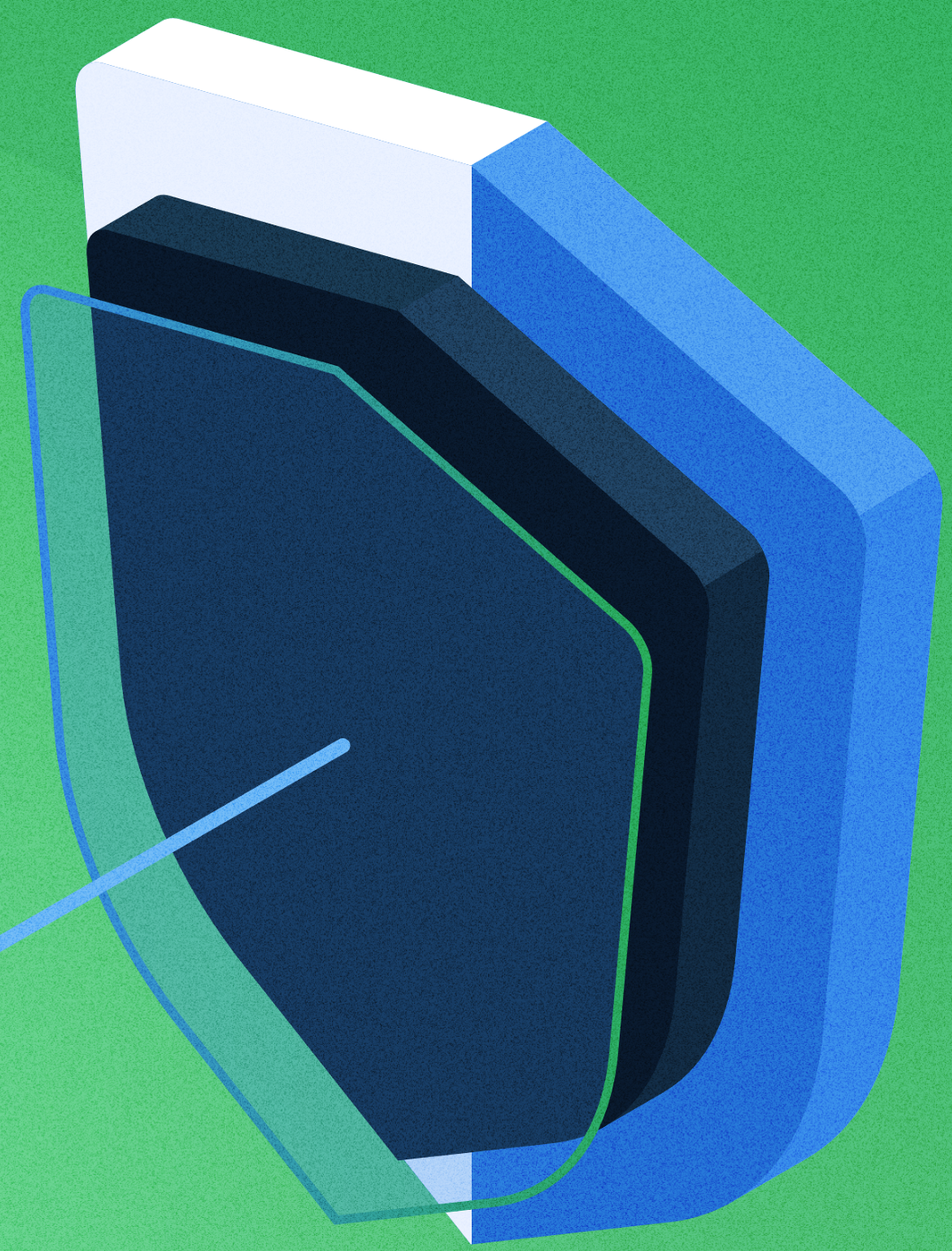
StormWall

The State of DDoS Attacks in APAC in Q1 2024

a StormWall Report



Welcome to StormWall's Q1 2024 report on DDoS attacks in the Asia Pacific region.

In this report, we analyze DDoS attack data from our clients across various industries in the region. Our scrubbing centers in Asia can filter up to 3,500 Gbit/s of traffic during peak times, allowing us to process a significant amount of data.

This puts us in a unique position to accurately evaluate the DDoS attack landscape. Throughout this report, we will highlight the main trends and causes of DDoS attacks that occurred in APAC during the third quarter of 2023.

Major Trends: DDoS attacks in APAC

Three trends stood out the most in the first quarter of 2024: yearly increase of DDoS traffic is at 108%, the impact of elections on the overall volume of malicious traffic and the most targeted industries, and a very concerning increase in botnet strength due to the growing number of devices. Let's break down the key trends in more detail.

This quarter, attacks are up 108% compared to Q1 2023

The growth is driven most by increased attacks on the government, entertainment, and finance industries

Elections in various APAC countries had a direct impact on the geographic distribution of attacks

Notable elections took place in Taiwan, Bangladesh, and Indonesia, and activists didn't stay on the sidelines. They attempted to influence the results by targeting critical services, leading to an increase in attacks in these countries. Attacks increased by 148% in Taiwan and by 74% in Bangladesh

Geopolitics remains a significant factor in the distribution of DDoS attacks across the Asia Pacific region

Countries with friendly ties to Russia experienced a higher proportion of attacks. China bore the brunt, with 16% of all DDoS attacks in APAC targeting the country. Singapore and Hong Kong faced 11% and 6% of the total, respectively

DNS attacks are on the rise

Globally, DNS attacks aren't that common. In Q1 2024, they accounted for only 4% of all incidents. In APAC, we're seeing that while DNS attacks are still less common than HTTP/HTTPS and TCP/UDP attacks, they are evolving much faster and are more widespread

Botnets are becoming increasingly powerful, alarmingly fast

The average number of devices in botnets has skyrocketed from around 4,000 in Q1 2023 to 16,000 in Q1 2024, which represents a 400% increase in power. That’s assuming the throughput of each device remains constant. However, it's likely that the throughput has also increased, meaning today's botnets are potentially more than four times stronger compared to last year

1.4 The most powerful attack we recorded (and mitigated) reached 1.4 Tbit/s

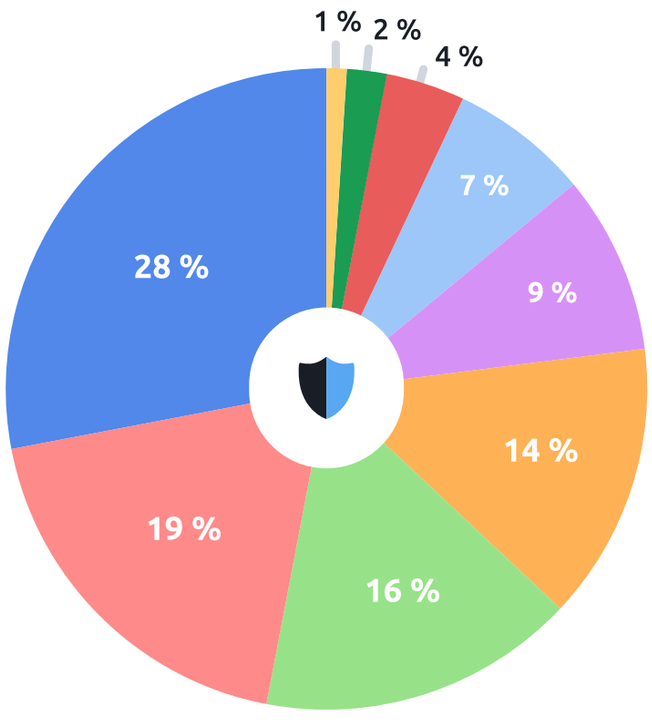
The increasing firepower of attackers is evident in the strongest attack we recorded so far in 2024. This attack, which targeted a StormWall client in China, was successfully mitigated by our DDoS protection system. To put the magnitude of the attack into perspective, the world's Internet traffic only briefly peaked at 22.36 Tbit/s on November 8, 2023, during the 4th day of the UEFA Champions League

Hackers are increasingly launching carpet bombing DDoS attacks

These attacks target entire networks rather than individual IP addresses. Instead of focusing their efforts on a single system, attackers are choosing multiple targets to overwhelm and compromise the network as a whole. In Q1 2023, we've seen a growing trend of these attacks in the APAC region

Most Attacked Industries in APAC in Q1 2024

We've observed the majority of attacks in 3 verticals in APAC in Q3 2023. The most attacked sector was government services. The second most attacked industry was financial services, and the third most-attacked was entertainment. Here's the full breakdown of the most attacked verticals:



1.	Government sector	28 %
2.	Finance	19 %
3.	Entertainment	16 %
4.	Telecommunications	14 %
5.	Retail	9 %
6.	Manufacturing	7 %
7.	Education	4 %
8.	Healthcare	2 %
10.	Others	1 %

Industries with highest YoY growth in DDoS attacks in Q1 2024:

1.	Government services	114 %
2.	Entertainment	86 %
3.	Telecommunications	72 %
4.	Finance	54 %
5.	Retail	48 %
6.	Manufacturing	22 %
7.	Education	18 %
8.	Healthcare	14 %

Below we break down the trends that have contributed to the concentration of attacks targeting the top 3 verticals: Government, Finance, and Entertainment sectors:

1. Government sector

Government services experienced 28% of cyberattacks, up 114% YoY, making it not only the most targeted sector but also witnessing the fastest growth in DDoS attacks.

During Q3 of 2023, DDoS attacks on government infrastructure in APAC accounted for a mere 6% of all incidents in the region, with a relatively modest 14% growth rate. So, what happened to cause the share of attacks on this sector to skyrocket by approximately 360% in just 8 months?

What makes government services the most targeted industry?

This is the result of elections held in several countries in the APAC region. For example, important parliamentary elections were held in Bangladesh, as well as in Bhutan and Pakistan. Taiwan had both presidential and parliamentary elections. We can see how this had a direct impact on the DDoS attacks in each country. In Taiwan, we saw a 148% increase in attacks against our customers, and in Bangladesh, a more modest but still significant 71% increase.

Attacks on Taiwanese government services more than doubled in the days leading up to the January 13 elections. Most of the malicious traffic originated from China, as several Chinese threat actors appear to have attempted to derail the election results. Government agencies and, alarmingly, the police infrastructure were the hardest hit. The attacks came and went like a tidal wave, with over 800 incidents recorded on election day alone.

Both activists and state-sponsored groups were involved. They used DDoS attacks as a means of disrupting government infrastructure and to create a smokescreen, concealing data exfiltration attempts.

How much this affected the outcome of elections themselves — if at all — is hard to say at this point, but this shows how DDoS attacks can be used as a political weapon. Today, hacktivism is heavily intertwined with DDoS attacks, to the extent that the industry where politically motivated attacks are most prevalent usually tops the list of most attacked industries. It's a trend we've been tracking since late 2024.

2. Finance

The financial services sector was also hit hard by DDoS attacks in the Asia-Pacific region, accounting for a 16% share and a 54% year-over-year growth.

In this industry, we continue to see the ripple effects of elections. A prime example is the surge in DDoS attacks targeting Taiwanese banks just before and during the election period on Saturday, January 13, 2024. The vast majority of these attacks, a whopping 89%, specifically targeted the banking sector. Most of the malicious traffic originated from China.

As the backbone of Taiwan's $760 billion economy, the country's banks and their underlying digital infrastructure are considered vulnerable to cyber threats. The situation has become so concerning that in December 2023, Taiwanese officials reached out to the U.S. for assistance in bolstering the cybersecurity of their financial infrastructure. Experts believe that if tensions in the region reach a boiling point, China's opening move will be a crippling cyberattack on Taiwan's banking system, potentially bringing the nation's economy to its knees. The attacks observed during the election period could be interpreted as Chinese threat actors testing the system's resilience.

3. Entertainment

The entertainment sector accounted for 16% of DDoS attacks in APAC in Q1 2024, and grew 86% year over year — the second highest growth rate after attacks on government services.

Data shows that hackers might target the entertainment sector more in 2024 than in 2023. Our analysis in Q3 2023 revealed that 14% of DDoS attacks were concentrated in this vertical, and the growth rate was much slower in Q3 2023 — 28%, vs 86% this quarter. The entertainment industry includes sub-sectors such as streaming services, betting companies and gaming, but it is the gaming industry that has been hit the hardest.

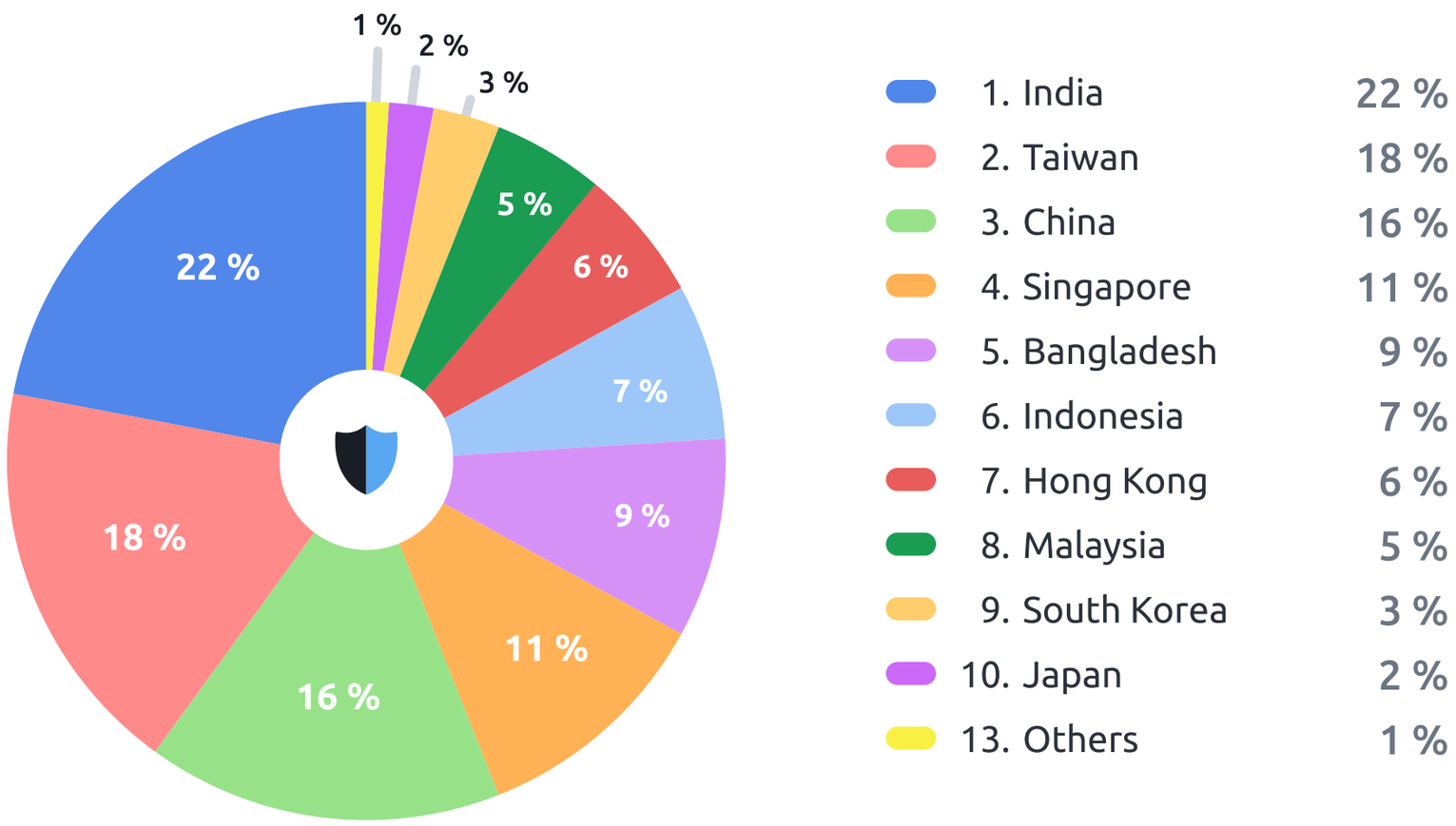
Why is gaming becoming a top target for DDoS attacks?

Gaming is a lucrative sector within the entertainment industry,and it has been heavily targeted by attackers, especially in countries like China, India, and Korea. China's gaming industry alone is projected to reach $66 billion by 2024. Multiplayer games, such as Honor of Kings, League of Legends, and CrossFire, are particularly vulnerable to DDoS attacks, which can make the games unplayable, leading to user outflow and financial losses for developers. Attackers exploit this to pressure developers and demand ransoms.

Examples of DDoS attacks in the gaming industry include the launch of Tekken 8, which was disrupted by relentless attacks, and a League Championship Series match at the LCK Arena in central Seoul, which was repeatedly interrupted, forcing games to be held at random times and locations, ultimately reducing attendance.

DDoS attacks in APAC: Breakdown by Country

Here is a breakdown of the distribution of DDoS attacks in Southeast Asia by country in the first quarter of 2024:



The geographic distribution of the attacks shows interesting upsets, especially compared to Q3 2023. Let's break them down:

- **Unusually high attack volume in Taiwan and Bangladesh**

Taiwan and Bangladesh, which accounted for 18% and 9% of the total DDoS attacks respectively, held elections in Q1 2024. These events had a significant impact on the volume of DDoS attacks in these regions. Taiwan was the second most attacked country in APAC, with its share

increasing from just 4% in Q3 2023. Bangladesh, with a 9% share, ranked fifth, despite accounting for less than 1% of attacks in Q3 2023. Surprisingly, both of these countries outranked Indonesia, which accounted for only 7% of the DDoS traffic, despite its much larger size and population.

- **Attacks on Hong Kong and South Korea have been less frequent**

In Q3 2023, these two countries were the most heavily targeted in APAC, even surpassing China and India. However, in Q1 2024, they weren't hit as hard compared to other countries in the region. Hong Kong accounted for 6% of the total DDoS traffic in APAC, while South Korea made up only 3%.

- **Singapore's share of attacks is steadily rising**

As one of the most developed economies in the APAC region, and a country with political ties to Russia, Singapore is becoming an increasingly frequent target of DDoS attacks. Its share of attacks increased from 8% in Q3 2023 to 11% in Q1 2024. Hackers are particularly targeting the healthcare and banking sectors.

7. Media

The media sector saw an increase in DDoS attacks of 4% and 16% respectively. Attacks on this vertical were related to political elections, which took place in more than 15 countries in Q1 2023. The reason for the attacks is hactivism. Media websites are, of course, important platforms for political candidates. It can be advantageous for rivals to disrupt sources of information, especially to suppress unfavourable stories.

The takeaway is that despite the modest 4% share of attacks, the increase in attacks on the media is significant. It illustrates how DDoS is becoming a source of disinformation on a global scale.

8. Education

In the education sector, there were 2% of attacks, accounting for an 11% share of the total. Although the number of attacks decreased by 50% from Q3 2023, the growth rate remains consistent. During the last period, we recorded a 12% YoY growth, only 1% higher than in Q1 2023. Similar to the retail sector, when holiday seasons see DDoS activity skyrocket, attacks on education often peak during specific periods such as admissions, and are carried out by both hacktivists and students attempting to disrupt exams.

In conclusion

As we wrap up our analysis of DDoS attack trends in the Asia Pacific region for Q1 2024, several key points stand out:

The yearly increase in DDoS traffic reached an alarming 108%, largely driven by attacks on government, entertainment, and telecommunications sectors

Elections in various APAC countries, notably Taiwan, Bangladesh, and Indonesia, had a direct impact on the geographic distribution and volume of malicious traffic. Activists attempted to influence results by targeting critical services

Geopolitics continues to shape the DDoS landscape in APAC. Countries with friendly ties to Russia, particularly China, Singapore, and Hong Kong, bore the brunt of attacks

The strength of botnets has grown at an alarming rate, with the average number of devices increasing by 400% compared to Q1 2023. The most powerful attack recorded reached an unprecedented 1.4 Tbit/s

The overarching trend this quarter was the influence of politics on the DDoS landscape. We still see that most malicious traffic originates from hacktivists and state-sponsored groups. These adversaries are well-equipped and have access to significant resources. However, there is also a positive aspect to this trend — predictability.

As DDoS attacks coincide with political events, we can better plan for them and anticipate future trends. Elections in 2024 will continue, with general elections in India taking place from April 19 to June 1, the 2024 Iranian legislative election on March 1 (first round) and May 10 (second round), the 2024 North Korean parliamentary election, and the 2024 South Korean legislative election on April 10.

Based on the trends observed in the last quarter, it is likely that DDoS attacks will concentrate around these countries in Q2 2024, with government and banking services being the most targeted sectors.