2025 Q4 DDoS threat report: A record-setting 31.4 Tbps attack caps a year of massive DDoS assaults

By Omer YoachimikJorge PachecoCloudforce One

Published: 2026-02-05 · Archived: 2026-04-05 15:03:05 UTC

2026-02-05

7 min read

Welcome to the 24th edition of Cloudflare's Quarterly DDoS Threat Report. In this report, Cloudforce One offers a comprehensive analysis of the evolving threat landscape of Distributed Denial of Service (DDoS) attacks based on data from the Cloudflare network. In this edition, we focus on the fourth quarter of 2025, as well as share overall 2025 data.

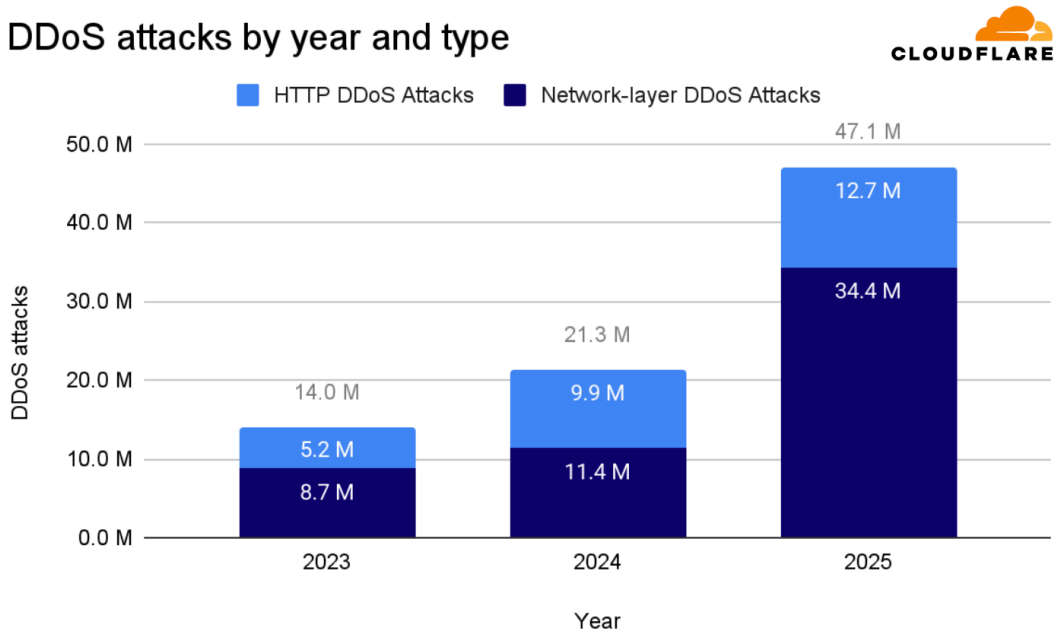
The fourth quarter of 2025 was characterized by an unprecedented bombardment launched by the Aisuru-Kimwolf botnet, dubbed "The Night Before Christmas" DDoS attack campaign. The campaign targeted Cloudflare customers as well as Cloudflare's dashboard and infrastructure with hyper-volumetric HTTP DDoS attacks exceeding rates of 200 million requests per second (rps), just weeks after a record-breaking 31.4 Terabits per second (Tbps) attack.

Key insights

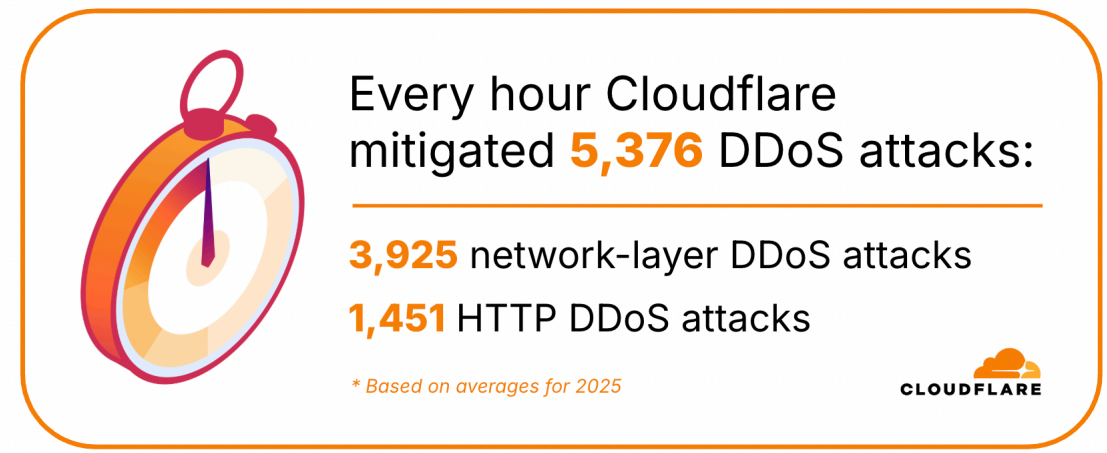
1. DDoS attacks surged by 121% in 2025, reaching an average of 5,376 attacks automatically mitigated every hour.
2. In the final quarter of 2025, Hong Kong jumped 12 places, making it the second most DDoS'd place on earth. The United Kingdom also leapt by an astonishing 36 places, making it the sixth most-attacked place.
3. Infected Android TVs — part of the Aisuru-Kimwolf botnet — bombarded Cloudflare's network with hyper-volumetric HTTP DDoS attacks, while Telcos emerged as the most-attacked industry.

2025 saw a huge spike in DDoS attacks

In 2025, the total number of DDoS attacks more than doubled to an incredible 47.1 million. Such attacks have soared in recent years: The number of DDoS attacks spiked 236% between 2023 and 2025.



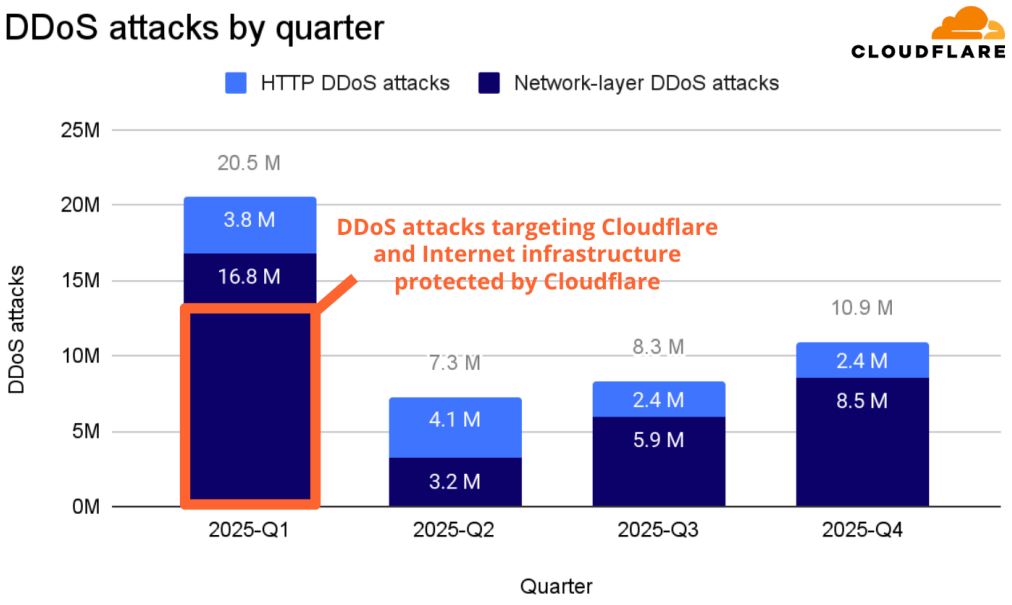
In 2025, Cloudflare mitigated an average of 5,376 DDoS attacks every hour — of these, 3,925 were network-layer DDoS attacks and 1,451 were HTTP DDoS attacks.



Network-layer DDoS attacks more than tripled in 2025

The most substantial growth was in network-layer DDoS attacks, which more than tripled year over year. Cloudflare mitigated 34.4 million network-layer DDoS attacks in 2025, compared to 11.4 million in 2024.

A substantial portion of the network-layer attacks — approximately 13.5 million — targeted global Internet infrastructure protected by Cloudflare Magic Transit and Cloudflare's infrastructure directly, as part of an 18-day DDoS campaign in the first quarter of 2025. Of these attacks, 6.9 million targeted Magic Transit customers while the remaining 6.6 million targeted Cloudflare directly.



This assault was a multi-vector DDoS campaign comprising SYN flood attacks, Mirai-generated DDoS attacks, and SSDP amplification attacks to name a few. Our systems detected and mitigated these attacks automatically. In fact, we only discovered the campaign while preparing our DDoS threat report for 2025 Q1 — an example of how effective Cloudflare's DDoS mitigation is!

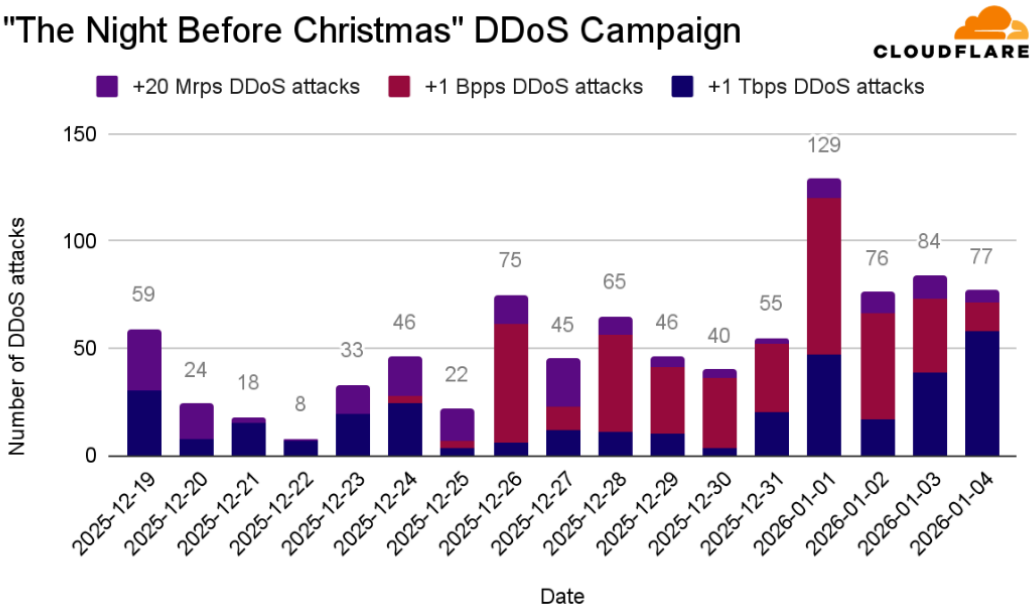
In the final quarter of 2025, the number of DDoS attacks grew by 31% over the previous quarter and 58% over 2024. Network-layer DDoS attacks fueled that growth. In 2025 Q4, network-layer DDoS attacks accounted for 78% of all DDoS attacks. The amount of HTTP DDoS attacks remained the same, but surged in their size to rates that we haven't seen since the HTTP/2 Rapid Reset DDoS campaign in 2023. These recent surges were launched by the Aisuru-Kimwolf botnet, which we will cover in the next section.

"The Night Before Christmas" DDoS campaign

On Friday, December 19, 2025, the Aisuru-Kimwolf botnet began bombarding Cloudflare infrastructure and Cloudflare customers with hyper-volumetric DDoS attacks. What was new in this campaign was its size: The botnet used hyper-volumetric HTTP DDoS attacks exceeding rates of 20 million requests per second (Mrps).

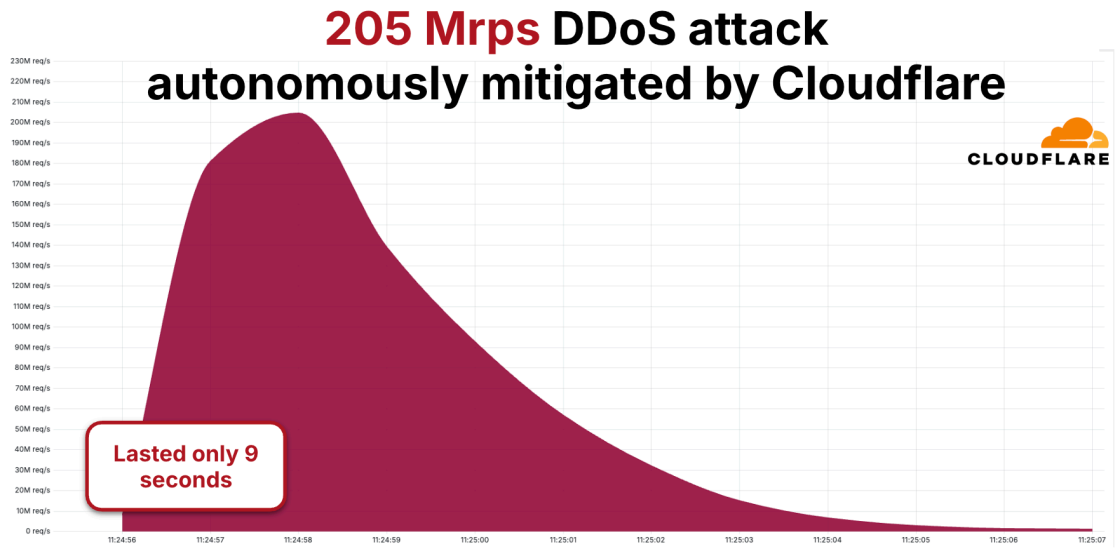
The Aisuru-Kimwolf botnet is a massive collection of malware-infected devices, primarily Android TVs. The botnet comprises an estimated 1-4 million infected hosts. It is capable of launching DDoS attacks that can cripple critical infrastructure, crash most legacy cloud-based DDoS protection solutions, and even disrupt the connectivity of entire nations.

Throughout the campaign, Cloudflare's autonomous DDoS defense systems detected and mitigated all of the attacks: 384 packet-intensive attacks, 329 bit-intensive attacks, and 189 request-intensive attacks, for a total of 902 hyper-volumetric DDoS attacks, averaging 53 attacks a day.



The average size of the hyper-volumetric DDoS attacks during the campaign were 3 Bpps, 4 Tbps, and 54 Mrps. The maximum rates recorded during the campaign were 9 Bpps, 24 Tbps, and 205 Mrps.

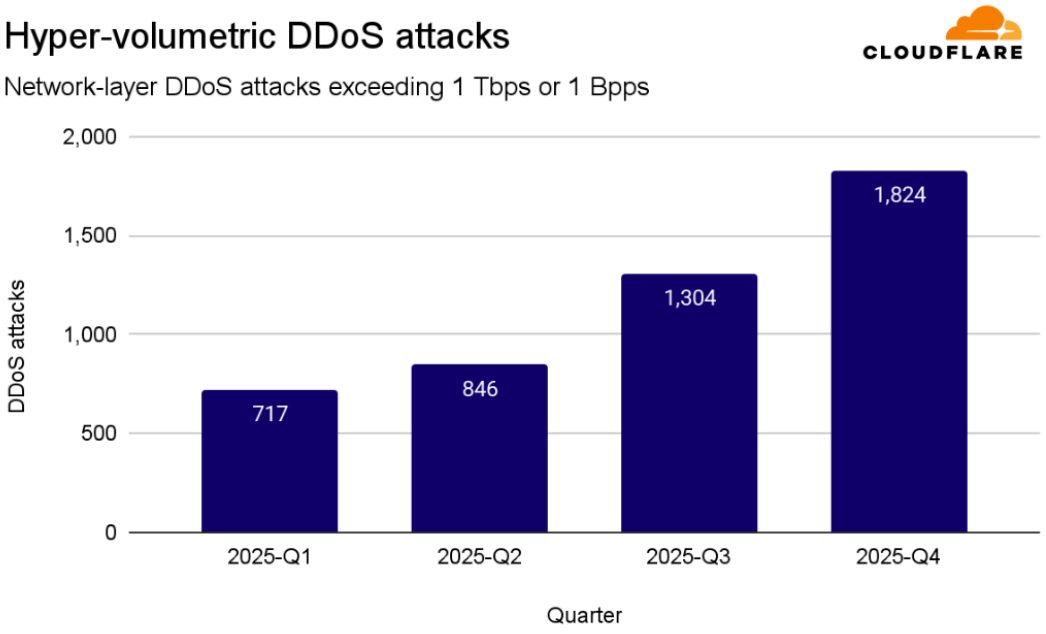
To put that in context, the scale of a 205 Mrps DDoS attack is comparable to the combined populations of the UK, Germany, and Spain all simultaneously typing a website address and then hitting 'enter' at the same second.



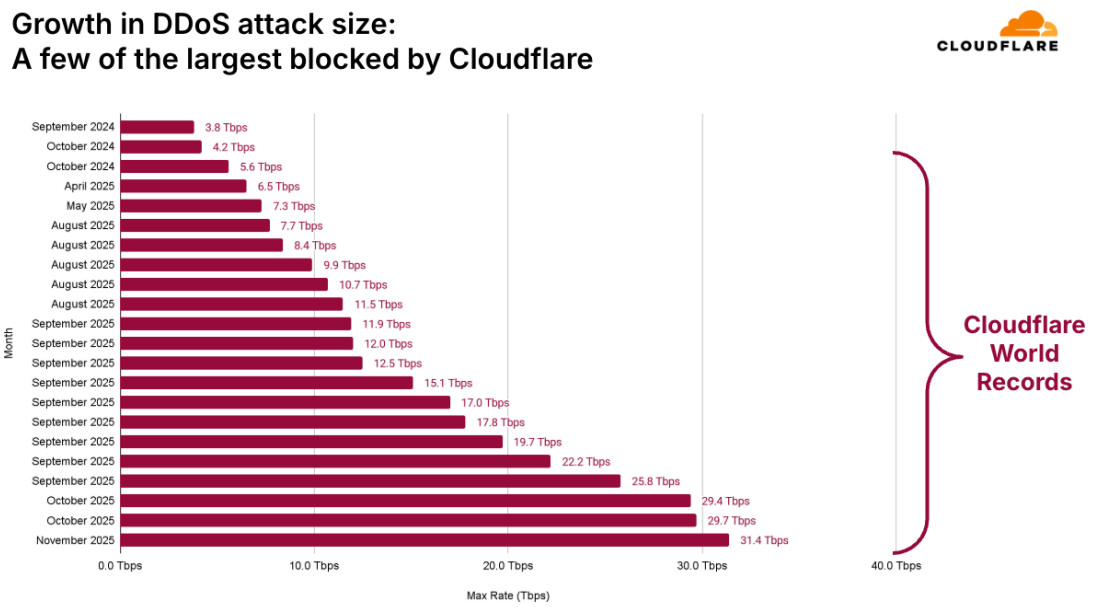
While highly dramatic, The Night Before Christmas campaign accounted for only a small portion of the hyper-volumetric DDoS attacks we saw throughout the year.

Hyper-volumetric DDoS attacks

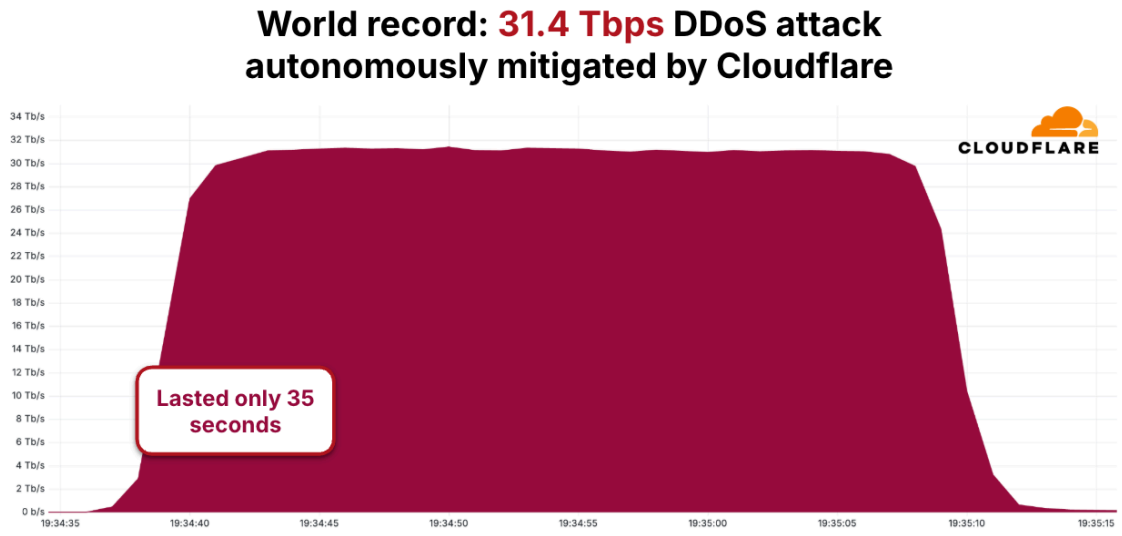
Throughout 2025, Cloudflare observed a continuous increase in hyper-volumetric DDoS attacks. In 2025 Q4, hyper-volumetric attacks increased by 40% compared to the previous quarter.



As the number of attacks increased over the course of 2025, the size of the attacks increased as well, growing by over 700% compared to the large attacks seen in late 2024, with one reaching 31.4 Tbps in a DDoS attack that lasted just 35 seconds. The graph below portrays the rapid growth in DDoS attack sizes as seen and blocked by Cloudflare — each one a world record, i.e. the largest ever disclosed publicly by any company at the time.



Like all of the other attacks, the 31.4 Tbps DDoS attack was detected and mitigated automatically by Cloudflare's autonomous DDoS defense, which was able to adapt and quickly lock on to botnets such as Aisuru-Kimwolf.



Most of the hyper-volumetric DDoS attacks targeted Cloudflare customers in the Telecommunications, Service Providers and Carriers industry. Cloudflare customers in the Gaming industry and customers providing Generative AI services were also heavily targeted. Lastly, Cloudflare's own infrastructure itself was targeted by multiple attack vectors such as HTTP floods, DNS attacks and UDP flood.

Most-attacked industries

When analyzing DDoS attacks of all sizes, the Telecommunications, Service Providers and Carriers industry was also the most targeted. Previously, the Information Technology & Services industry held that unlucky title.

The Gambling & Casinos and Gaming industries ranked third and fourth, respectively. The quarter's biggest changes in the top 10 were the Computer Software and Business Services industries, which both climbed several

spots.

The most-attacked industries are defined by their role as critical infrastructure, a central backbone for other businesses, or their immediate, high-stakes financial sensitivity to service interruption and latency.

Most-attacked locations

The DDoS landscape saw both predictable stability and dramatic shifts among the world's most-attacked locations. Targets like China, Germany, Brazil, and the United States were the top five, demonstrating persistent appeal for attackers.

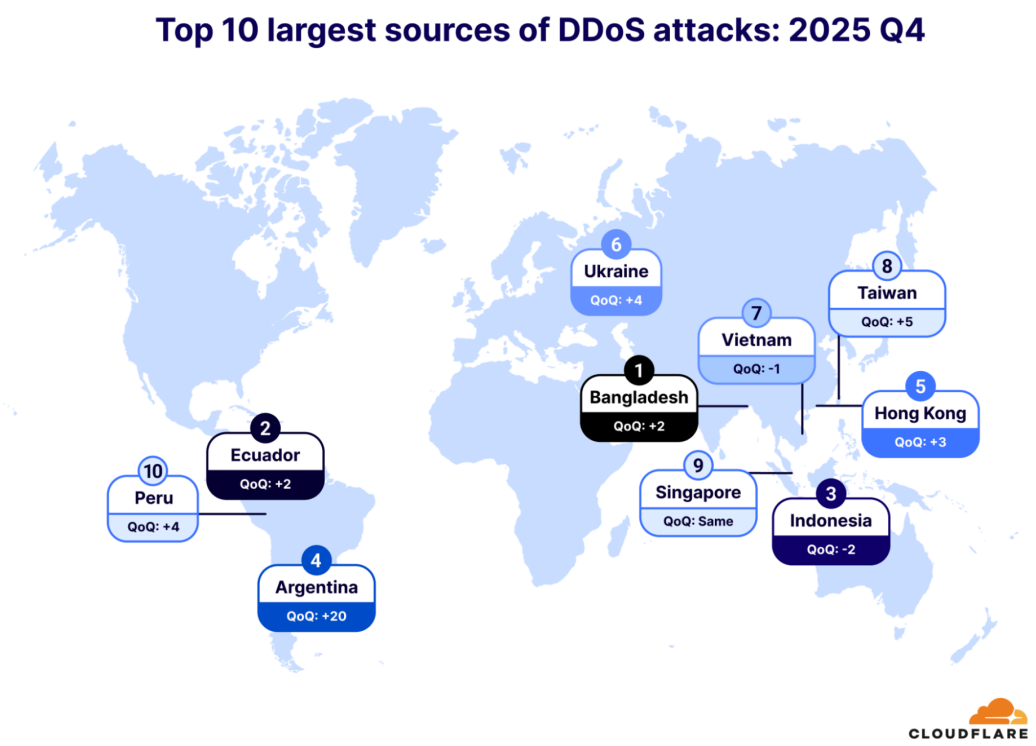
Hong Kong made a significant move, jumping twelve spots to land at number two. However, the bigger story was the meteoric rise of the United Kingdom, which surged an astonishing 36 places this quarter, making it the sixth most-attacked location.

Vietnam held its place as the seventh most-attacked location, followed by Azerbaijan in eighth, India in ninth, and Singapore as number ten.

Top attack sources

Bangladesh dethroned Indonesia as the largest source of DDoS attacks in the fourth quarter of 2025. Indonesia dropped to the third spot, after spending a year as the top source of DDoS attacks. Ecuador also jumped two spots, making it the second-largest source.

Notably, Argentina soared an incredible twenty places, making it the fourth-largest source of DDoS attacks. Hong Kong rose three places, taking fifth place. Ukraine came in sixth place, followed by Vietnam, Taiwan, Singapore, and Peru.

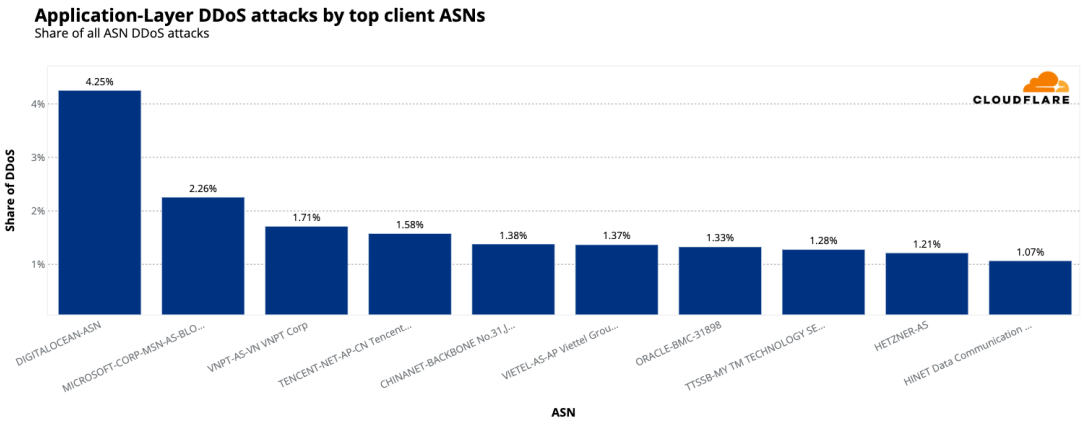


Top source networks

The top 10 list of attack source networks reads like a list of Internet giants, revealing a fascinating story about the anatomy of modern DDoS attacks. The common thread is clear: Threat actors are leveraging the world's most accessible and powerful network infrastructure — primarily large, public-facing services.

We see most DDoS attacks coming from IP addresses associated with Cloud Computing Platforms and Cloud Infrastructure Providers, including DigitalOcean (AS 14061), Microsoft (AS 8075), Tencent (AS 132203), Oracle (AS 31898), and Hetzner (AS 24940). This demonstrates the strong link between easily-provisioned virtual machines and high-volume attacks. These cloud sources, heavily concentrated in the United States, are closely followed by a significant presence of attacks coming from IP addresses associated with traditional Telecommunications Providers (Telcos). These Telcos, primarily from the Asia-Pacific region (including Vietnam, China, Malaysia, and Taiwan), round out the rest of the top 10.

This geographic and organizational diversity confirms a two-pronged attack reality: While the sheer scale of the highest-ranking sources often originates from global cloud hubs, the problem is truly worldwide, routed through the Internet's most critical pathways from across the globe. In many DDoS attacks, we see thousands of various source ASNs, highlighting the truly global distribution of botnet nodes.



To help hosting providers, cloud computing platforms and Internet service providers identify and take down the abusive IP addresses/accounts that launch these attacks, we leverage Cloudflare's unique vantage point on DDoS attacks to provide a free DDoS Botnet Threat Feed for Service Providers.

Over 800 networks worldwide have signed up for this feed, and we've already seen great collaboration across the community to take down botnet nodes.

Helping defend the Internet

DDoS attacks are rapidly growing in sophistication and size, surpassing what was previously imaginable. This evolving threat landscape presents a significant challenge for many organizations to keep pace. Organizations currently relying on on-premise mitigation appliances or on-demand scrubbing centers may benefit from re-evaluating their defense strategy.

Cloudflare is dedicated to offering free, unmetered DDoS protection to all its customers, regardless of the size, duration, or volume of attacks, leveraging its vast global network and autonomous DDoS mitigation systems.

About Cloudforce One

Driven by a mission to help defend the Internet, Cloudforce One leverages telemetry from Cloudflare's global network — which protects approximately 20% of the web — to drive threat research and operational response, protecting critical systems for millions of organizations worldwide.

Cloudflare's connectivity cloud protects entire corporate networks, helps customers build Internet-scale applications efficiently, accelerates any website or Internet application, wards off DDoS attacks, keeps hackers at bay, and can help you on your journey to Zero Trust.

Visit 1.1.1.1 from any device to get started with our free app that makes your Internet faster and safer.

To learn more about our mission to help build a better Internet, start here. If you're looking for a new career direction, check out our open positions.

DDoS ReportsDDoSCloudforce OneSecurityAdvanced DDoSAI

Source: https://blog.cloudflare.com/ddos-threat-report-2025-q4/