DDoS Attacks in APAC: An Analysis of 2023 Trends by StormWall

At StormWall we've analyzed DDoS attacks against our clients that took place in 2023. In this report, we are going to break down most affected verticals, popular vectors and geographical distribution of DDoS attacks, focusing on the Asia-Pacific region.

This analysis is based on data from our scrubbing centers, which are strategically located in various locations across the globe, including Singapore. Our network has the capability to filter huge volumes of network traffic — 3500 Gbit/s at peak.

Some of the leading enterprises and thousands of small APAC businesses in retail, fintech, telecommunications, and other sectors rely on our network, application, and website protection services. This naturally lets us see a wide range of DDoS attacks across different business verticals, and gives us a rare perspective to understand DDoS trends and share insights with the community.

APAC: An overview of DDoS trends in 2023

- **Attack power is increasing**. Many DDoS attacks we recorded in APAC in 2023 exceeded 1 Gbit/s. The most powerful reached 1.4 Gbit/s. This is significantly higher than last year's numbers and shows that bad actors' capabilities are increasing.

- **Geopolitics continues to shape the DDoS landscape**. Local and global geopolitical conflicts result in increased hacktivism and growing involvement of state-sponsored threat actors.

- **Multi-vector attacks are the main threat of the year.** Over half of all attacks in 2023 targeted at least 2 vectors — which is a 118% increase compared to 2022.

- **DNS attacks on the rise in APAC**. Powerful DNS attacks were twice as commonly used in Asia-Pacific as the rest of the world. Telecommunication providers were exposed to this vector the most.

- **The 3 most targeted verticals.** The telecommunications industry was by far the most targeted, accounting for 31% of DDoS attacks in APAC. Finance is in second place (18%), followed by retail (16%).

- **The 3 most affected countries**. We recorded the most attacks in China (26%), then India (18%) followed by Hong Kong (14%).

The big picture

When comparing 2023 DDoS traffic to 2022, we see a **38% YoY increase**.

In 2023, the Asia-Pacific region attracted both profit-seeking hackers and hacktivists, who were majorly influenced by political affiliation of many Asian countries with Russia and ongoing armed conflicts. Towards the year's end, APT and hacktivism-related attacks spiked majorly across all business sectors — both numerically and in terms of attack power. This trend coincided with the ongoing Israel-Hamas war, which began in October 2023.

Percentage distribution of DDoS attack power

- <10 Gbit/s 24%
- 10-100 Gbit/s 41%
- 100-500 Gbit/s 28%
- >500 Gbit/s 7%

Analyzing attack power, lesser incidents (<10 Gbit/s) made up 24% of DDoS traffic in APAC, targeting smaller or less-protected companies. The bulk of attacks (41%) fell in the 10 Gbit/s to 10 Gbps range. We can call these attacks moderately strong — sending enough traffic to disrupt services. Attacks over 100 Gbit/s fall into the “very strong” category, capable enough to clog enterprise-level networks.

Attack power peaked at 1.4 Tbit/s

The most powerful attack we recorded in 2023 reached 1.4 Tbit/s and lasted 7 minutes. This distributed attack targeted a victim located in Singapore, and it took place in the 4th quarter of 2023. This shows that by year’s end attackers could muster very considerable firepower. The short duration implores a test-run, or, possibly, a display of power.

Multi-vector attacks up 118%

Attacks targeting 2 or more vectors made up almost 50% of all DDoS APAC traffic in 2023. Comparing 2022 to 2023 figures, we see a 118% increase in such incidents.

Multi-vector DDoS attacks strike at more than one service at the same time. For example, a flood of HTTP requests to a website can be combined with a UDP flood targeting the network infrastructure. In rare cases, we saw attackers combining over 20 protocols in a single

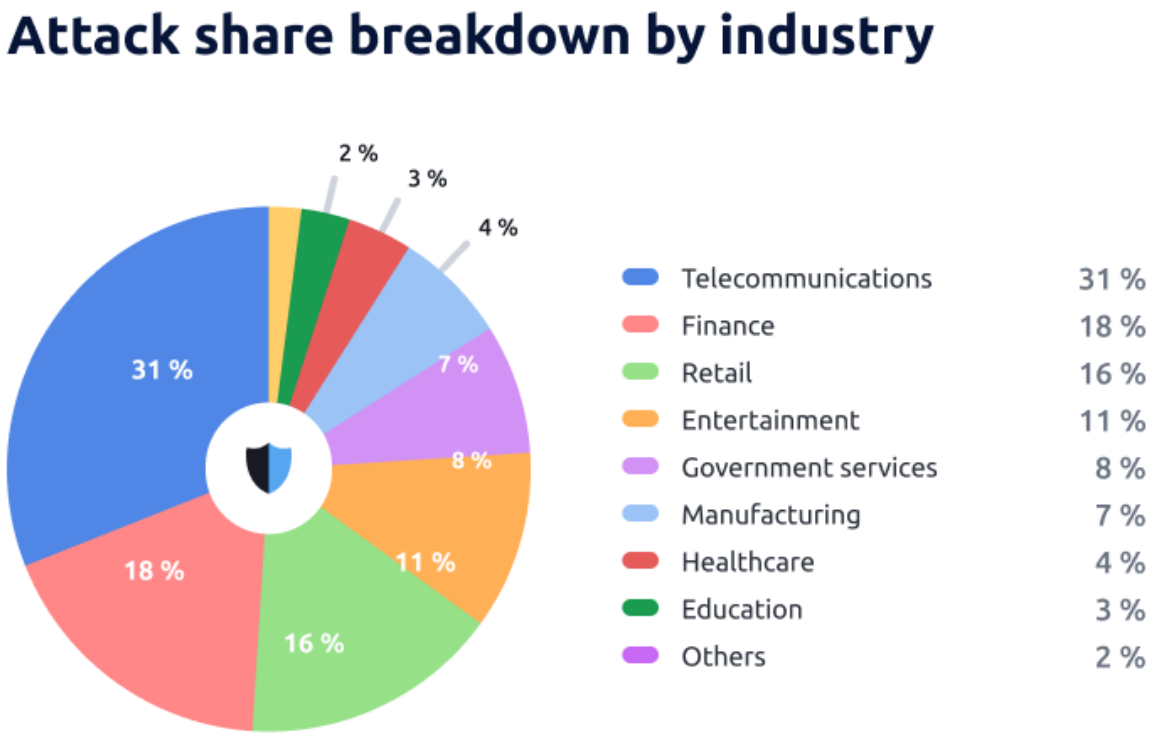
campaign, though attacks aimed at more than 5 vectors made up less than 10% of the overall traffic.

Attacks targeting the DNS were twice as popular in APAC compared to global average

Our data shows that DNS attacks account for 6% of all DDoS incidents we've tracked in the APAC region. In contrast, around the world, only 3% of attacks target DNS. This difference really stood out in the last half of 2023, especially in the third and fourth quarters, when we saw a major spike in DNS attacks against companies in APAC.

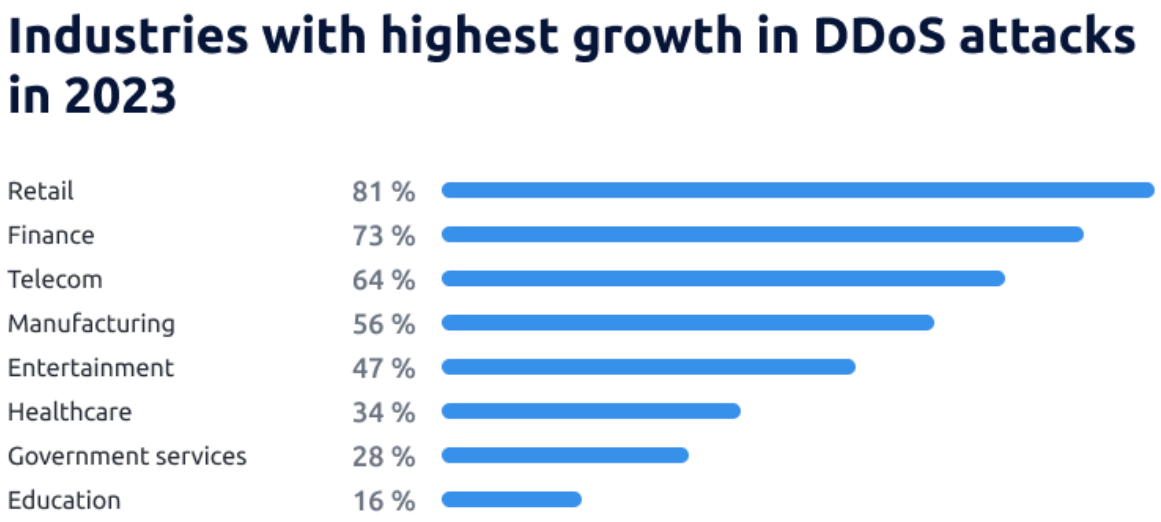
The most common types of DNS attacks were 'Carpet Bombing' DNS water-torture attacks, and the 'Bits and Pieces' method, which involves sending small bursts of junk traffic across many IP addresses simultaneously.

Attack share breakdown by industry



Industry	Attack Percentage
Telecommunications	31%
Finance	18%
Retail	16%
Entertainment	11%
Government services	8%
Manufacturing	7%
Healthcare	4%
Education	3%
Others	2%

APAC Industries with highest growth in DDoS attacks in 2023:



Industry	YoY Growth Percentage
Retail	81%
Finance	73%
Telecom	64%

Manufacturing	56%
Entertainment	47%
Healthcare	34%
Government services	28%
Education	16%

Here are the main takeaways:

- The telecom sector was the top target for DDoS attacks in APAC during 2023, taking more than 30% of the hits. Finance came in second with 18% of attacks, and Retail was close behind in third place with 16%.

- The data shows a significant imbalance in attack distribution. Notably, companies in the telecom industry are about 3.5 times more likely to be targeted by DDoS attacks compared to those in other sectors.

- Retail experienced the most notable increase in DDoS attacks, with an 81% rise compared to 2022. These attacks mainly targeted e-commerce sites, many of which increased adoption thanks to introducing online loyalty programs, and online booking platforms that bounced back in popularity to nearly pre-pandemic levels.

Let’s break down attacks on each industry in more detail.

Telecommunications

DDoS attacks targeting the telecommunications sector accounted for 31% of all incidents in APAC in 2023. This means telecom companies were more than three times as likely to be hit by these attacks compared to businesses in other sectors. Specifically, telecom saw a 64% increase in attacks year over year.

Within the telecom industry, wired carriers were the main target, with about 83% of the attacks, while wireless carriers faced roughly 14% of them.

The most significant increase in attacks occurred in the second half of 2023. This coincided with a notable shift: many broadband gaming users moved to 5G fixed wireless access. As telecom providers expanded their networks and user numbers peaked, this growth drew increased attention from hackers.

Finance

Finance was the second most targeted sector for DDoS attacks, with 18% of all incidents and a 73% year-over-year growth. This increase makes finance the industry with the second-fastest growth in DDoS activity, trailing only behind Retail.

A notable tactic in these attacks was their use for smokescreening, which involves using a DDoS attack to obscure other malicious activities, such as credential stuffing for account takeovers or targeted ransomware threats.

Retail

Retail, which represented 16% of the total DDoS attack volume, saw the highest year-over-year growth at 81%. This surge is particularly significant compared to other regions where similar growth often stemmed from hacktivism linked to global events. In APAC, the rise in retail attacks appears more connected to the region's economic development.

We classify most of the attacks as Ransom DDoS. Here, attackers overwhelm a server to cause service downtime, then demand a ransom. This tactic hits online businesses like e-commerce platforms particularly hard, as any downtime can be costly. What’s more, we've recorded a rise in non-DDoS attacks carried out by bots, including credential stuffing attacks, and data scraping.

Entertainment

The entertainment sector in APAC faced 11% of all DDoS attacks, marking a 47% growth year over year. Our analysis highlights that online gaming providers are particularly vulnerable. The appeal for hackers lies in the nature of real-time multiplayer gaming networks, where even slight latency can disrupt gameplay, resulting in negative publicity and player turnover for the affected company.

Like in the retail sector, many of these attacks fall into the category of Ransom DDoS. It's also worth noting that the proportion of attacks targeting the entertainment industry in APAC is higher than the global average, standing at 11% compared to 8%.

Government services

Government services in APAC accounted for 8% of total DDoS attacks, with a year-over-year growth of 28%. A few years back, such an increase would have been headline-worthy.

However, in the current global context, this rate can be considered conservative. Globally, attacks on government services have surged by 108%, largely driven by heightened hacktivist

activity. This indicates that the APAC region has been relatively less impacted by hacktivism in the government sector compared to the global average.

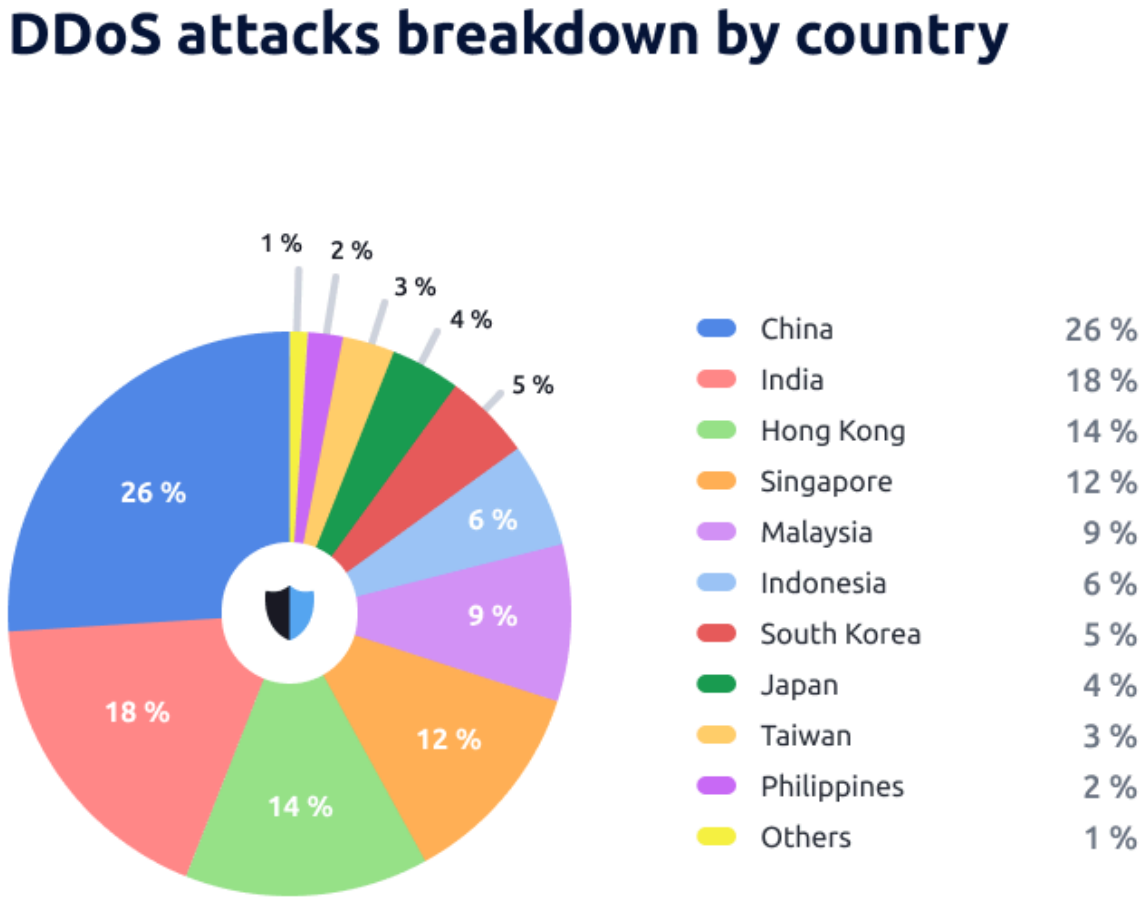
Other noteworthy industries

- **In the manufacturing industry,** DDoS attacks increased by 56% compared to the previous year. Though they represent just 7% of the overall attack share, this growth is significant — it suggests that hackers are paying more attention to this vertical. A trend manufacturers should be mindful of.

- **In the healthcare sector,** 4% of the APAC region's DDoS attacks were recorded, with a 34% increase in incidents. Singapore witnessed the highest number of attacks in this sector.

- **The education industry** accounted for 3% of the region's DDoS attacks in 2023. With a year-over-year growth of just 16%, it's the slowest growing vertical among those we analyzed.

Attack breakdown by country



Country	Attack Percentage
China	26%
India	18%
Hong Kong	14%
Singapore	12%
Malaysia	9%
Indonesia	6%
South Korea	5%

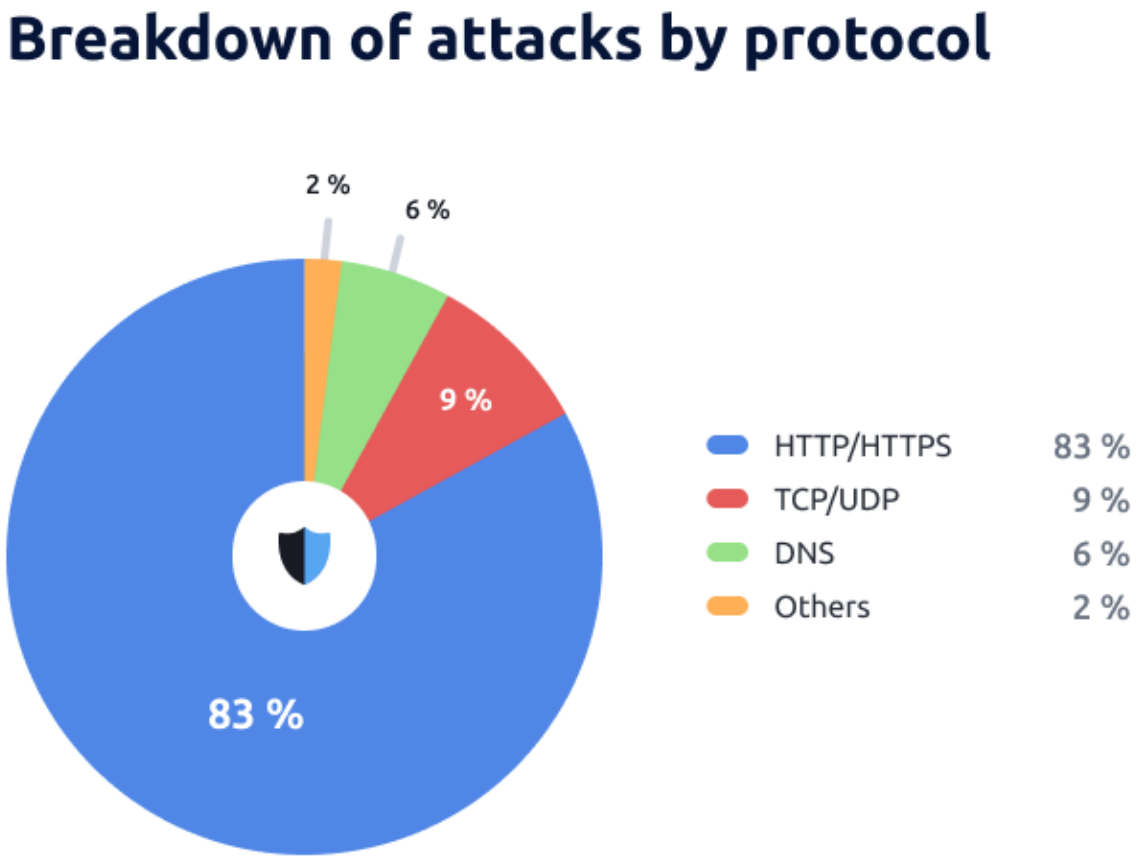
Japan	4%
Taiwan	3%
Philippines	2%
Others	1%

In the APAC region, China and India were the most targeted countries, facing 26% and 18% of DDoS attacks, respectively. Combined, they experienced nearly half of the region's attacks. This high incidence is not just due to their large populations but also their status as emerging economies, which makes them attractive targets for hackers.

Hong Kong saw 14% of the attacks, which is a very high figure considering its smaller size. Singapore was close behind with 12%. In both these regions, the finance sector was hit particularly hard, and there was significant hacktivist activity.

Interestingly, despite being a major origin for APT-related bot traffic, Indonesia only accounted for 6% share of the DDoS attacks in APAC.

DDoS Attacks: breakdown by protocol



- HTTP/HTTPS 83%
- TCP 9%
- DNS 6%
- Others 2%

HTTPS attacks in the APAC region saw a significant rise in 2023, with a 62% increase compared to 2022. These types of attacks were often launched using mixed and VM botnets. These botnets either combine different malware strains under a single command and control center or leverage cloud computing resources instead of IoT devices to generate requests.

Also notable is the high incidence of DNS attacks in APAC, at 6%. This rate is twice higher than the global average.

Conclusions

Let’s summarize our main findings.

- **Significant increase in DDoS activity**: The Asia-Pacific region saw a 38% increase in DDoS attacks in 2023 compared to the previous year, indicating a rising threat landscape.

- **Distribution of attack power**: Most DDoS attacks (41%) were moderately strong, ranging from 10 Gbit/s to 100 Gbit/s. However, the most powerful attack reached 1.4 Tbit/s, suggesting attackers in APAC are gaining formidable capabilities.

- **Surge in multi-vector attacks**: There was a 118% increase in multi-vector DDoS attacks, indicating a growing sophistication among attackers.

- **Telecom and finance sectors were targeted most**: The telecommunications sector was hit hardest by far, accounting for 31% of attacks. Finance was the second most targeted industry with 18%.

What can businesses do to protect against DDoS attacks?
We recommend implementing DDoS protection services from reliable providers. Key features to look out for is automation, presence of local scrubbing centers and intelligent traffic filtering. These aspects ensure that junk traffic can be identified and neutralized without creating noticeable latency for real users.

Our team at StormWall will keep on continuously monitoring the evolution of the DDoS landscape in the APAC region, informing the community about notable changes.