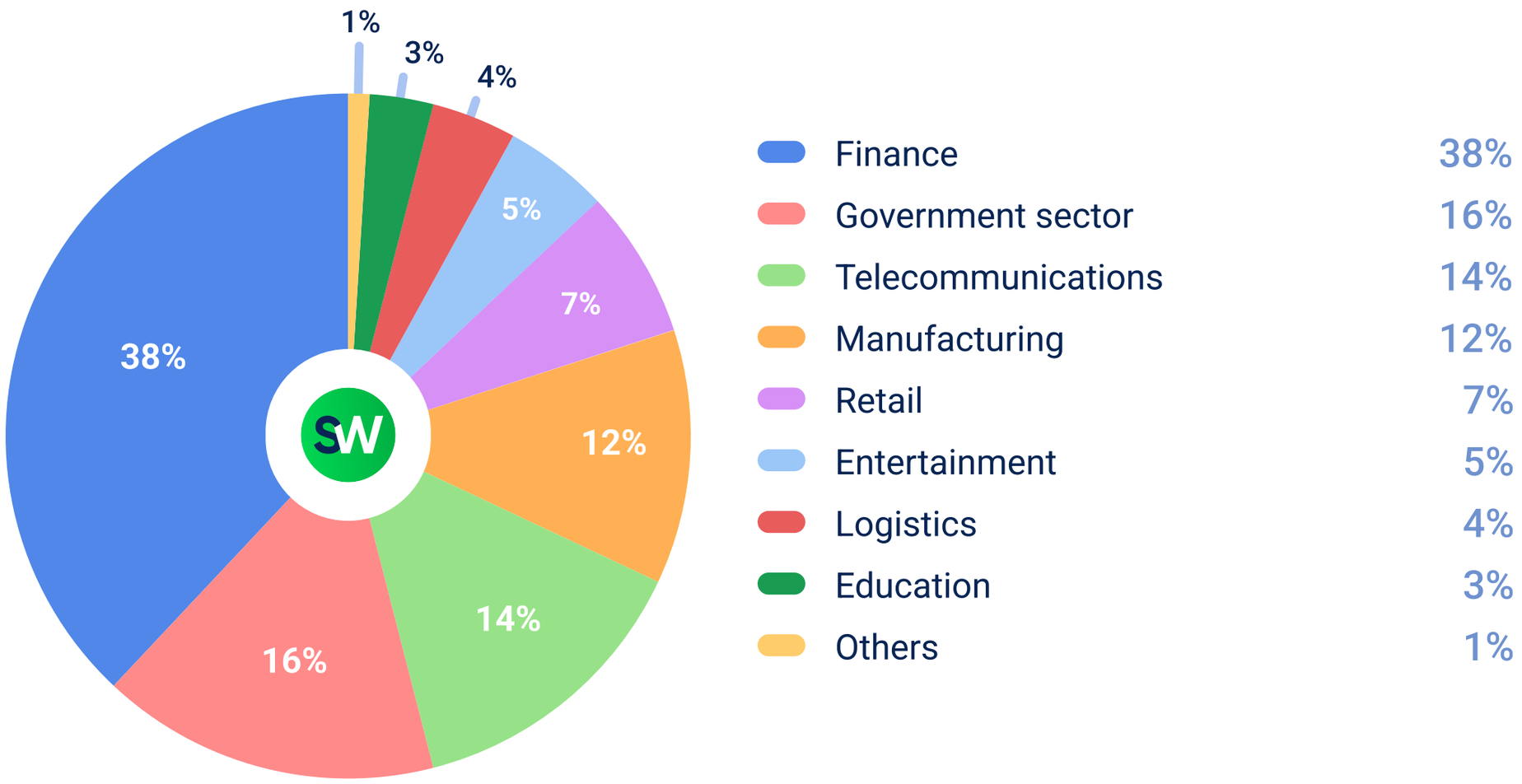


Probing Attacks Emerge as New Threat Vector

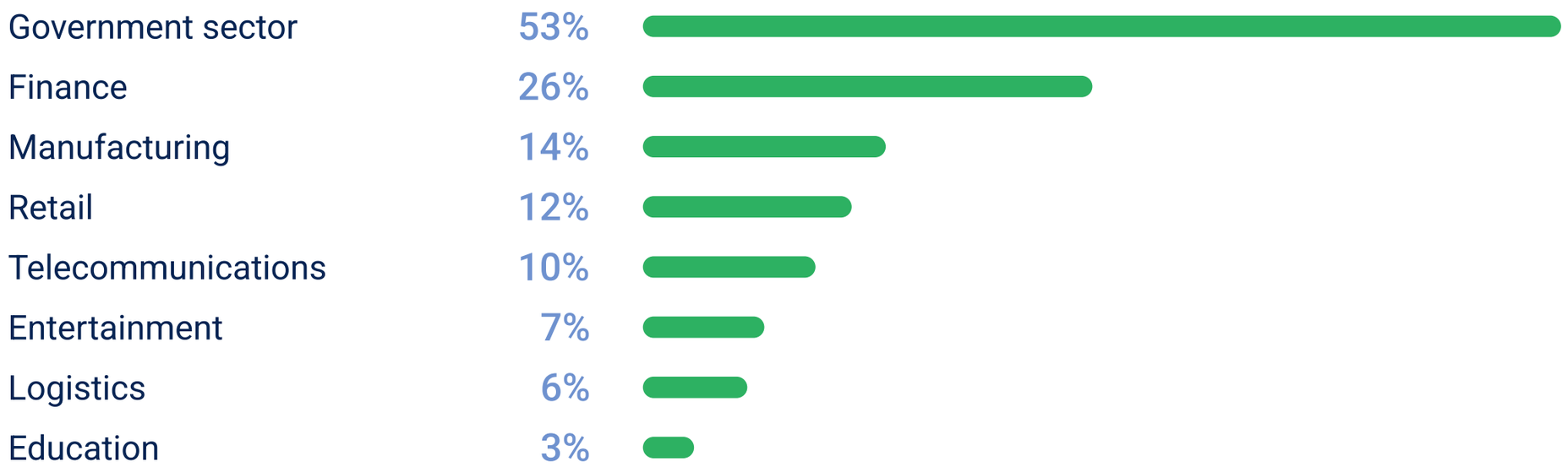
Probing attacks increased by nine times in the second quarter of 2025. This shows a big change in how attackers prepare for DDoS campaigns. Probs are now used extensively to find open ports, services, and weak spots before launching attacks.

Attacks **by Industry**

Now, let's break down the distribution of DDoS attacks by industry in MENA in Q2 2025:



Industries with highest YoY growth in DDoS attacks in MENA in Q2 2025:



- Finance was the biggest target—it increased from 21% of total attacks in Q1 to 38% in Q2.
- In the second quarter of 2025, the government sector accounted for 16% of all DDoS attacks in the MENA region. This is up from 14% in the first quarter of 2025.
- In Q1, 36% of cyberattacks targeted retail. In Q2, that number dropped to 7%, which is an 81% decrease of the relative attack share.
- Telecommunications was the third most targeted sector at 14%.
- Manufacturing saw the biggest QoQ increase, going from 4% to 12% and growing 137%.

Who Is at Most Risk for a DDoS Attack?

What vertical is most likely to be attacked and what vertical is least likely to be attacked? The table below shows the relative likelihood by sector:

Industry	Chance of Being Attacked
Finance	1 in 30
Government	1 in 60
Telecommunications	1 in 70
Manufacturing	1 in 80
Retail	1 in 140
Entertainment	1 in 200
Logistics	1 in 250
Education	1 in 330
Healthcare	1 in 670
Others	1 in 1 000

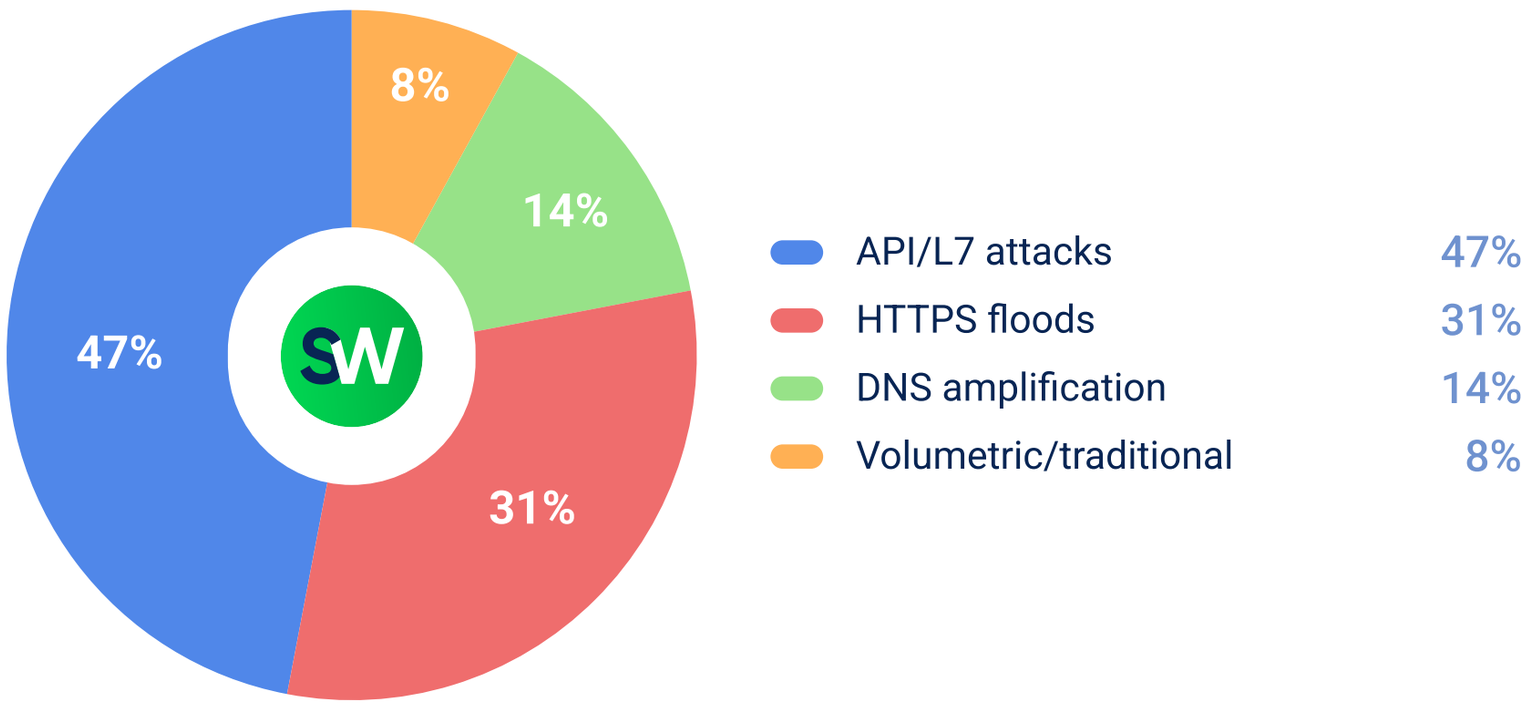
Note: this is a relative risk within the MENA region and only based on the observed distribution of attacks. Real-world risk also depends on exposure surface, security posture and threat actor interest.

Top 3 Most Attacked Verticals

Finance

Attack Share	YoY Growth
38%	26%

Financial services became the most attacked vertical in MENA in Q2 2025. Around 79% of cyberattacks were aimed at banking APIs and payment processing systems.



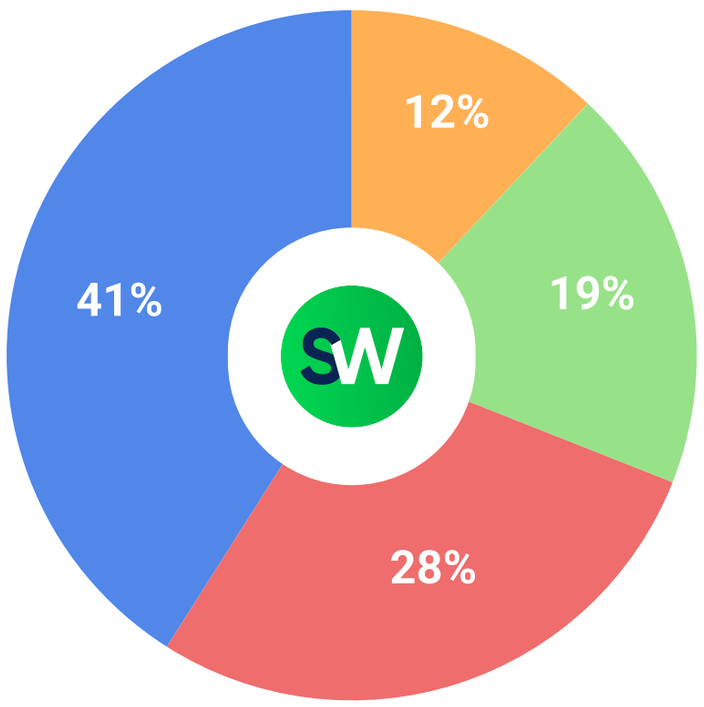
The biggest attack on the financial sector was 1.8 Tbit/s and targeted a bank in the UAE. The longest attack lasted six days and was about 380 Gbps. On average, the attacks lasted 14 minutes.

Government

Attack Share	YoY Growth
16%	53%

Government infrastructure was the second most attacked industry in Q2 2025 as the conflict between Iran and Israel led to a new level of targeting of state infrastructure: within the vertical, around 68% of the attacks were aimed at national government websites.

When it comes to most popular attack vectors, carpet bombing was by far the most used.

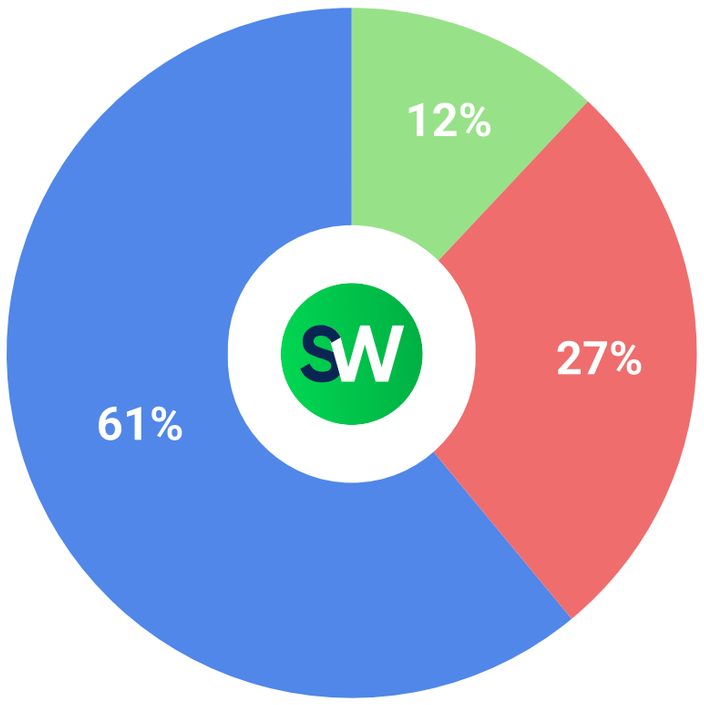


Carpet bombing	41%
Direct path attacks (L3/L4)	28%
API/L7 attacks	19%
DNS amplification	12%

Telecommunications

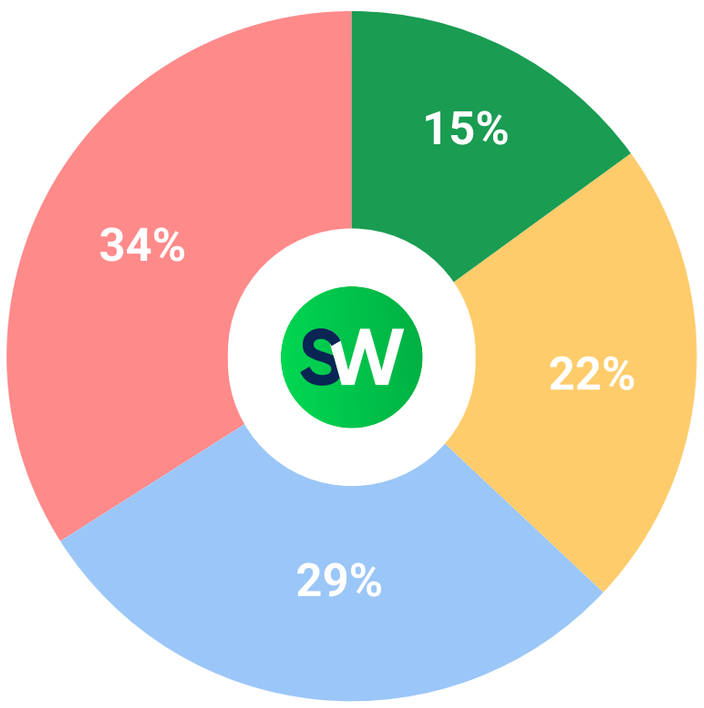
Attack Share	YoY Growth
14%	10%

In this vertical, mobile network operators were the targets of the most attacks:



Mobile network operators	61 %
ISPs & broadband providers	27 %
VoIP & messaging services	12 %

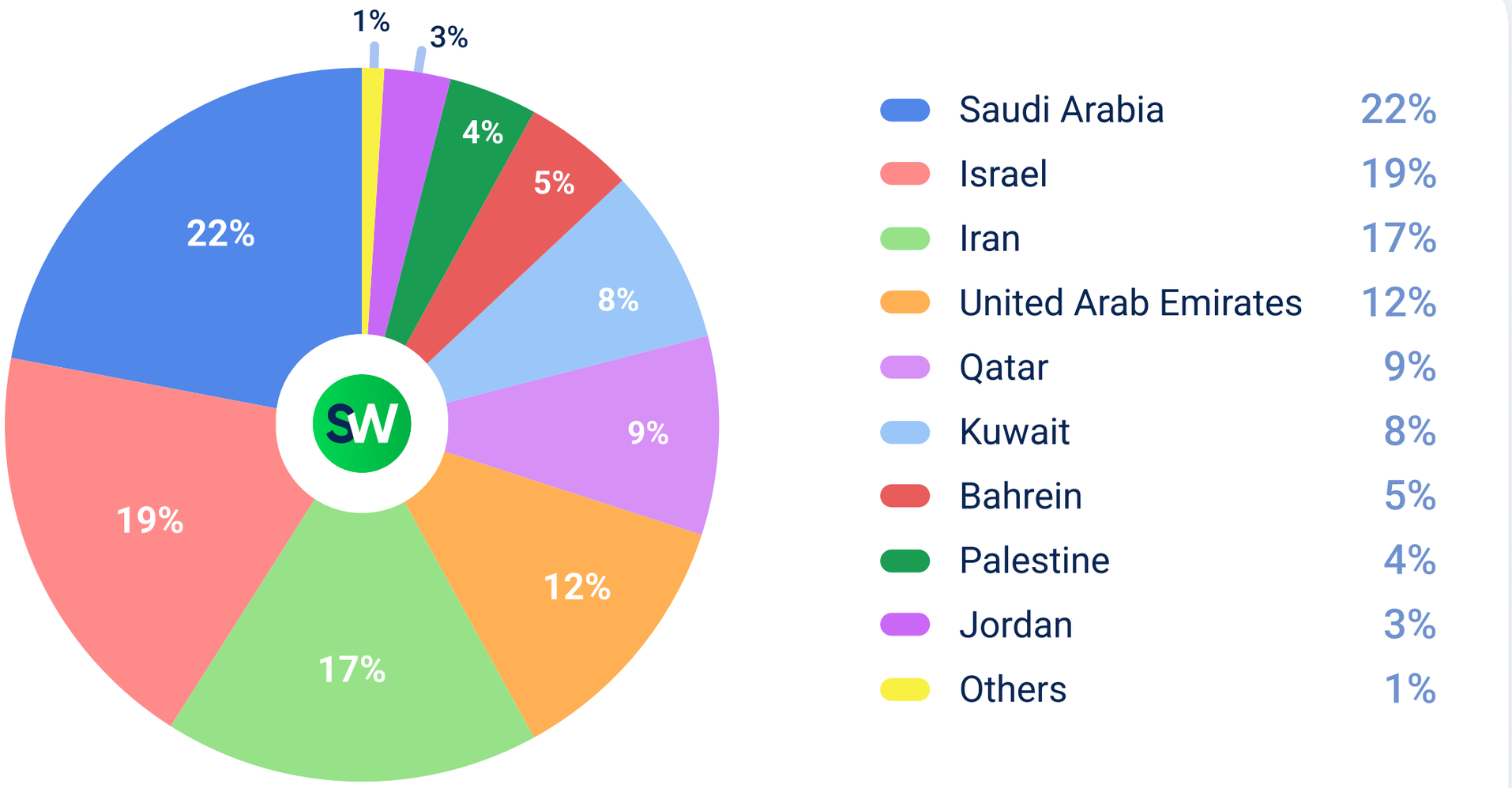
Multi-vector amplification attacks were the most common type of cyberattack on telecommunications, taking advantage of the sector's critical role in regional communications:



Multi-vector amplification	34%
DNS amplification	29%
API attacks	22%
Traditional floods	15%

DDoS Attacks by Country

Let’s break down how DDoS attacks were distributed by country in Q2 2025:



Saudi Arabia is the most targeted country, but its share dropped from 28% in Q1 2025 to 22%. Iran's share stayed about the same, going up a bit from 16% to 17%.

A pro-Israel hacking group executed a devastating attack on Iran's largest cryptocurrency exchange, Nobitex, on June 18, 2025, destroying over $90 million in digital assets across multiple cryptocurrencies including Bitcoin, Ethereum, and Dogecoin. The attackers transferred the stolen funds to "vanity addresses" containing anti-IRGC messages, effectively burning the money rather than stealing it for profit, making this a politically motivated destructive attack.

The same group also claimed responsibility for an attack on Iran's state-owned Bank Sepah on June 17, 2025, allegedly destroying IRGC data and causing widespread ATM outages across the country.

Israel's targeting share increased by 73% since the first quarter of 2025, growing from 11% to 19%, as a result of the conflict between Iran and Israel.

Iran used GPS spoofing to attack Israeli infrastructure. In June 2025, almost 1,000 ships in the Persian Gulf experienced interference to their GPS signals. Iranian operatives also hijacked thousands of Israeli security cameras to gather real-time intelligence and assess missile strike damage. They exploited vulnerabilities in Chinese-made surveillance equipment. Israeli cybersecurity officials warned that around 66,000 personal cameras in Israel were using easy-to-guess passwords and could easily be hacked.

Other important changes from the first quarter of 2025 to the second quarter of 2025 include:

- Palestine: 2% → 4%
- Qatar: 8% → 9%
- Bahrain: 7% → 5%
- Kuwait: 6% → 8%

During the quarter, a total of 8.2 million DDoS attack events targeted Israel's digital infrastructure. This is more than four times the number of attacks seen in the first quarter. Most of these were multivector attacks, accounting for 6.1 million incidents. These included coordinated carpet bombing campaigns, attacks focused on the API, and state-sponsored volumetric floods.

Most incidents lasted less than 8 minutes. The most severe attacks happened during the first two weeks of May, which also happened to be when the military was increasing its activities.

Quick **Highlights**

- DDoS attacks in MENA increased by 236% YoY, marking an absolute record for the region in Q2 2025.
- The escalation was primarily driven by geopolitical tensions from the Israel-Palestine and Iran-Israel conflicts.
- API-layer attacks increased by 162% YoY.
- There was a 9× increase in probing attacks.
- Finance became the primary target (38%), experiencing 26% YoY growth in attacks. Government sector (16%) and telecommunications (14%) followed.
- Saudi Arabia (22%), Israel (19%), and Iran (17%) were the most targeted countries.
- The largest attack recorded was 1.8 Tbit/s against a UAE bank.

Hacktivists now account for 73% of MENA's attack traffic, with a ninefold increase in probing showing how tactics have evolved. Instead of launching immediate brute-force attacks, attackers first scan for weaknesses. Then, they exploit them with targeted API attacks. These API attacks need 88% less traffic to cause the same damage. This change from using a lot of spray attacks to targeting specific weak points may catch you off guard if your defenses are built for yesterday's threats.