# StormWall 2023 Report

*Analysis of DDoS attacks in 2023 in Asia-Pacific*

## 38% Increase in DDoS Activity Across Asia
## Multi-Vector Attacks Up Multifold

**StormWall's analysis of DDoS attacks in 2023 shows a 38% year-over-year surge in the Asia-Pacific region.**

### *Multi-vector attacks up 118% YoY*

2023 was marked by a dramatic 118% increase in multi-vector attacks, the report finds, highlighting a shift towards more complex attack strategies. Multi-vector attacks target several infrastructure elements simultaneously and often combine DDoS and non-DDoS attack methods, which makes them particularly destructive.

The rise in hacktivism is one of the factors that played a role in the popularity of multi-vector attacks. Throughout 2023, global politics shaped the threat of DDoS attacks. As more and more state-supported hacker groups got involved in cyber warfare linked to worldwide conflicts, they created advanced tools and complex attack methods. Some of their techniques leaked into the public domain, making DDoS attacks more sophisticated overall.

### *Telecommunications is the most attacked industry in APAC*

Looking at the attack data by vertical, the telecommunications sector was hit the hardest, accounting for 31% of all DDoS attacks in APAC. This sector saw a 64% increase in attacks from the previous year, StormWall data shows. The finance and retail sectors followed with 18% and 16% of total attacks, respectively. In terms of biggest YoY growth, the retail sector was in the lead with 81% spike in attacks.

### *41% of DDoS attacks were between 10 Gbit/s and 100 Gbit/s*

In the Asia-Pacific region, DDoS attacks with a bandwidth below 10 Gbit/s constituted 24% of the total DDoS traffic, typically directed at smaller or less-protected companies. The majority of attacks, accounting for 41%, fell within the 10 Gbit/s to 100 Gbit/s range. These attacks can be considered moderately strong, as they generate enough traffic to disrupt services. Notably, attacks in the 100 – 500 Gbit/s range made up 28% of the total, and attacks exceeding 500 Gbit/s — 7% of the total. The StormWall report categorizes them as "very strong", posing a significant threat to clogging enterprise-level networks.

# StormWall 2023 Report

*Analysis of DDoS attacks in 2023 in Asia-Pacific*

### *Over 80% of attacks targeted the application layer*

Looking at the breakdown of attacks by protocol in the Asia-Pacific region, 83% targeted HTTP/HTTPS, frequently executed by mixed and VM botnets. Notably, HTTP/HTTPs attacks were up 62% in 2023 compared to the previous year. Following this protocol, TCP accounted for 9% and DNS — for 6%, which is twice the global average. Other protocols constituted the remaining 2%.

### *Distribution of attacks by country*

China, India, and Hong Kong were the top targets for DDoS attacks in their region, facing 26%, 18%, and 14% of the attacks respectively, StormWall says. Together, they suffered almost half of all regional attacks. As large and quickly developing economies, these countries represent appealing targets for hackers.

The strongest attack happened in Singapore, hitting 1.4 Tbit/s and lasting 7 minutes. It occurred in the last quarter of 2023. This indicates that by the end of the year, attackers had the capability to launch very powerful attacks.

## More detail

Download and read the StormWall DDoS Attacks in Asia Pacific in 2023 report in full:

https://www.startupnewsasia.com/wp-content/uploads/2024/02/StormWall-DDoS-Attacks-APAC-Analysis-of-2023-Trends.pdf

MORE INFORMATION

For more info on StormWall services, products and analyses:

Online: https://stormwall.network/

On Facebook: https://www.facebook.com/stormwall.network

On Instagram: https://www.instagram.com/stormwall.network/

On LinkedIn: https://www.linkedin.com/company/stormwall/

On Twitter/X: https://twitter.com/stormwall_net