Arelion DDoS Threat Landscape Report 2025 Reveals Unprecedented Scale, Sophistication and Sector-Specific Targeting

Peak traffic records shattered as geopolitical tensions and new vectors reshape the threat landscape

Stockholm, June 12, 2025 – Arelion has today announced the publication of its DDoS Threat Landscape Report 2025, offering a detailed analysis of Distributed Denial-of-Service (DDoS) attack trends observed throughout 2024 on its #1 ranked global Internet backbone, AS1299. Drawing on proprietary traffic data, the report examines record-breaking volumetric and packet-rate peaks, evolving attack vectors, sector-specific campaigns and geopolitical forces driving today's cyber-warfare.

Global Conflict and Cyber-Warfare
Geopolitical tensions continued to spill into cyberspace during 2024. The ongoing Ukraine conflict and allied support operations fuelled a substantial rise in DDoS activity across Europe, with Sweden experiencing 2.5x more attacks, Germany 3x and France 5x year-on-year. While Poland saw a relative decline compared to 2023 peaks, the Baltic states and Finland emerged as new focal points, highlighting DDoS as a persistent instrument of hybrid warfare. Beyond Europe, Arelion noted increasing interest from state-linked and hacktivist groups targeting subsea cable infrastructure and other critical Internet assets, signalling a more aggressive phase of cyber-enabled conflict.

Attack Distribution and Intensity

- **Record Volumetric Peaks**
  The average volumetric attack size in 2024 was 23.0 Gb/s - an increase of 97 percent from 2023. October 2024 witnessed the single largest volumetric assault on AS1299 at 1.57 Tbps, marking a 63 percent increase from the previous year. This surge was driven by coordinated TCP SYN and DNS amplification traffic aimed at major US cloud providers. This reflects attackers' ability to marshal greater raw capacity year-on-year, outpacing improvements in network defences.

- **Notable Cloudflare Incident**
  2024 brought one of the most intensive single-target campaigns to date, unleashing 4.2 Tb/s against Cloudflare via a multi-vector TCP SYN + DNS amplification flood. By contrast, the largest single-target strike in 2023 topped out at 960 Gb/s and originated from a UDP-based attack in Europe.

- **Packet-Rate Extremes**

In August 2024, adversaries delivered a peak of 440 Mpps (up from 343 Mpps high in 2023), primarily through UDP floods against leading Asian gaming platforms. The 28 percent rise in packets-per-second peaks demonstrates the shift towards high-velocity, short-burst assaults.

- **Rising Average Packet Rates and Intensities**
  Over the year, the mean packet rate climbed by 24 percent to 6.2 Mpps, reflecting the growing efficiency of high-pps vectors. Meanwhile, the average volumetric size of attacks nearly doubled to 23 Gb/s, even as mean duration remained largely unchanged—demonstrating a deliberate shift towards shorter, high-intensity "blasts" rather than prolonged "carpet-bombing" assaults.

Attack Vectors and Sector Focus

- **Global Attack Vectors**
  When considering AS1299's global traffic, Arelion recorded a relatively even spread of attacks across North America, Europe and Asia, with the United States seeing the largest intensity of DDoS activity of which SYN, UDP and NTP amplification were the most common global attack vectors in 2024. When compared to 2023, there is an even continental spread across North America, Europe and Asia.

- **DNS Amplification Dominance**
  DNS amplification sustained its position as the leading attack vector in 2024, accounting for 55 percent of all amplified traffic despite a slight tapering towards year-end. While still dominant, the drop from 88 percent in 2023 indicates attackers are diversifying into other amplification methods.

- **Carpet Bombing Down**
  Despite its efficacy, carpet bombing activity surprisingly dropped in 2024.

- **Gaming Industry in the Crosshairs**
  The online gaming sector endured sustained DDoS pressure, with one of the largest gaming platforms in the United States suffering the second-largest attack.

Commenting on the report, Mattias Fridström, Chief Evangelist at Arelion, said:

"In 2024, adversaries pushed both scale and sophistication to unprecedented levels. Record-shattering volumetric peaks and high-pps floods demonstrate that DDoS remains a cornerstone of cyber-warfare. Organisations must combine elastic, multi-layered defences—such as on-demand scrubbing, protocol-aware filtering and application-layer intelligence—

with pre-emptive, transparent communications to maximise their chances of preserving stakeholder trust during incidents."

The full report can be downloaded here.

About Arelion

Arelion solves global connectivity challenges for multinational enterprises whose businesses rely on digital infrastructure. On top of the world's #1 ranked IP backbone and a unique ecosystem of cloud and network service providers, we provide an award-winning customer experience to customers in more than 129 countries worldwide. Our global Internet services connect more than 700 cloud, security and content providers with low latency. For further resilience, our private Cloud Connect service connects directly to Amazon Web Services, Microsoft Azure, Google Cloud, IBM Cloud and Oracle cloud across North America, Europe and Asia. Discover more at Arelion.com, and follow us on LinkedIn and X.

Media contacts for Arelion:
Jeannette Bitz, Engage PR
+1 510 295 4972
jbitz@engagepr.com

Arelion
Martin Sjögren, Senior Manager PR and Analyst Relations
+46 (0)707 770 522
martin.sjogren@arelion.com