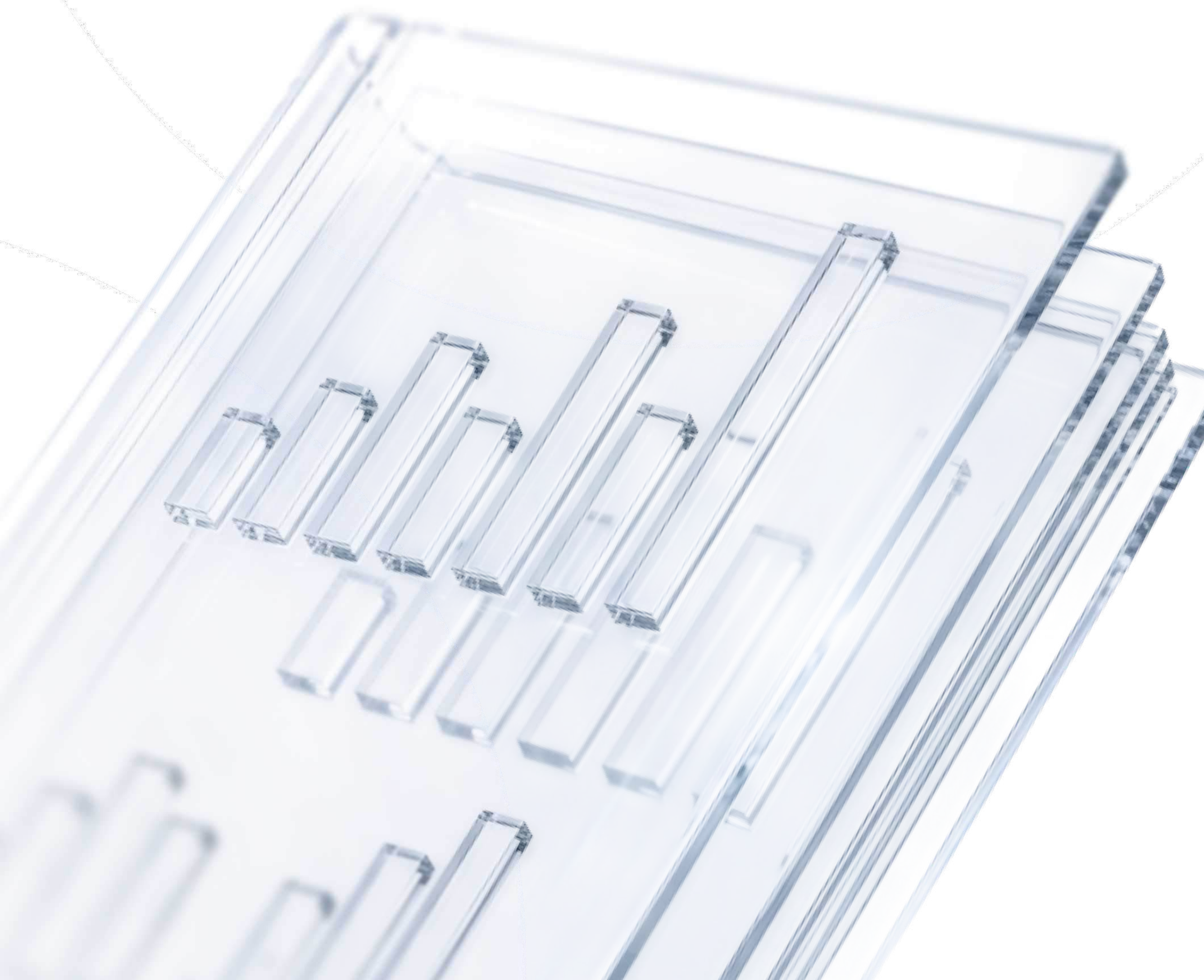
StormWall

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

The State of DDoS Attacks in APAC

in Q2 2026, a StormWall Report



StormWall

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

This report looks at the DDoS attacks StormWall mitigated for its APAC customers between April and June 2026. StormWall is a cybersecurity provider operating dedicated scrubbing centers across Asia Pacific, the US, Europe, and the Middle East, including a facility in Singapore. Our network has more than 8 Tbit/s of filtering capacity, and the volume of attack traffic we process daily gives us a close view of how DDoS activity in the region is evolving.

Key Takeaways

StormWall mitigated **1.72 million DDoS attacks in APAC in Q2 2026,** up 83% year over year.

Commercially motivated attacks — where attackers sought financial gain or an unfair competitive advantage — accounted for 76% of observed activity in APAC. The remaining attacks were attributed to hacktivism, which, while still significant, no longer defined the region's baseline threat activity.

This contrasts somewhat with StormWall's global findings, where more than 70% of attacks observed in Q2 were attributed to hacktivist groups.

With that context, the following trends defined DDoS activity in APAC in Q2 2026:

- Telecommunications was the most attacked industry, with 26% of all attacks, followed by entertainment at 19% and the government sector at 16%.
- The average power of Layer 7 attacks increased 2.5× compared with Q1 2026.
- AI-assisted attacks increased 32% year over year.
- Multi-vector attacks increased 62% year over year.
- The average number of devices used in a botnet attack grew 4×, from 15,000 to 60,000.
- China (21%), India (20%), and Indonesia (13%) were the most attacked countries in APAC.
- South Korea and Australia experienced notable hacktivist and botnet-driven disruptions during the quarter.

Let's break down these trends in more detail.

DDoS Attacks Up 83% YoY

StormWall mitigated 1.72 million DDoS attacks against its APAC customers in Q2 2026, an increase of 83% year over year.

Commercial campaigns were the dominant source of DDoS activity in APAC during the quarter:

Attack motivation	Share	Main pattern
Commercial	76%	Service disruption and financial pressure
Hacktivist	24%	Activity tied to geopolitical events

This distribution contrasts with what StormWall observed globally in Q2 2026, when more than 70% of attacks were attributed to hacktivist groups, largely in connection with the Russia–Ukraine war and conflicts in the Middle East. This difference had a direct impact on the techniques used and the types of attacks observed — but more on that later.

Top 3 Most **Attacked Industries**

Telecommunications was the most attacked industry in APAC in Q2 2026, accounting for 26% of all DDoS attacks, followed by Entertainment (19%), and the government sector (16)%.

Vertical	Attack Share	YoY Growth
Telecommunications	26%	108%
Entertainment	19%	84%
Government sector	16%	28%

Notably, in absolute terms, the volume of attacks targeting the telecommunications industry more than doubled year over year.

Layer 7 Attacks Power **Up 2.5× QoQ**

The average power of application-layer attacks increased 2.5× compared with Q1 2026. These attacks target websites, applications, login flows, and APIs.

Layer 7 attacks do not need to saturate an organization's internet connection to cause an outage. They can exhaust application resources, database connections, or expensive API operations while generating less obvious traffic.

Globally, Layer 7 attack volume increased 82% year over year, with attackers making greater use of automation and residential proxy networks.

For APAC organizations, network capacity alone is therefore becoming a weaker proxy for resilience. Protection needs to distinguish abusive application behavior from legitimate customer traffic, especially around high-traffic APIs and business-critical transactions.

AI-Assisted Attacks **Up 32% YoY**

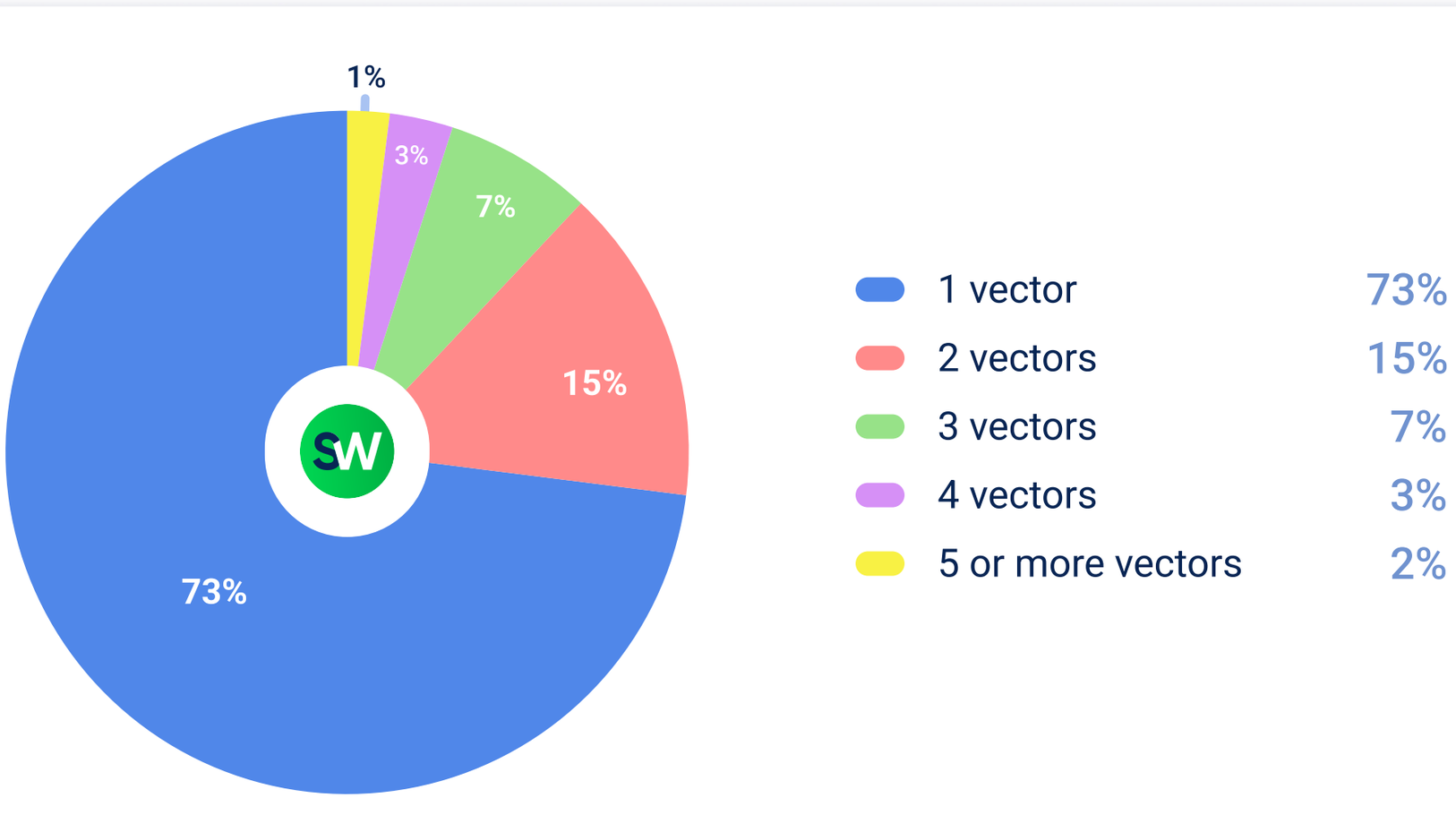
The number of attacks involving AI increased 32% compared with Q2 2025. AI tools can lower the effort required to identify targets, automate attack preparation, adapt request patterns, and coordinate changes between vectors.

Globally, according to StormWall's telemetry, AI-assisted attacks already account for about 34% of DDoS incidents, up from 22% in Q1 2026. Mentions of malicious AI tools on dark-web channels also increased 219% year over year.

Multi-Vector Attacks **Up 62% YoY**

Multi-vector attacks — where attackers combine two or more methods in a single campaign — increased by 62% year over year in APAC.

The distribution by number of vectors was as follows:



This puts the total multi-vector share at 27%. Most combined attacks used two vectors, but around 12% of all attacks used three or more.

Botnet Size **Increased by 4×**

The average number of devices involved in botnet attacks against StormWall's APAC customers increased from 15,000 in Q2 2025 to 60,000 in Q2 2026 — a fourfold increase.

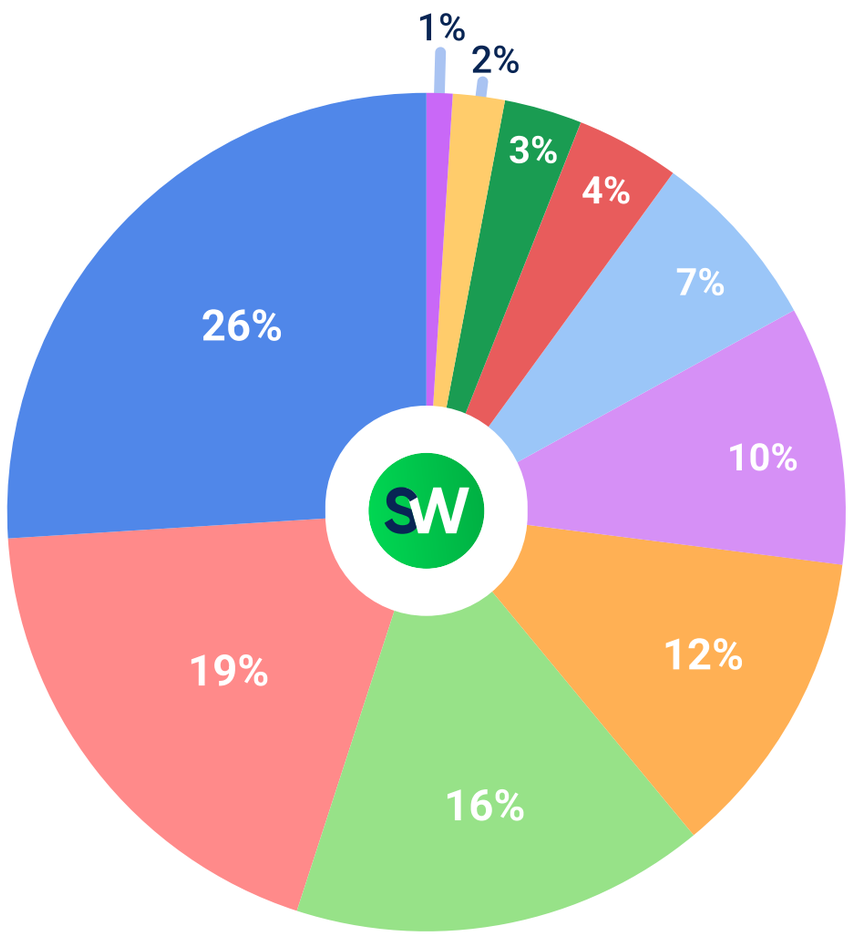
Period	Average devices per botnet attack
Q2 2025	15,000
Q2 2026	60,000

The March 2026 disruption of the Aisuru, Kimwolf, JackSkid, and Mossad botnets did not produce a sustained decline in attack volumes. StormWall observed attackers shifting to other infrastructure, including Masjesu, xlabs_v1, more than 116 active Mirai-derived variants, and RapperBot.

APAC remains central to this trend because the region contains large pools of consumer routers, cameras, Android TV boxes, and other devices that are exposed to automated exploitation. In the first half of 2026, Singapore, China, and Indonesia were among the world's leading sources of DDoS traffic. The result is a resilient supply chain for DDoS-for-hire services: removing one botnet can interrupt its operators, but vulnerable devices are rapidly recruited into replacements.

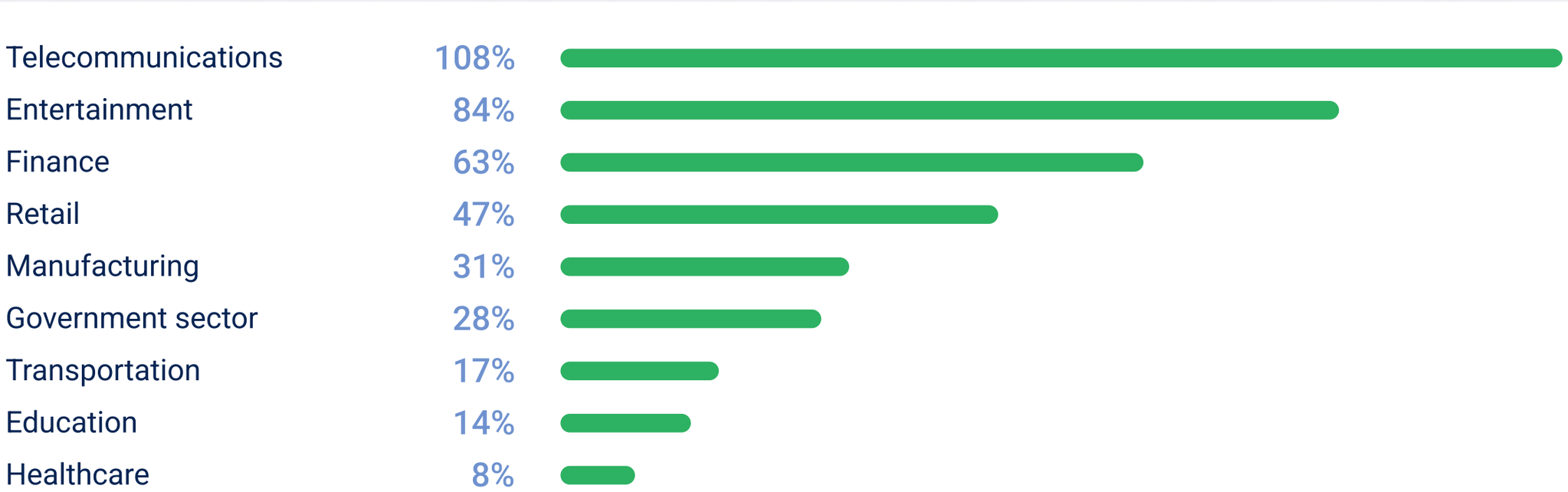
DDoS Attacks by Vertical

Here is the distribution of DDoS attacks by industry among StormWall's APAC customers in Q2 2026:



Telecommunications	26%
Entertainment	19%
Government sector	16%
Finance	12%
Retail	10%
Manufacturing	7%
Transportation	4%
Education	3%
Healthcare	2%
Others	1%

Industries with the highest year-over-year growth in DDoS attacks in Q2 2026:



Compared with our data from the end of 2025, the distribution of attacks across industries has shifted considerably, with a clear change in which sectors are being targeted most heavily:

- Telecommunications: 18% in 2025 → 26% ^
- Entertainment: 10% → 19% ^
- Government sector: 27% → 16% v
- Finance: 8% → 12% ^
- Retail: 14% → 10% v
- Manufacturing: 3% → 7% ^

As is evident from the data, the telecommunications and entertainment sectors together accounted for 45% of attacks in Q2. The increase in attacks targeting financial services is also notable, as is the relative decline in attacks targeting government services. Taken together, these shifts point to a threat landscape increasingly dominated by commercially motivated attacks.

Who Is at Most Risk for a DDoS Attack?

The table below shows the relative likelihood of an organization being attacked across different sectors in APAC:

Industry	Chance of Being Attacked
Telecommunications	About 1 in 4
Entertainment	About 1 in 5
Government sector	About 1 in 6
Finance	About 1 in 8
Retail	1 in 10
Manufacturing	About 1 in 14
Transportation	1 in 25
Education	About 1 in 33
Healthcare	1 in 50
Others	1 in 100

Note: this is relative risk based on the observed distribution of attacks in StormWall's customer base. Real-world risk also depends on an organization's public exposure, security posture, business model, geography, and threat actor interest.

In Detail: Top 3 Most Attacked Verticals

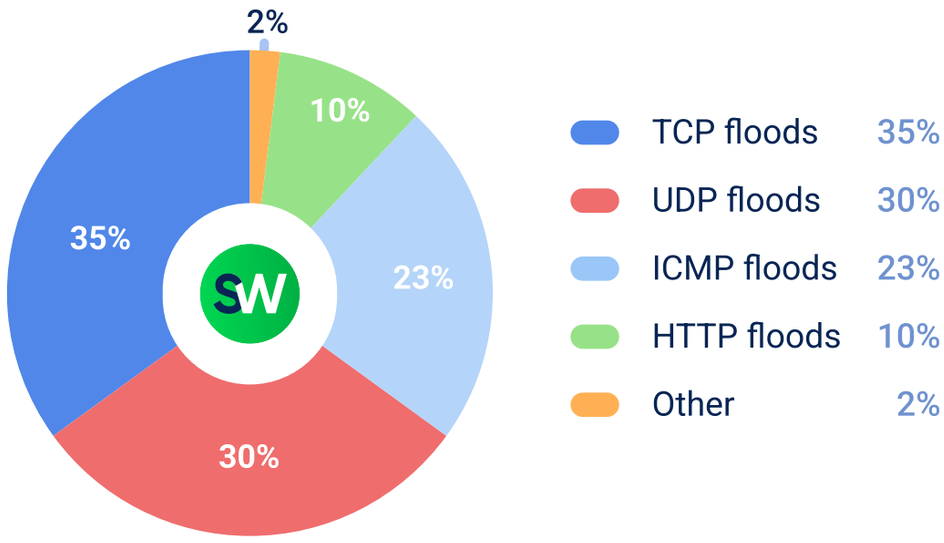
Telecommunications

Attack Share	YoY Growth
26%	108%

Telecommunications accounted for more than one in four attacks in APAC and was the only vertical where attack volume more than doubled year over year.

StormWall's telemetry also found that telecommunications had the highest share of botnet-driven attacks of any industry. More than 86% of the attack mix consisted of TCP, UDP, and ICMP floods, and average attack bandwidth was five times higher than a year earlier.

The most used attack vectors in this vertical were as follows:



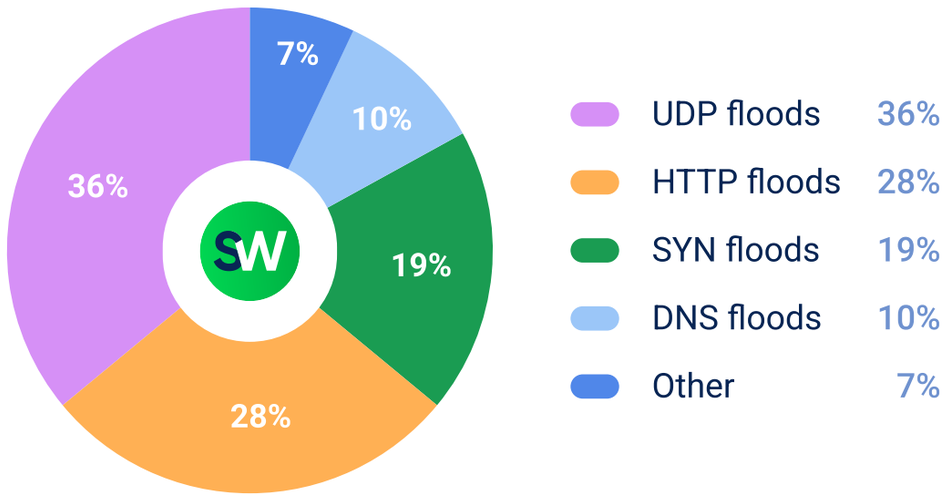
Entertainment

Attack Share	YoY Growth
19%	84%

Entertainment was the second most attacked industry in Q2 2026, accounting for almost one in five attacks.

StormWall's data also showed average attack bandwidth against entertainment companies increasing 2.5×, indicating that attackers are placing more pressure on services where downtime quickly affects revenue and customer retention.

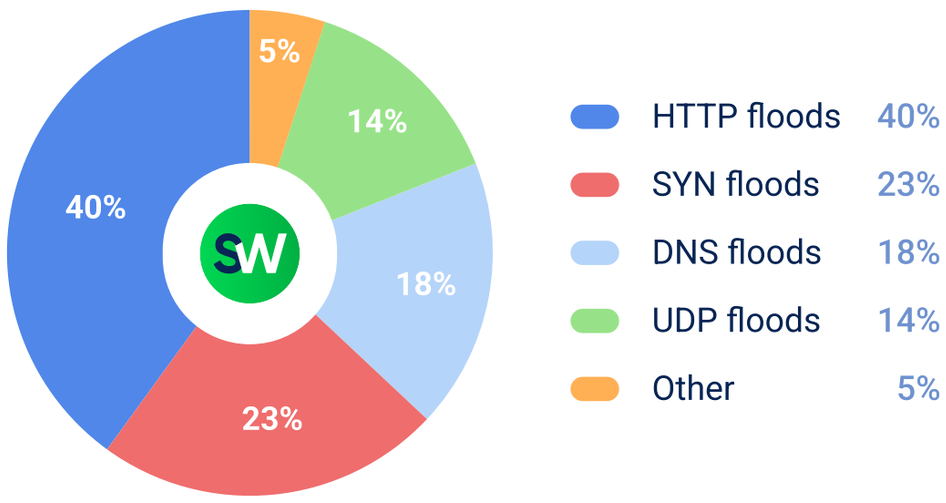
UDP floods remained the largest individual vector, particularly against gaming and other real-time services:



Government Sector

Attack Share	YoY Growth
16%	28%

When 2025 closed, the government sector was the most attacked vertical in APAC by far. This has since changed — and while the absolute volume of attacks is growing, relatively speaking, the share of attacks on the government vertical is decreasing as the attacker provider is changing from a potlically motivated one to a commercially motivated one.

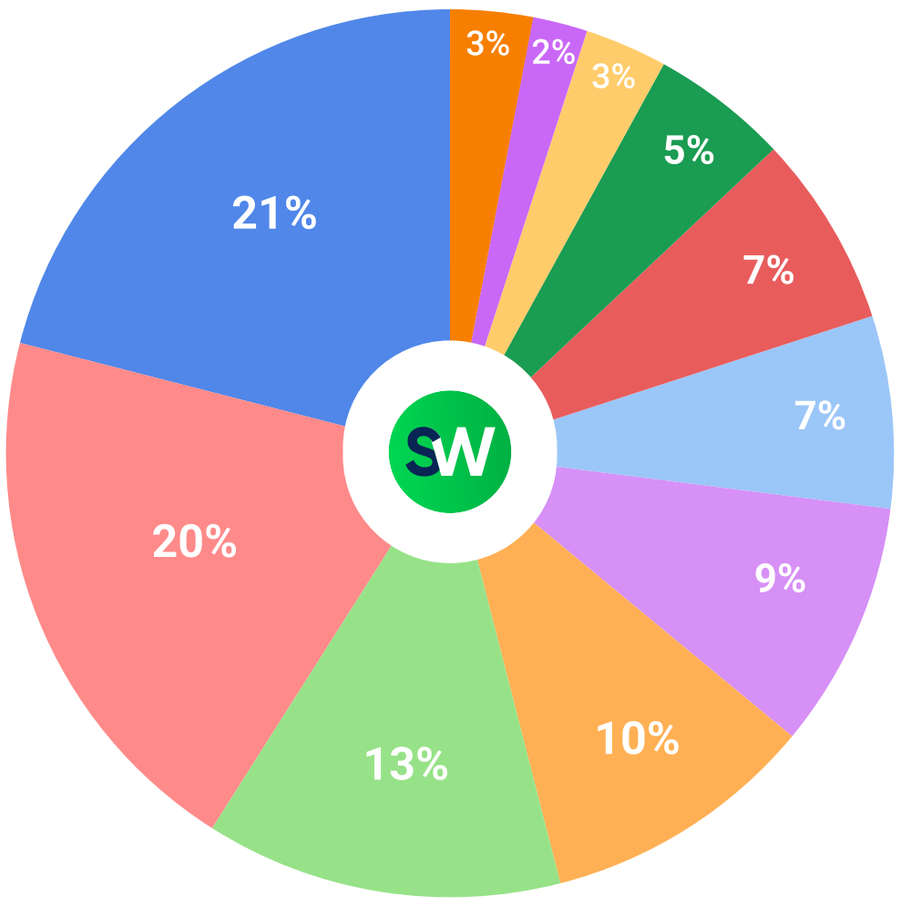


Government services remain a key target for politically motivated groups active across APAC. In South Korea, for example, hacktivist groups targeted the Ministry of Foreign Affairs, the Ministry of Trade, Industry and Energy, Korea Land & Housing Corporation, and Korea Hydro & Nuclear Power in April. The Ministry of Foreign Affairs website was briefly taken offline as a result.

In terms of the most commonly used attack vectors, they were as follows:

DDoS Attacks **by Country**

Here is the distribution of DDoS attacks by country in APAC in Q2 2026:



China	21%
India	20%
Indonesia	13%
Malaysia	10%
South Korea	9%
Singapore	7%
Hong Kong	7%
Australia	5%
Japan	3%
Taiwan	2%
Others	3%

Compared to Q1 2026:

- China: 19% → 21% ^
- India: 18% → 20% ^
- Indonesia: 12% → 13% ^
- Malaysia: 9% → 10% ^
- South Korea: 6% → 9% ^
- Singapore: 10% → 7% v
- Hong Kong: 8% → 7% v
- Australia: 4% → 5% ^
- Japan: 6% → 3% v
- Taiwan: 3% → 2% v
- Others: 5% → 3% v

China and India together accounted for 41% of the attacks observed in APAC, up from 37% in Q1. South Korea's share increased from 6% to 9% amid a wave of attacks by international hacktivist groups against government institutions and companies in April.

The shares attributed to Singapore and Hong Kong decreased, although this does not necessarily indicate a reduction in the number of attacks affecting organizations in either market: the total volume of DDoS attacks across APAC remained substantially higher than a year earlier. Network-layer telemetry also showed that Hong Kong continued to absorb an unusually high concentration of malicious traffic, accounting for over 40% of observed attack bytes in Q2, compared with ~19% in Q1, indicating sustained pressure on infrastructure serving the market.

Quick Summary

- StormWall mitigated 1.72 million DDoS attacks against its APAC customers in Q2 2026, up 83% year over year.
- Commercially motivated campaigns accounted for 76% of activity.
- Telecommunications (26%), entertainment (19%), and the government sector (16%) were the three most attacked industries.
- Telecommunications attacks increased 108% year over year, the fastest growth of any vertical.
- The average power of Layer 7 attacks increased 2.5× compared with Q1 2026.
- AI-assisted attacks increased 32% year over year, while multi-vector attacks increased 62%.
- The average number of devices used in a botnet attack increased from 15,000 to 60,000.
- China (21%), India (20%), and Indonesia (13%) were the most attacked countries in APAC.
- The March botnet takedowns did not reduce attack volumes for long as attackers shifted to replacement infrastructure.

The second quarter in APAC was characterized by a growing volume of commercially motivated attacks, punctuated by intermittent bursts of hacktivist activity around major geopolitical events. At the same time, larger botnets and AI-assisted services that provide access to them are making both types of attacks more powerful and sophisticated.

The result is a threat environment in which quieter political periods do not necessarily translate into fewer attacks, while defenders must contend with simultaneous shifts in motive, attack vector, and scale.

StormWall recommends that organizations across APAC adopt modern DDoS protection capable of defending against the full range of today’s DDoS threats.