StormWall

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

The State of DDoS Attacks

in APAC in 2024, a StormWall Report

In analyzing the DDoS attacks StormWall mitigated in 2024, we've uncovered critical patterns affecting businesses across Asia-Pacific. This report highlights the most targeted sectors, and documents emerging attack vectors.

These insights draw from real-world data collected at StormWall's scrubbing centers worldwide, including our Singapore facility. As a whole, StormWall's network can handle massive traffic surges – exceeding 5 Tbps during sustained attacks.

Our diverse client base in the APAC region has helped us spot DDoS trends as they emerge. We're publishing these findings now because we believe security teams across APAC need current, practical data to strengthen their defenses.

An Breakdown of Ddos Attack Trends **in APAC in 2024**

DDoS attacks in Asia rose 92% in 2024 compared to 2023. The increase aligned with elections in 17 Asia-Pacific countries, including India, Indonesia, South Korea and Taiwan, triggering more hacktivist activity. By the third quarter, hacktivism had intensified so much that Hong Kong and South Korea experienced higher volumes of malicious traffic than China and India – traditionally the region's most targeted countries.

Let's look at these trends in more detail:

- **Attacks increased by 92% compared to 2023,** marking this one of the highest year-over-year increases in StormWall's reporting history.
- **Attack targets shifted between quarters.** While the government sector received the most attacks in 2024 overall, the patterns changed throughout the year. Government websites were the primary target in Q1 and Q2, coinciding with major elections in the APAC region. E-commerce sites received the most attacks in Q3 and Q4.
- **Geopolitics dominated cyber attacks in major ways.** Countries with political or economic ties to Russia came under heavy attack, including Indonesia, India, and China. Regional rivalries fueled attacks too — for example, there was malicious traffic flowing from Pakistan to India and back. This matters because it shows a key shift: over the past 2–3 years, geopolitical factors, not profit from extortion, have shaped how malicious traffic moves across the globe.
- **Telecommunications providers in the Asia-Pacific region faced escalating attacks throughout the year.** The sector climbed from the fourth most targeted industry in Q1 to third in Q2, finally settling at second place for both Q3 and Q4.

Let's discuss the most notable DDoS attack trends in the APAC region in more detail:

Political events drive attack patterns across APAC

For example, during South Korea's legislative elections, the country became APAC's primary target, receiving 26% of all malicious traffic in the region in April. And in another example, Japan saw similar patterns, with DDoS traffic spiking over 300% before the G7 summit hosted between May 19 and 21, as attackers targeted the Cabinet Office's public relations.

Overall, the government vertical absorbed 27% of APAC's DDoS attacks, showing 108% year-over-year growth. However, these attacks began declining in the second half of the year.

Attacks on government began declining in the second half of the year

This shift began occurring in September — political targets then saw less activity as government-focused attacks dropped 74%, and attackers instead pivoted toward financial targets. Singapore exemplifies this shift as one of the region's main financial hubs — attacks were up 166% in September-October, primarily targeting banks and payment processors.

There was a rise in Layer 7 and API-targeted attacks

Layer 7 and API attacks surged significantly in 2024, rising 85% and 76% respectively. This uptick aligns with increased targeting of financial services — the second most attacked sector — where API-driven services and web applications form the operational backbone through payment gateways and trading platforms.

DNS attacks showed distinct regional growth in APAC

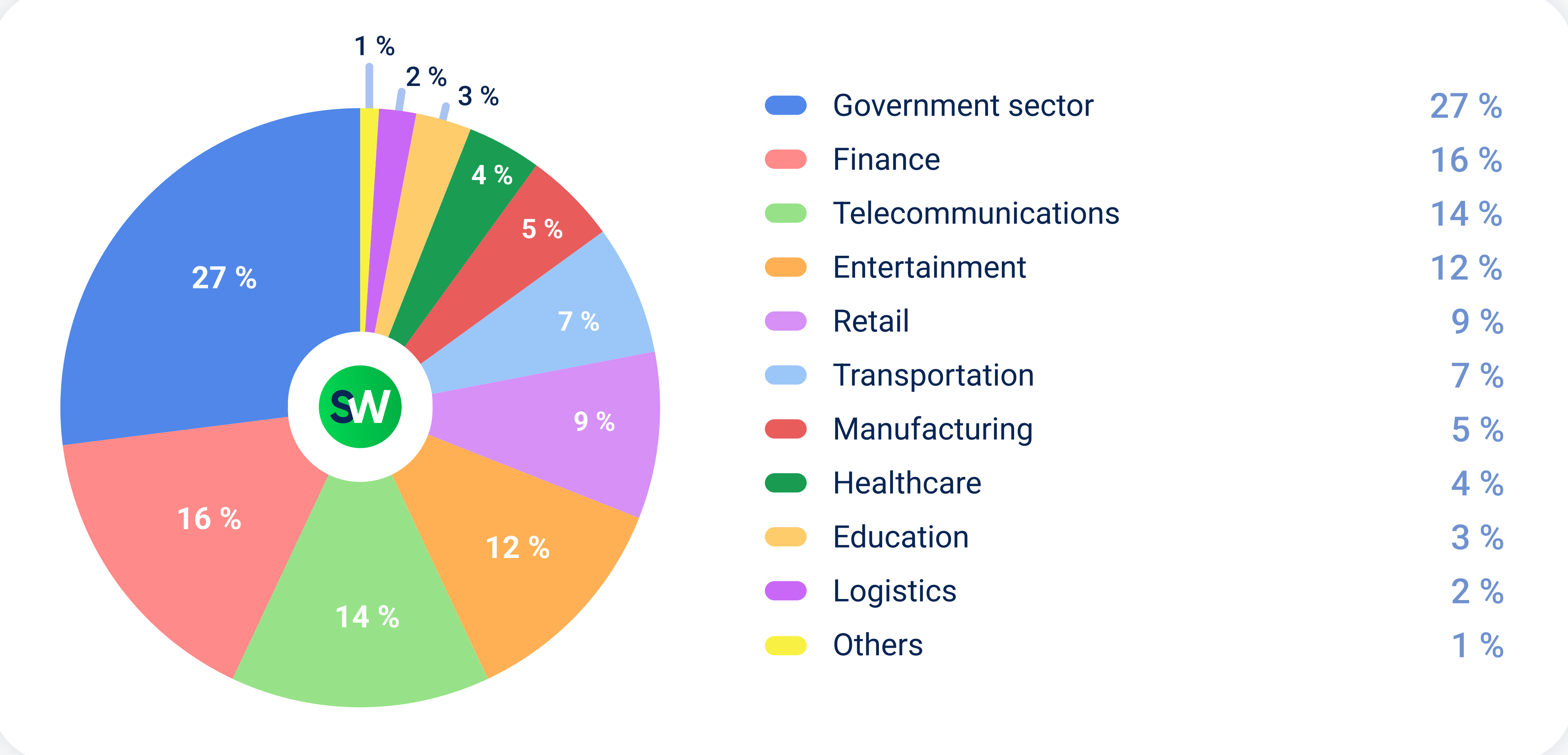
Layer 7 and API attacks surged significantly in 2024, rising 85% and 76% respectively. This uptick aligns with increased targeting of financial services — the second most attacked sector — where API-driven services and web applications form the operational backbone through payment gateways and trading platforms.

Multiple attacks **over 1 Tbps mitigated**

In 2024, StormWall mitigated multiple attacks in excess of 1 Tbps in the APAC region, targeting various sectors of the economy, most notably financial services, telecommunications, and entertainment.

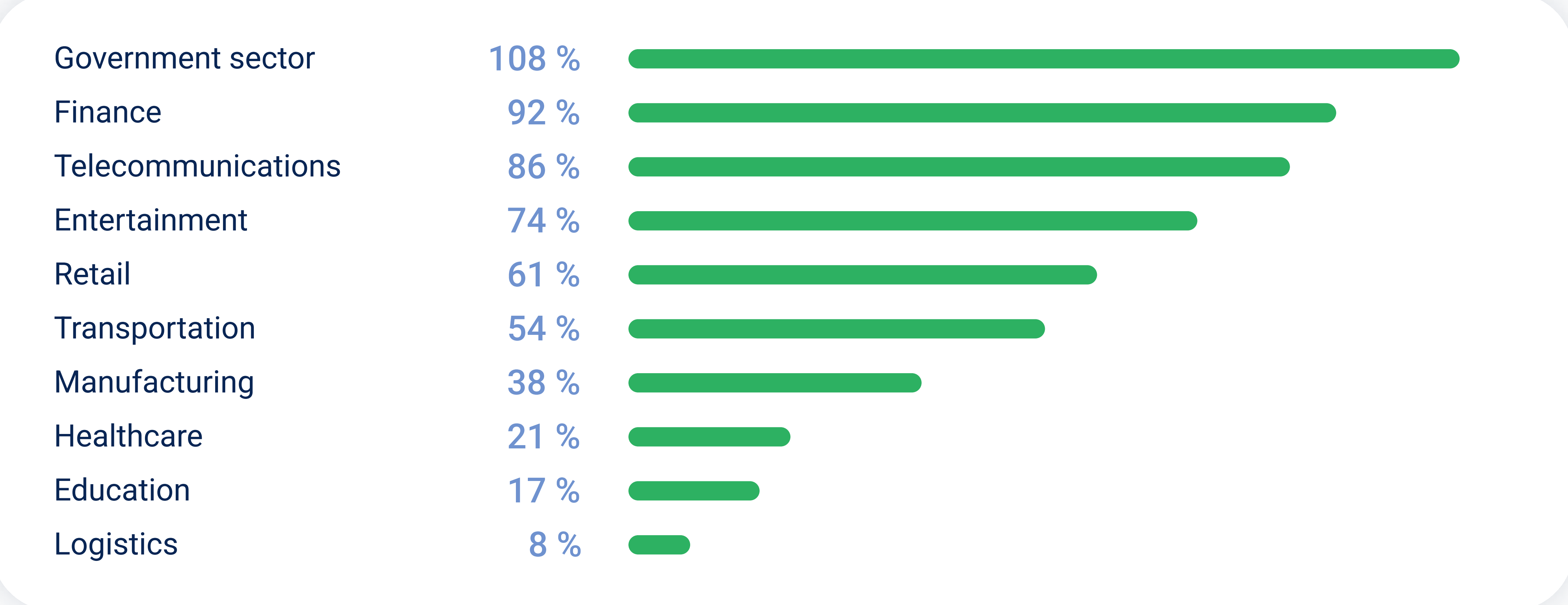
Attack Share Breakdown **by Industry**

Here is the distribution of DDoS attacks by vertical in 2024:



🟦	Government sector	27 %
🟥	Finance	16 %
🟩	Telecommunications	14 %
🟧	Entertainment	12 %
🟪	Retail	9 %
🟦	Transportation	7 %
🟥	Manufacturing	5 %
🟩	Healthcare	4 %
🟨	Education	3 %
🟪	Logistics	2 %
🟨	Others	1 %

Industries with highest YoY growth in DDoS attacks in 2024:



Government sector	108 %
Finance	92 %
Telecommunications	86 %
Entertainment	74 %
Retail	61 %
Transportation	54 %
Manufacturing	38 %
Healthcare	21 %
Education	17 %
Logistics	8 %

Let’s unpack the top-3 most attacked verticals in more detail:

1. **Government sector**

The Government vertical experienced the highest number of attacks at 27% and the highest year-on-year increase at 108%.

This stands in stark contrast to 2023, when DDoS attacks on government infrastructure made up only 8% of regional incidents. The spike coincided with a series of critical elections across Asia Pacific. During Taiwan's presidential and parliamentary votes in January 2024, for example, as government services faced more than double the usual attack volume in the days before the January 13 elections, and on election day over 800 incidents were recorded.

Similar patterns emerged in other countries during their electoral periods. For example, Bangladesh experienced a 71% increase during its parliamentary elections. The most powerful attack against a government service took place in South Korea in the second quarter – it reached 1.5 Tbit/s. The longest sustained attack lasted 3 days at a consistent load of 700 Gbit/s.

2. **Finance**

Financial services accounted for 16% of all attacks and showed a 92% year-over-year increase.

The impact of regional elections extended to this sector, as evidenced by the attacks on Taiwanese banks during the January 13 election period. Banking was clearly the primary target, with 89% of attacks concentrated on banking operations. Most traffic originated from China.

The threat landscape shifted in the second half of the year. As hacktivist activity decreased in Q3 and Q4, attackers refocused on profit-driven targets. The sector's growing API exposure — with over 1.3 billion banking API calls recorded in 2024 — created new attack vectors. This vulnerability showed in the numbers: API attacks surged 138% in Q3 2023 alone.

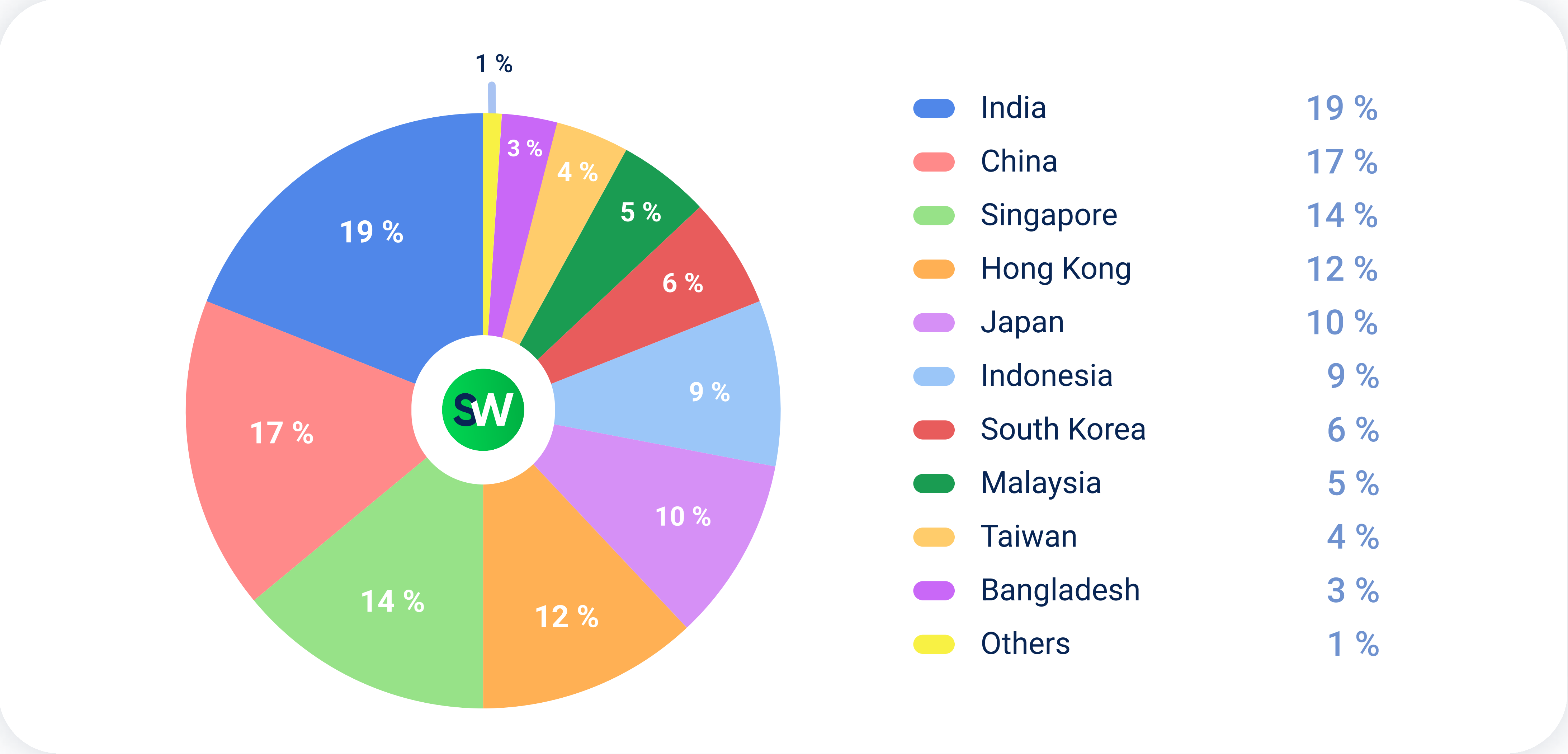
3. **Telecommunications**

Telecommunications ranked third in DDoS targets, absorbing 14% of attacks — an 86% rise from last year. DNS attacks proved especially effective here, given how telecoms depend on DNS for routing everything from calls to messages.

DNS Amplification and DNS Flood attacks comprised 45% of these incidents. Both exploit UDP protocol weaknesses, hammering servers with queries for non-existent domains. These attack methods, essentially, turn the sector's need for always-on DNS service into a weak spot.

Attack complexity was notably high, with over 85% of incidents targeting multiple vectors. The most common pattern involved simultaneous attacks across five to eight vectors.

Ddos Attacks in APAC: **Breakdown by Country**



Looking at the attack distribution by country, China's attack volume plunged 9 percentage points, falling from 26% to 17% — the single biggest shift in the data. This knocked China from first to second place, with India taking the lead despite its small decline from 19% to 18%.

Japan surged forward dramatically, climbing from 4% to 10% of attacks. The country moved four positions higher with this 6-point increase. Attacks on Indonesia and Singapore also increased, with Indonesia rising 3 points to 9% and Singapore up 2 points to 14%. Attacks on Malaysia, on the other hand, saw a sharp decline — they dropped 4 percentage points to end at 5%.

Meanwhile, Bangladesh entered the top 10 most attacked with 3% of attacks, replacing the Philippines which had held 2% in 2023. The remaining changes were minor: Hong Kong dipped from 14% to 12%, South Korea inched up from 5% to 6%, and Taiwan moved from 3% to 4%.

Conclusions

As we analyze DDoS attack trends in the Asia Pacific region for 2024, let's recap the key findings:

- **The government sector was the most targeted,** accounting for 27% of all attacks with a 108% year-over-year increase. Attacks on government services were increasing in the first half of the year, but started to decrease in the second half.
- **In the second half of the year, attackers pivoted from government targets to financial services.** This was particularly evident in Singapore, where attacks increased 166% in September-October, primarily targeting banking and payment processing systems.
- **Layer 7 and API-targeted attacks saw dramatic increases, rising 85% and 76% respectively.** This trend aligned with the increased targeting of financial services in the second half of the year, where API-driven services form the operational backbone of many institutions.
- **India emerged as the most targeted country with 19% of attacks.** It displaced China which fell to second place with 17%.
- **Attacks on Japan increased to 10% of attacks from the previous 4%,** which makes it one of the most significant geographical shifts.

In summary, DDoS attacks in APAC saw two distinct phases in 2024. The first half of the year was dominated by election-related attacks and hacktivism, with government websites in Taiwan, South Korea, and other countries experiencing heavy traffic during voting. In the second half, attackers shifted their focus to banks and telecoms.

This suggests a return to profit-driven attacks and a threat landscape that more closely resembles the pre-2023 landscape-at least in terms of attack targets. As we move into 2025, financial services and telecoms are likely to see the highest levels of DDoS traffic. StormWall will continue to monitor these trends to help organizations prepare their defenses.