Arelion's 2026 DDoS report shows Aisuru botnet responsible for nearly one third of DDoS attacks

Surge in hypervolumetric attacks targeting gaming and cloud providers accompanies global rise of AI-driven botnets

Stockholm, July 15, 2026 – Arelion today announced the findings of its latest DDoS threat landscape report, providing insights on global Distributed-Denial-of-Service (DDoS) trends using traffic data from its #1 ranked Internet backbone, AS1299. The report shows that a single botnet, Aisuru, now drives approximately 33 percent of global DDoS attack traffic on Arelion's network. Additionally, DDoS attacks have become hypervolumetric, with record-breaking attacks hitting 6.1 terabits per second (Tbps).

Arelion's report highlights that AI has greatly lowered the barrier to launching complex DDoS attacks, with automated botnets able to overwhelm critical infrastructure within seconds. The Aisuru botnet emerged as the most disruptive DDoS threat of 2025, harnessing more than 500,000 compromised Internet of Things (IoT) devices and Android-based systems to launch record-breaking attacks. Aisuru reached 31.4 Tbps in December 2025 at its peak, making it one of the largest DDoS attacks ever recorded.

Aisuru primarily targeted major gaming and cloud providers, with attacks often exceeding 1 Tbps across Arelion's backbone. By early 2026, KimWolf (Aisuru's variant) had also infected over 2 million Android TV and streaming devices. Attacks of previous years favored smaller, faster packets designed to evade detection, but Aisuru changed that dynamic, combining brute-force volume with multi-vector complexity.

Arelion's report shows that the hypervolumetric DDoS attacks of 2025-2026 mark a new era of cyber threats, mostly driven by automated attacks enabled by AI. These attack volumes often exceed 1 Tbps, totaling billions of packets per second.

Various factors are driving this shift, with IoT proliferation, distributed cloud infrastructure and 5G networks enabling botnets of unprecedented scale to be dispersed across millions of endpoints. The shift of the threat surface from data center servers to home devices has enabled botnets to drive large-scale DDoS attacks from distributed home networks.

Average attack volumes rose significantly, with gigabits per second (Gbps) rising by 22 percent to 6,120 Gbps, million packets per second (Mpps) increasing by 60 percent to 999 Mpps and peak attack traffic in Gbps rising by 290 percent, underscoring the shift to hyperscale-level disruption.

Meanwhile, average attack duration dropped by 20 percent to 8.9 minutes, indicating a trend toward shorter, more frequent "carpet bombing" campaigns. The result is a broader and heavier distribution

across all size categories, placing greater pressure on mitigation strategies designed for lower-intensity threats.

The report also establishes that nation-state actors remain key players in the threat landscape. In 2025, geopolitically motivated attacks persisted across NATO-aligned European nations, most notably Spain and Bulgaria.

The Middle East emerged as a DDoS frontline, with state-aligned groups intensifying DDoS campaigns against critical infrastructure. As state actors have restricted internet access internally while clandestinely backing external cyberattacks, weaponized DDoS attacks have directly and indirectly supported military action on the ground.

Despite hundreds of daily attacks from the Aisuru botnet, Arelion's high-capacity backbone absorbed the malicious traffic with minimal customer disruption, highlighting the importance of network-based mitigation and capacity at scale. In one example, a major online gaming platform sustained multi-vector attacks peaking at several Tbps.

Arelion's always-on, network-level mitigation filtered the malicious traffic and preserved legitimate sessions, helping the platform minimize disruption despite the sheer size of the attack. By stopping malicious traffic within its global backbone before it reaches customer networks, Arelion helps businesses maintain continuity, protect critical applications and strengthen their DDoS defenses as threats continue to evolve.

"AI has shifted the DDoS threat landscape significantly, making it much easier for cybercriminals to launch massive, automated multi-vector attacks with capacities far exceeding anything we've seen before," said Mattias Fridström, Vice President and Chief Evangelist at Arelion. "Attacks are happening at scale, so service providers and enterprises must defend at scale. As attack traffic becomes larger, more distributed and less predictable, organizations require both the capacity and agility to adapt to unexpected traffic patterns. These findings highlight the need for always-on, network-level protection that can absorb massive terabit-scale floods and for coordinated, large-scale mitigation efforts across the Internet's entire ecosystem."

Read the full report here for more information.

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 close to 130 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.

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

Media Contact
Jeannette Bitz, Engage PR
+1 510 295 4972
jbitz@engagepr.com