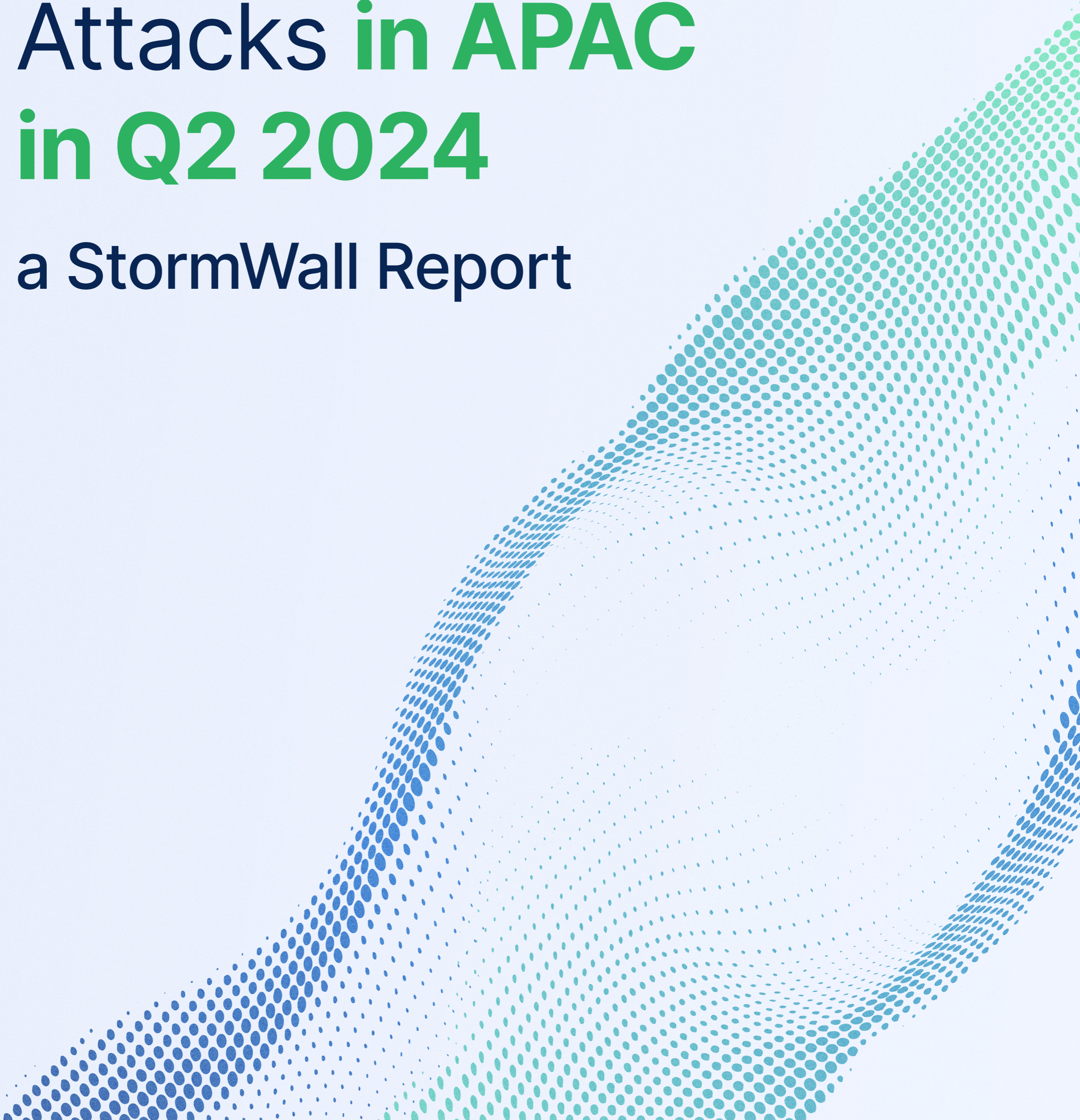




The State of DDoS Attacks **in APAC** **in Q2 2024**

a StormWall Report



Welcome to the APAC edition of the StormWall Q2 2024 DDoS Attack Report.

In this report, we analyze DDoS attack data collected from our customers across multiple industries. With specialized scrubbing centers in Asia, StormWall's network can handle traffic peaks of up to 4,500 Gbit/s. We defend our APAC clients against thousands of DDoS attacks daily.

This puts us in a unique position to provide an overview of the DDoS attack landscape. In this edition, we will detail the key trends and primary sources of DDoS attacks that our experts observed in the Asia-Pacific region in the second quarter of 2024.

Major Trends in Q2: DDoS attacks in APAC

In Q2 2024, DDoS attacks in Asia increased by 174% compared to Q2 2023. Elections in South Korea and North Korea pushed these countries into the top 3 most targeted in APAC, displacing China. Let's look at these trends in more detail:



Geopolitical impacts

South Korea (26% of attacks), India (18%), and North Korea (14%) were the top three most attacked countries. China, previously in the top three, now ranks fourth with 12% of attacks.



Heightened interest in Japan

There was a marked increase in attacks targeting Japan, which now ranks fifth among the most attacked countries with 9% of total attacks.



Taiwan, still a major target

Taiwan was the second most attacked country in APAC in Q1 2024, with an 18% share. Despite the share lowering to 4% this quarter, Taiwan still faces an abnormally high number of traffic floods.



Industry targeting shifts

The entertainment sector saw the highest year-on-year growth at 134%, with the gaming sub-sector particularly hard hit. This is followed by government services (116%) and transportation (107%). Government remains the most targeted sector overall, accounting for 27% of all attacks.



Botnets are still growing

The trend of increasingly powerful botnets continued from Q1, where the average number of devices in botnets had grown by 400% year-over-year.



Unusually high number of attacks on the transport sector

With a 107% increase in attacks, the transport sector has become a new focus for cybercriminals, now accounting for 11% of all attacks.

Threat actors target elections in South Korea and North Korea

South Korea was the most targeted country in APAC, with 26% of all malicious traffic we recorded hitting targets in the country, followed by North Korea with 14% of all DDoS attacks. That's a huge rise and the first time in a long time that we've seen China pushed out of the top 3 most attacked countries.

This revolves around geopolitics and how APTs operate.

- Attacks peaked during South Korea's legislative elections on 10 April 2024 and then again in June, echoing comments made by South Korean Ambassador Hwang on behalf of 57 member states of the UN, EU, US, UK and Japan on the human rights situation in the Democratic People's Republic of Korea (DPRK).
- There were coordinated attacks by at least 30 APT groups based in Russia, Sudan, Indonesia and elsewhere. Targets were mostly government infrastructure and transportation: Korean National Police, Ministry of Land, Infrastructure and Transport, and others.

Japan — the target of 9% of all malicious traffic

DDoS attacks against government and company websites in Japan began increasing in April, ahead of a Group of Seven summit the country hosted in May, between May 19 and 21.

Attackers hit the servers of government departments in Osaka, Aichi and Kumamoto prefectures, as well as Nara. The Cabinet Office's public relations was affected. APTs also targeted private companies: West Japan Railway, Tokyo Electric Power Company Holdings and others.

Overall, Japan was the fifth most targeted country, with 9% of DDoS traffic concentrated there this quarter. Last quarter's share was 2%.

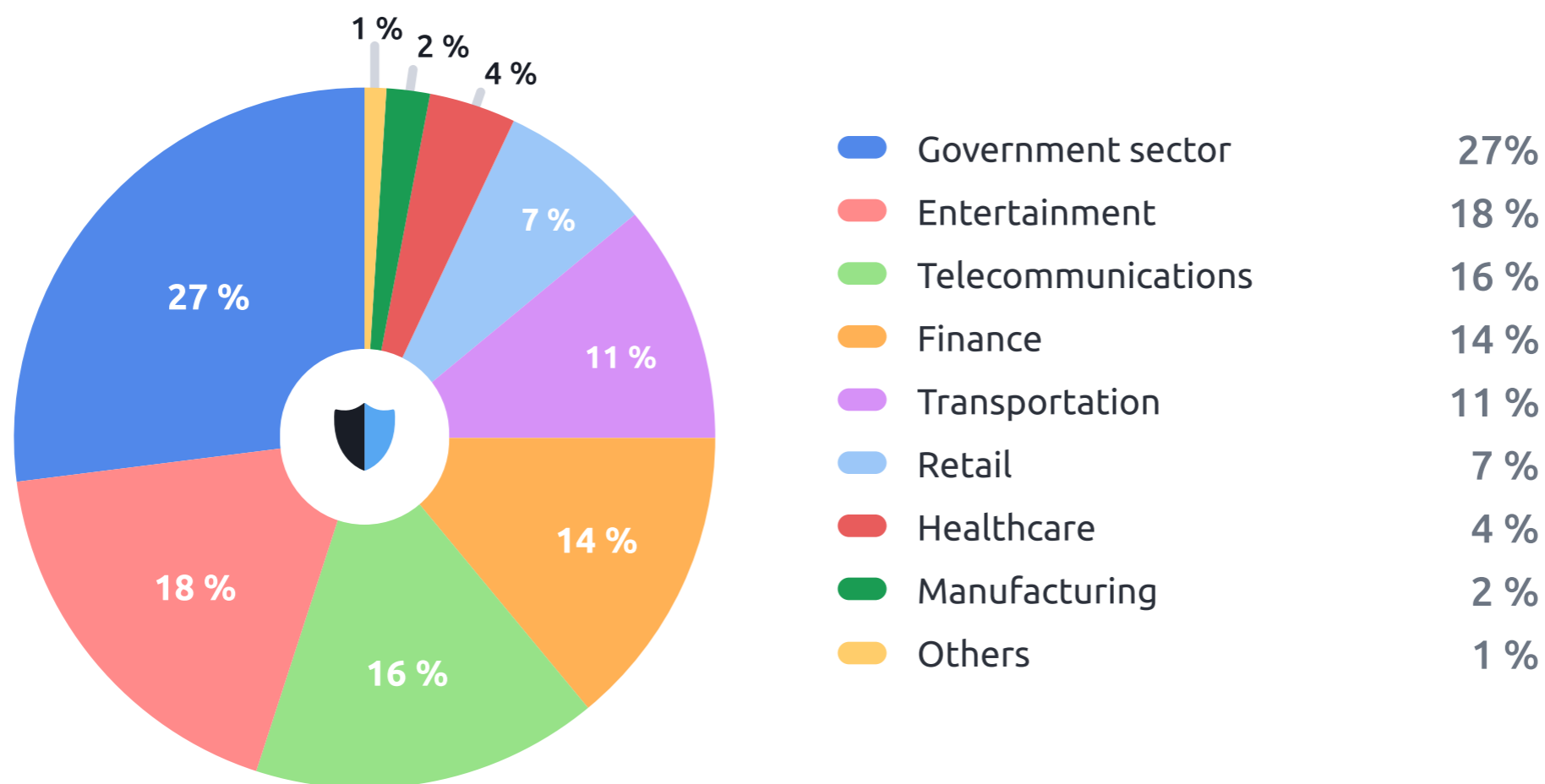
This raises a big question — what can countries do in this landscape, when DDoS attacks come as a tidal wave following geopolitical events?

The Japanese government's reaction was to announce an "active defense" system — a sort of Iron Dome, but against cyber attacks and DDoS. Part of it will involve sharing data on potential attack sources between telecom operators and the government — something the US and UK already do. But as it stands, Japan's data protection and cybercrime laws will need to be changed to make this vision a reality. It's unclear how long this will take.

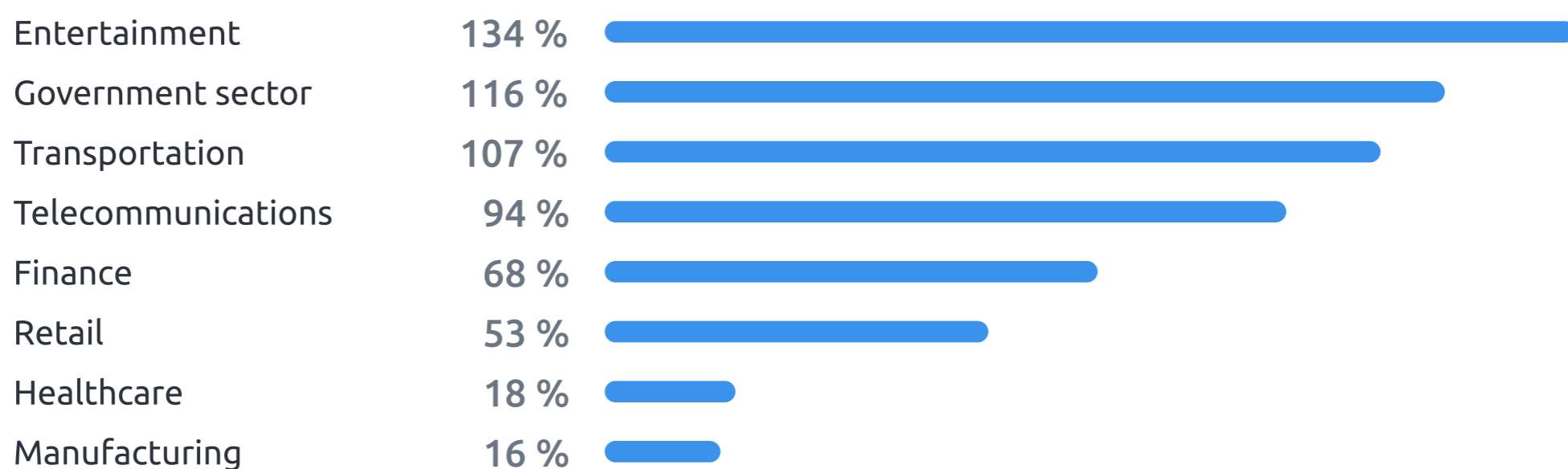
Our view: don't wait for the global security mechanism. We recommend that all companies with online infrastructure look for and implement modern DDoS protection. It will be enough to fend off 99.9% of DDoS attacks.

Attack Share Breakdown by Industry

Here is the distribution of DDoS attacks by vertical in Q2 2024:



Industries with highest YoY growth in DDoS attacks in Q2 2024:



Here are the main trends to highlight this quarter:

- The government sector continues to be the most targeted, and the proportion of attacks here is fairly static – down 1% from 28% in Q1 to 27% in Q2. The same goes for the year-on-year growth, which increased slightly from 114% in Q1 to 116%. As discussed above, this is where we're seeing the impact of geologics and related APT activity.

- The entertainment industry saw a significant shift this quarter. It moved from third place (16%) to second (18%), with year-on-year growth increasing dramatically from 86% in Q1 to 134% in Q2. This surge is particularly evident in attacks on gaming and streaming services, especially in India and Japan.
- The Telecommunications sector went from fourth (14%) to third place (16%) by attack volume. Its year-on-year growth increased from 72% to 94%.
- The finance sector dropped from second (19%) to fourth place (14%). However, its year-on-year growth actually increased from 54% to 68%, suggesting that while attackers may be broadening their targets, the finance sector remains a significant focus.
- Last but not least, transportation is new in the top 5 with 11% of attacks and a 107% year-on-year growth.

Let's break down the standout verticals in more detail.

Government sector

The Government vertical experienced the highest number of attacks at 27% and the second highest year-on-year increase at 116%.

The majority of attacks targeted South Korea and North Korea, both of which held elections in April and June 2024, respectively. Hackers primarily used direct-path attacks, focusing on government agencies and law enforcement infrastructure. Over 30 highly organized and capable APTs (Advanced Persistent Threats) were involved. The largest attack we mitigated in Q2 2024 reached a volume of 1.5 Tbit/s and targeted a client in South Korea. Additionally, the longest attack on a government website lasted over three days, with a continuous load of 700 Gbit/s.

The ability to unleash such firepower comes from botnets. Last year, we observed several trends around botnet usage. Hackers experimented with VM-botnets, using cloud computing to boost the firepower of cells with relatively few devices. However, the trend that ultimately prevailed was simple scaling.

The average number of devices in botnets grew from 6,000 in Q2 2023 to 18,000 in Q2 2024, meaning that, on average, botnets tripled in size. The best countermeasure is to use a DDoS protection service with enough capacity to defend against traffic floods of this magnitude.

Entertainment

The entertainment industry was hit by 18% of DDoS attacks, experiencing the highest year-over-year growth at 134%, even surpassing the government sector.

The gaming subvertical was the biggest target, with hackers particularly focused on esports. One of the primary targets was the LCK, the premier league for "League of Legends," which held playoffs in Korea. According to some participants, DDoS attacks hindered teams' ability to practice and skewed match results, causing some of the strongest teams to depart early.

Another significant incident was a DDoS attack on Final Fantasy 14 servers, which lasted over three days and prevented players from logging in. These attacks cause major player and spectator outflow, which is why criminals use them as leverage to demand ransom payments to stop the attacks.

Telecommunications

The telecommunications sector was the third most targeted vertical, with a 16% share of attacks and a 94% year-on-year increase.

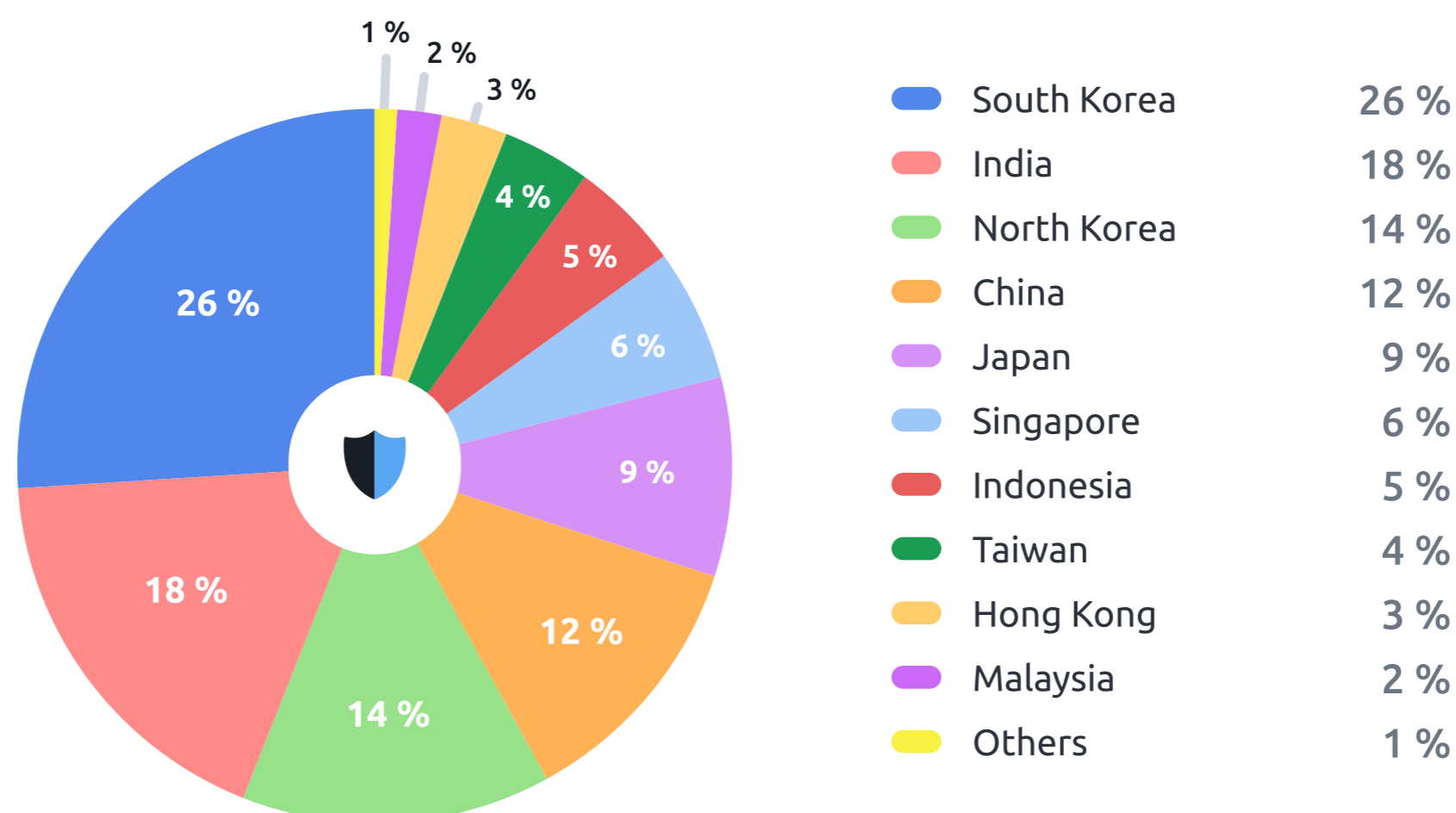
DNS attacks were particularly prevalent in this vertical – they are highly effective against telecom infrastructure because the sector relies heavily on DNS for routing calls, messages, and data traffic.

DNS attacks exploit the UDP protocol used by DNS, which lacks the built-in security mechanisms of TCP. Hackers employed two subtypes of DNS attacks: DNS Amplification and DNS Flood, which overwhelm servers with high volumes of queries for non-existent domains. Both methods exploit the telecom sector's need for high-availability DNS services, effectively turning the infrastructure's strengths into vulnerabilities.

The key to mitigation is intelligently sifting through legitimate traffic while blocking illegitimate requests. StormWall achieves this with an AI algorithm that has near-perfect accuracy. As a result, real users can still access the resource without noticeable latency, even during an attack.

DDoS attacks in APAC: Breakdown by Country

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



This quarter, South Korea saw the most DDoS attacks in the APAC region, holding a 26% share. This was more than India (18%) and China (12%), which have traditionally been the biggest targets, often trading places for the top spot due to their large economies.


However, this year has shown that the size of a country or its economy isn't as influential on its DDoS


threat landscape as active political events. For instance, in Q1, 18% of attacks targeted Taiwan due to its elections.


Although Taiwan was still heavily targeted this quarter with 4% of the total attacks, hackers shifted their focus to South Korea and North Korea, which saw 14% of the attacks. India (18%) and China (12%) remain in the top five most attacked countries, but surprisingly, Japan took the fifth spot with a 9% share of attacks, up from just 2% in Q1.


Conclusions


As we conclude our analysis of DDoS attack trends in the Asia Pacific region for Q2 2024, let's recap the main points:


- 


DDoS attacks in Asia surged by 174% compared to Q2 2023, marking a significant escalation in cyber threats across the region.
- 

Political events, particularly elections in South Korea and North Korea, dramatically shifted the geographic focus of attacks. These countries displaced China in the top 3 most targeted nations, highlighting the strong correlation between geopolitical events and cyber attack patterns.
- 

The entertainment sector, especially gaming, saw the highest year-on-year growth at 134%, followed by government services (116%) and transportation (107%). This shift indicates a broadening of targets by attackers.
- 

Botnet power continued to grow, with the average number of devices in botnets tripling from 6,000 in Q2 2023 to 18,000 in Q2 2024. This escalation
- 

Japan emerged as a new major target, ranking fifth among the most attacked countries with 9% of total attacks, up from 2% in the previous quarter. This surge coincided with Japan's hosting of the G7 summit in May.
- 

The transportation sector experienced an unusually high number of attacks, with a 107% increase, now accounting for 11% of all attacks. This trend suggests cybercriminals are diversifying their targets.
- 

The largest attack mitigated reached a volume of 1.5 Tbit/s, targeting a client in South Korea, while the longest attack on a government website lasted over three days with a continuous load of 700 Gbit/s.

Overall, it's clear that most DDoS attacks come from hacktivists and APTs - these are organized groups with significant resources.

On the positive side, this brings a degree of predictability to attack patterns – where major political events occur, attacks follow. At StormWall, we'll continue to monitor the situation and provide regular updates.