StormWall

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

The State of DDoS Attacks in **APAC in Q1 2025**

a StormWall Report

StormWall

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

Welcome to StormWall's report covering DDoS attacks in the APAC region. We'll examine the primary attack patterns and attack sources identified by our security experts in the Asia-Pacific during the first quarter of 2025.

At StormWall, we specialize in safeguarding businesses against DDoS attacks. Our network of scrubbing centers in the APAC region continuously filters malicious traffic, peaking at over 5 Tbps, which provide us with unique insights into the changing DDoS threat landscape across the region.

The Big **Picture**

In Q1 2025, StormWall's data analysis shows three major trends:

1. Attacks on Taiwan and China
2. 96% YoY increase in carpet bombing attacks
3. 74% YoY increase in API attacks

Attacks on **Taiwan and China**

In the past 2–3 years, politically motivated attacks have often overtaken financial crime as the primary cause of DDoS. In APAC, the main driver is the nation-state tensions (China–Taiwan, India–Pakistan, Russia–Japan, etc.).

In Q1 2025, China–Taiwan tensions took center stage—China was the most attacked country (22% relative share), while Taiwan was the third most attacked country (14% relative share).

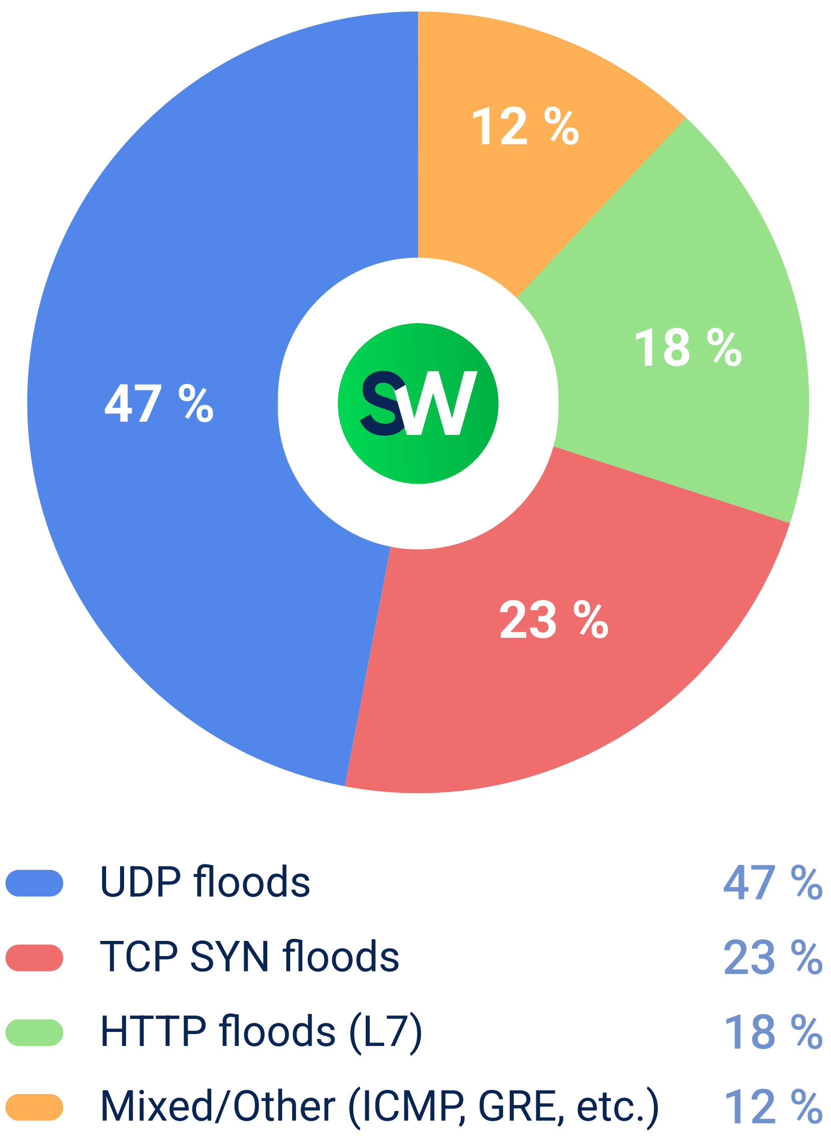
Taiwan's government and critical services have been frequent targets of Chinese "grey-zone" cyber harassment, with some attacks timed to coincide with People's Liberation Army military drills. These often took the form of DDoS assaults against Taiwan's transportation and financial sectors, aimed at intimidating the island.

Carpet Bombing Attacks **up 96% in Q1 2025**

StormWall observed 96% YoY increase in carpet-bomb DDoS campaigns in APAC. This was already a growth that intensified in late 2024, when nearly 30% of all DDoS incidents mitigated by StormWall were multi-destination horizontal attacks, roughly double the proportion seen just two years earlier.

Carpet bombing attacks often combine with multiple vectors, hitting large ranges of IP addresses, and prefixes with varied flood types (UDP, TCP, HTTP, etc.) in quick succession in what's called the "everything, everywhere, all at once" approach.

The breakdown of flood types used in carpet bombing attacks observed in APAC in Q1 2025 is as follows:



Why this matters

In carpet bombing attacks, traffic volumes per IP stay below traditional DDoS thresholds, which makes this technique very stealthy. Legacy DDoS protection tuned for single-destination floods can’t “see” that anything is wrong until edge routers, firewalls, or load balancers start to fail.

API Attacks Surged **by 74%**

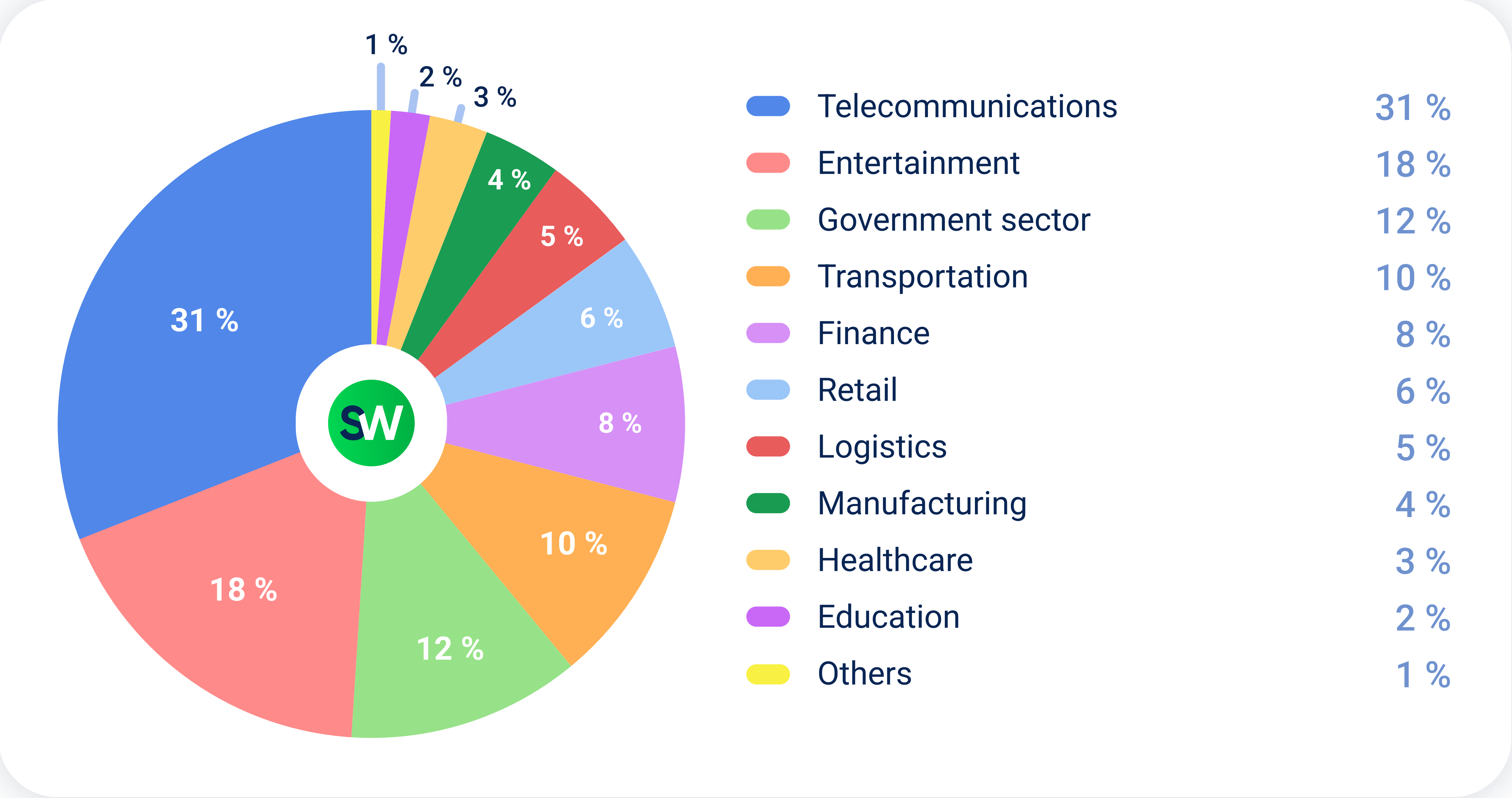
StormWall data showed that in Q1 2025, Layer 7 web DDoS rose 95% and API-centric attacks 74% year-over-year. There was a pronounced spike in application-layer DDoS attacks in APAC during January–February, primarily targeting banks and critical infrastructure.

Why this matters

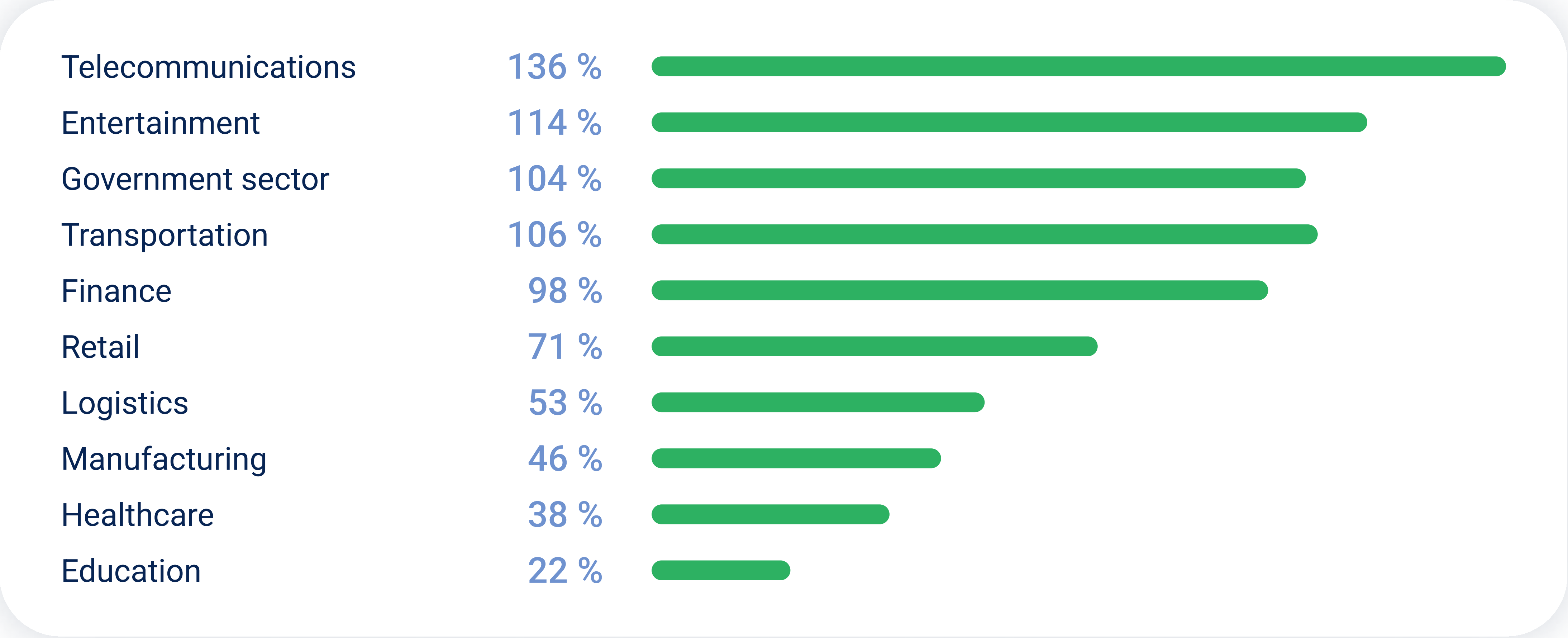
API DDoS attacks mimic legitimate API requests, which makes them harder to detect and block using rate-limiting or IP-based filtering. Attackers often target expensive API endpoints (authentication, search) to exhaust CPU or memory of the backend services, which can crash the entire application.

Attacks **by Industry**

Now, let’s break down the distribution of DDoS attacks by industry in APAC in Q1 2025:



Industries with highest YoY growth in DDoS attacks in APAC in Q1 2025:



Five industries experienced over a twofold or near twofold year-over-year increase in DDoS attacks. It's interesting that attack share roughly halves as you move down after the top few most-targeted industries. Here are other trends worth highlighting:

- In Q1 2025, the telecommunications sector became the most targeted industry for DDoS attacks in APAC, with attack volume nearly doubling compared to the previous quarter—increasing its share from 16% to 31%.
- Attacks on the entertainment sector grew by 29% quarter-over-quarter. Its year-over-year growth reached 114%.
- The government sector recorded a 71% increase in attacks compared to Q4 2024, becoming the third most targeted industry in the region.
- Transportation attacks rose by 67% quarter-over-quarter, with year-over-year growth doubling to 106%.
- In contrast, the finance sector—previously the most targeted—saw its share of attacks fall from 31% to 8%, making it the fifth most targeted industry in Q1 2025. Its year-over-year growth stood at 98%.
- Retail experienced a 50% decrease in attack volume, dropping from 12% to 6% of total attacks. Its year-over-year growth remained relatively strong at 71%.
- Logistics appeared among the most targeted industries, accounting for 5% of attacks and recording year-over-year growth of 53%.

Healthcare and Education stay around 2–3% attack share consistently. These sectors are unlikely to see attack volumes drop below this baseline without a fundamental change in attacker motivations.

Relative Risk of DDoS

Who's at the highest risk of DDoS, and who is least likely to be attacked? The table below shows the relative likelihood by sector:

Industry	Chance of Being Attacked
Telecommunications	1 in 3
Entertainment	~1 in 5.5
Government	1 in 8
Transportation	1 in 10
Finance	1 in 12.5
Retail	1 in 16.6
Logistics	1 in 20
Manufacturing	1 in 25
Healthcare	1 in 33
Education	1 in 50 chance
Others	1 in 100 chance

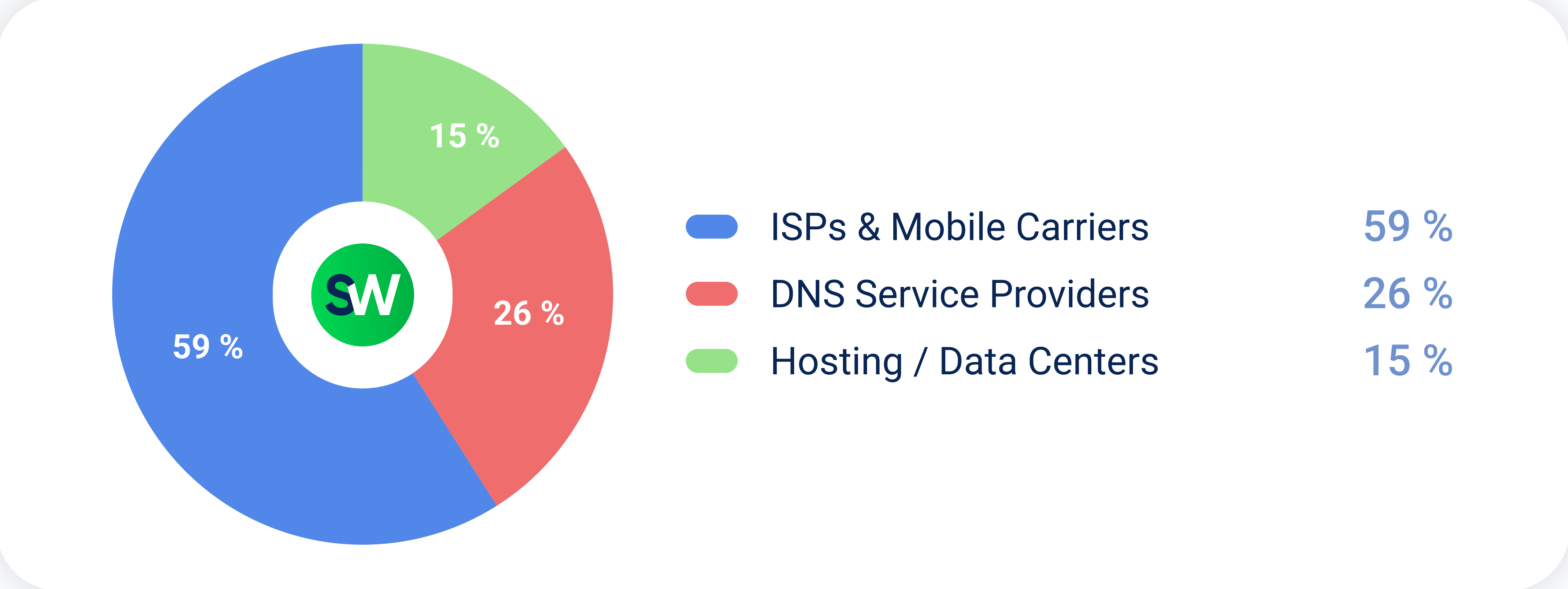
Note: this is a relative risk within the APAC region and only based on the observed distribution of attacks.Real-world risk also depends on exposure surface, security posture and threat actor interest. Let's take a closer look at the most targeted verticals:

Under a Magnifying Glass: Top 3 Most Attacked Verticals

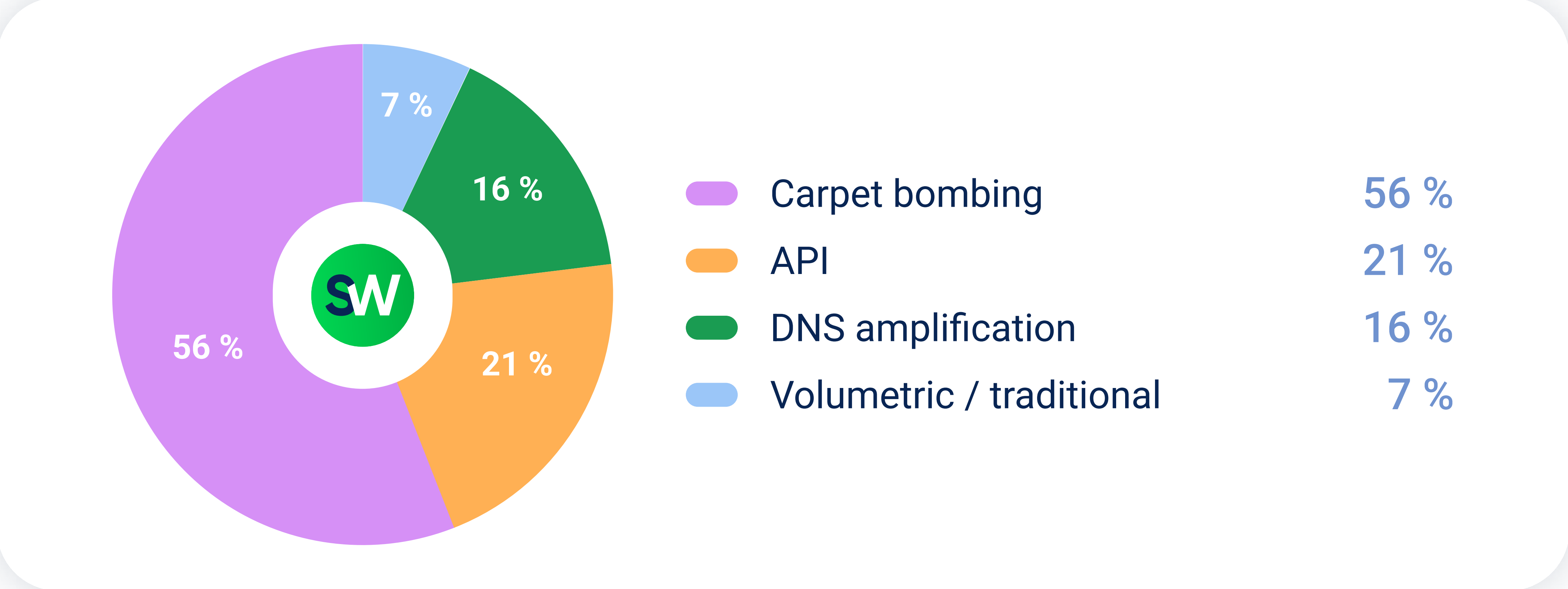
Telecommunications

Attack Share	YoY Growth
31 %	136 %

Telecom networks and DNS servers were hit by a wave of carpet bombing DDoS attacks. The largest share of attacks targeted ISPs and mobile carriers:



In addition to carpet bombing, L7/API attacks were also prevalent, followed by DNS amplification. Volumetric attacks, which are the least sophisticated, were also the least used:



The largest DDoS attack in Q1 2025 mitigated by StormWall, clocking at 2.3 Tbps, was aimed at a data center provider in China. The longest-lasting attack was also telecom-related: it lasted 11 days straight at ~850 Gbps against a telecom service in Taiwan.

Entertainment

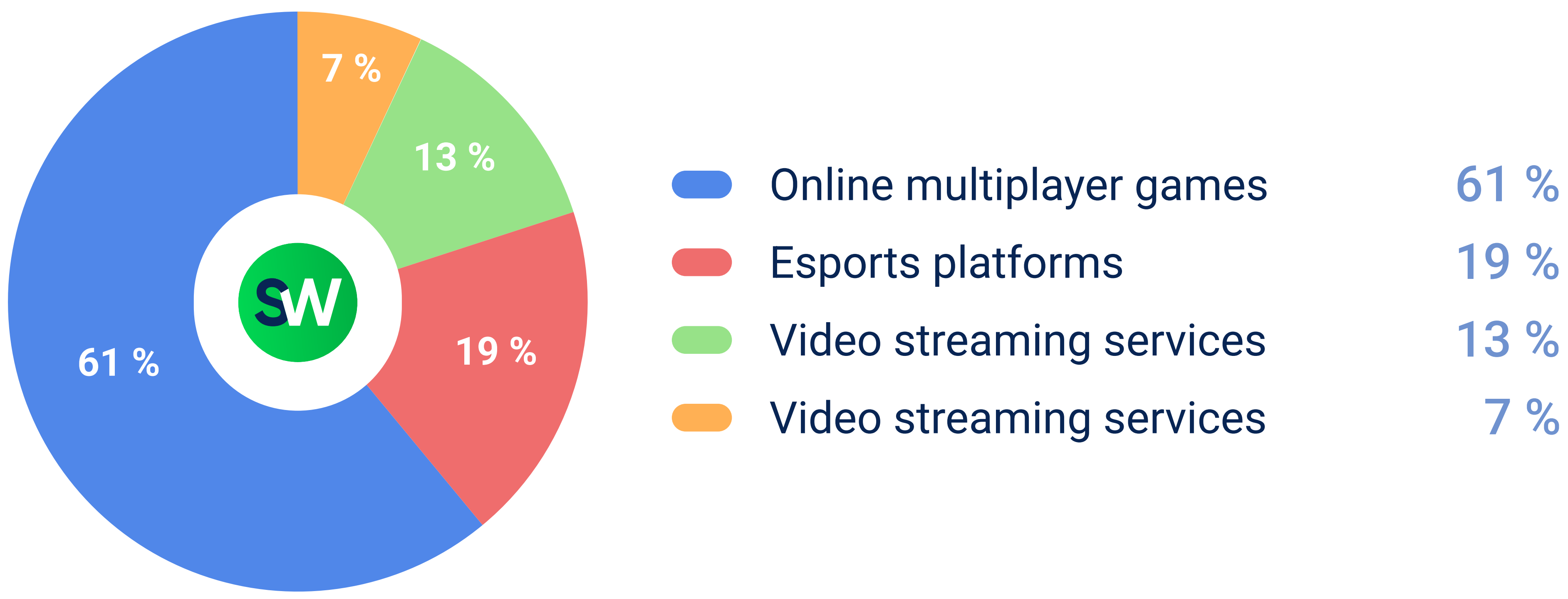
Attack Share	YoY Growth
18 %	114 %

Entertainment targets include online multiplayer games, esports platforms, video streaming services, and media broadcasters.

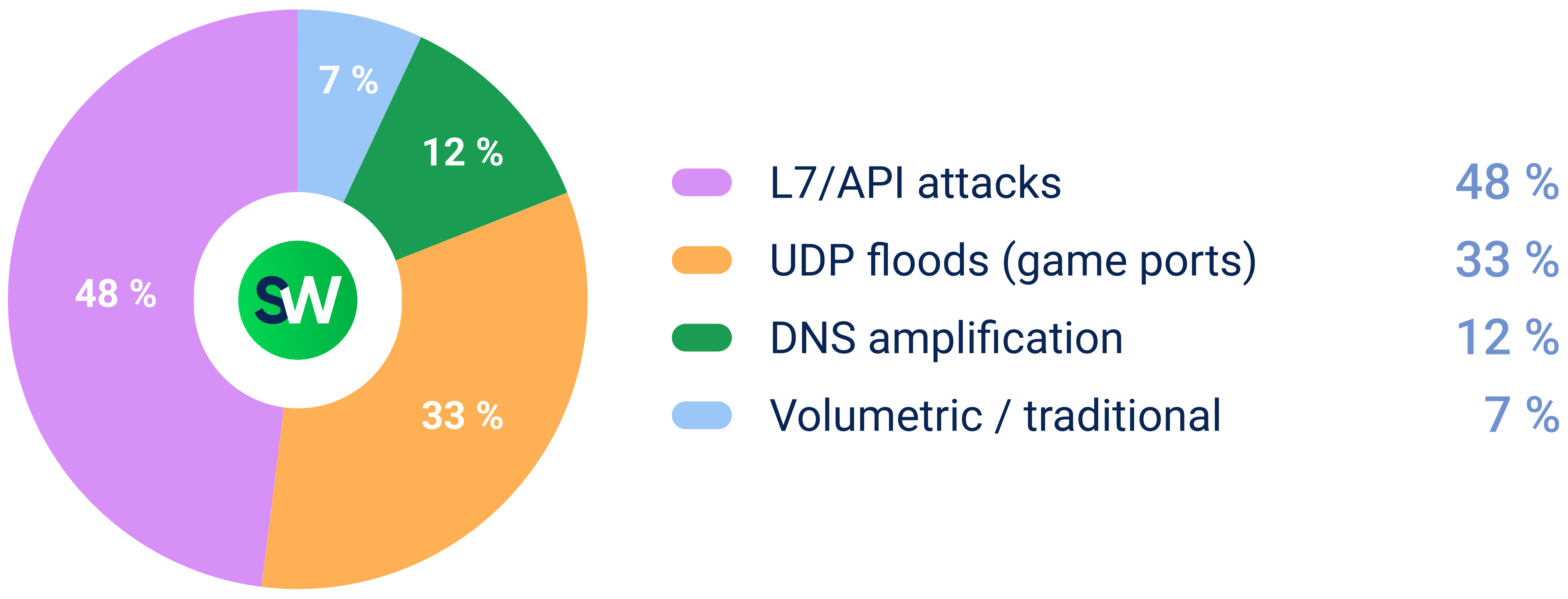
These are attractive targets for a few reasons: Some attackers (especially younger hackers or DDoS-for-hire users) treat gaming server attacks as a form of notoriety or vandalism. There have also been cases of competitive sabotage (knocking rival gamers or services offline).

Gaming is a huge business in Asia–China's gaming market alone is $60+ billion–making it a great target for extortion as well (e.g. threatening to DDoS a popular game unless a ransom is paid). Gaming sub-sites in China, India, and Korea have been particularly heavily targeted.

Most attacks focused on gaming infrastructure:



Attack techniques in this sector often target latency-sensitive environments, as the goal is to make the gaming experience worse:



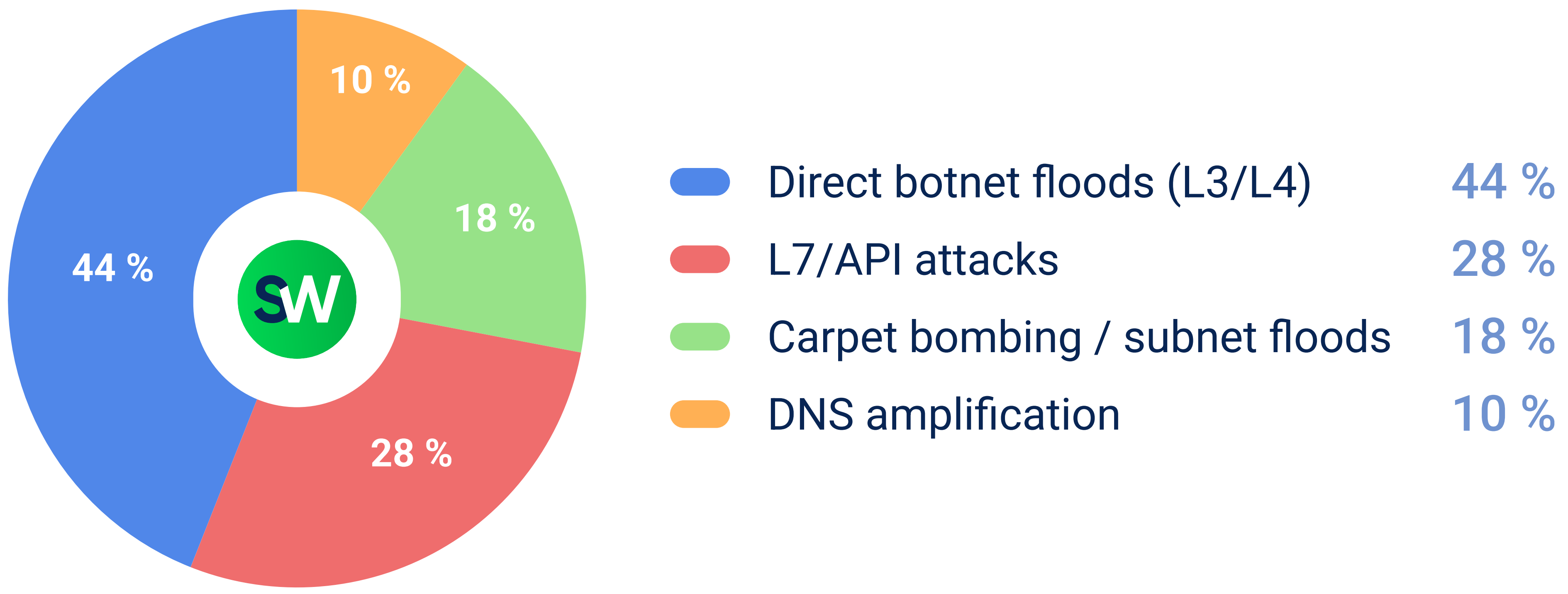
Government Sector

Attack Share	YoY Growth
12 %	104 %

In Q1 2025, multiple large-scale DDoS campaigns targeted government infrastructure across APAC. Notably:

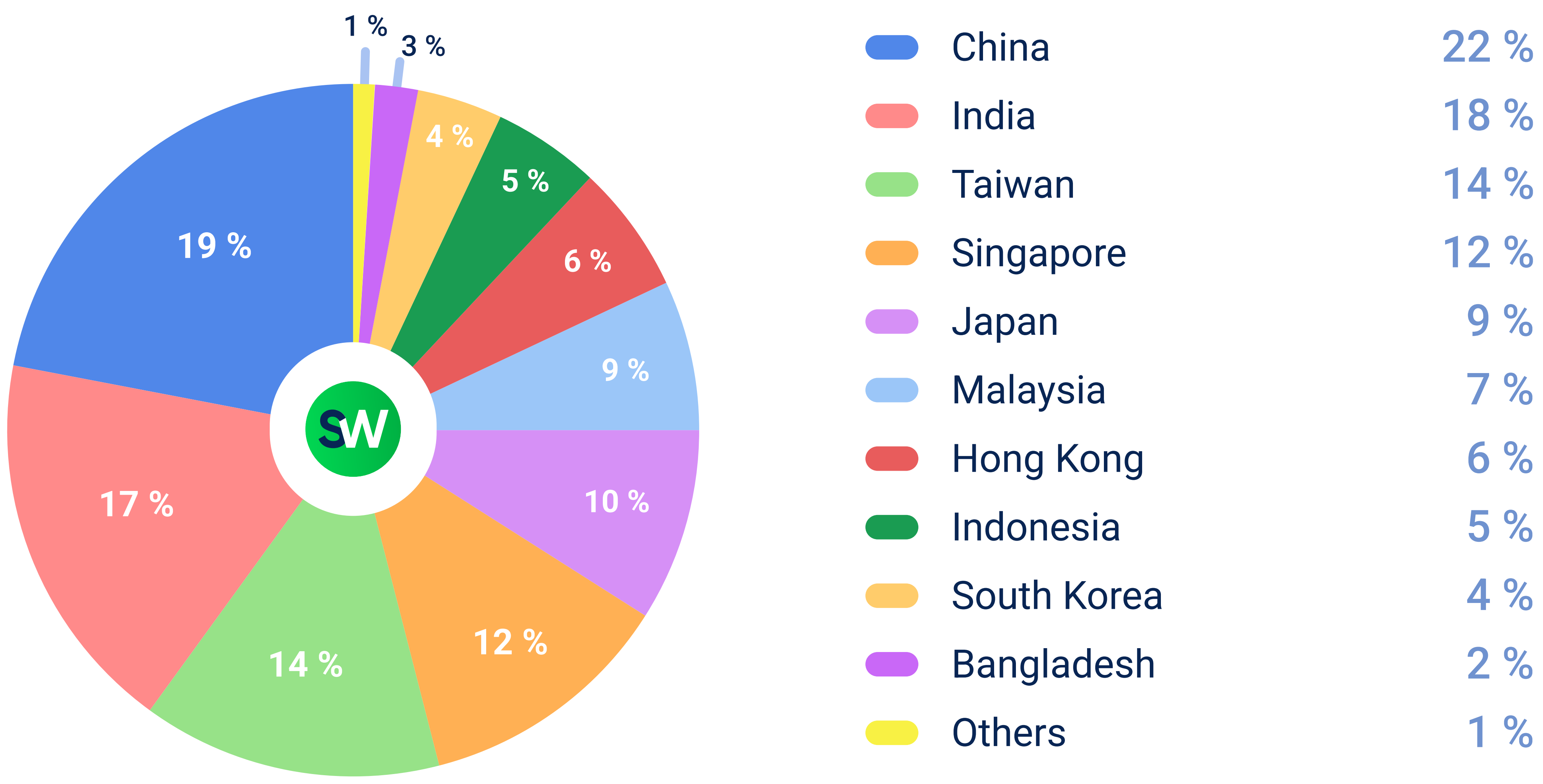
- **Taiwan:** Chinese nationalist hacktivists launched DDoS attacks targeting government offices. These attacks were short but extremely intense—averaging 600–900 Gbps over bursts lasting 1–2 hours.
- **Japan:** The “DDoSia” botnet, associated with pro-Russian actors, continued attacking Japanese government and industry sites. These attacks primarily used direct botnet traffic from compromised devices and cloud servers.
- **India–Pakistan:** Regional hacktivist groups engaged in tit-for-tat DDoS activity, mostly small-scale floods (50–100 Gbps) targeting government portals and regional infrastructure, often timed with political events.

Direct botnet floods were the most popular attack method, sometimes combined with application-layer (L7) attacks aimed at public APIs and login portals:



DDoS Attacks **by Country**

Let’s break down how DDoS attacks were distributed by country in Q1 2025:



Comparing this data with the fourth quarter of 2024, China became the most targeted country in APAC, with its share of attacks increasing from 18% to 22%. India saw its share of attacks decline from 21% to 18%.

Taiwan was hit with an unprecedented number of DDoS attacks for the tiny country, and its relative share rose from 2% in Q4 2024 to 14% in Q1 2025, driven by coordinated DDoS campaigns by Chinese hacktivist groups.

Other notable shift from Q4 2024 to Q1 2025 include:

- Singapore: 16% → 12% ⌄
- Japan: 7% → 9% ⌃
- Malaysia: 3% → 7% ⌃
- Hong Kong: 9% → 6% ⌄
- Indonesia: 12% → 5% ⌄

South Korea, Bangladesh, and other smaller markets remained relatively stable, with minor changes in attack share compared to the previous quarter.

Quick **Highlights**

- Telecommunications accounted for 31% of all DDoS attacks in APAC— nearly doubling its share from the previous quarter. With a 136% YoY surge and the largest recorded attack peaking at 2.3 Tbps, telecom infrastructure is the primary battleground.
- Entertainment targets—dominated by gaming platforms—faced 18% of all attacks. Asia's gaming sector is now a top extortion target.
- Government attacks rose by 104% YoY, fueled by politically motivated campaigns across Taiwan, Japan, and South Asia.
- Carpet bombing attacks up by 96% YoY. UDP floods were the most common vector followed by TCP SYN and HTTP floods.
- API-layer DDoS attacks are up 74% YoY. Attackers mimic real API calls, exhausting back-end systems with low-RPS floods that evade simple rate-limiting.
- China was the most attacked country (22%), followed by India (18%). Taiwan experienced the most dramatic rise (2% → 14%), a result of large-scale hacktivist campaigns.

This report shows that volumetric floods are becoming less common than sophisticated attack methods. SOC teams should prepare to defend against low-volume API and carpet bombing attacks. We recommend executives to consider allocating resources toward modern, application-aware DDoS protection to ensure defenses cover both network and API layers.