Analysis of Recent DDoS Attacks

Case Study: The Aisuru 29.6 Tbps Attack (October 2025)

Prepared by: AKHIL NS

October 17, 2025

Contents

1. Overview of Recent DDoS Threats

Distributed Denial of Service (DDoS) attacks continue to evolve in scale and sophistication. Below is a snapshot of five major DDoS incidents reported in 2025:

1. **Aisuru – 29.6 Tbps (October 2025):** Massive TCP-based carpet-bombing attacks targeting gaming platforms and ISPs.
2. **Cloudflare Mitigation – 7.3 Tbps (May 2025):** Short-duration hyper-volumetric attack mitigated by Cloudflare.
3. **Gcore Attack – 6 Tbps (October 2025):** Large volumetric attack neutralized by Gcore's mitigation infrastructure.
4. **Aisuru Early Blasts (May 2025):** Smaller but powerful attacks of 6–11 Tbps observed earlier in the same campaign.
5. **Microsoft/Azure Outage (2025):** Service degradation and downtime linked to heavy DDoS traffic and mitigation issues.

Among these, the **Aisuru 29.6 Tbps attack** stands out as one of the most significant and technically advanced DDoS campaigns ever recorded.

2. Case Study: The Aisuru 29.6 Tbps Attack

2.1 Target

The primary targets were major **online gaming platforms** and associated **Internet Service Providers (ISPs)**. Platforms such as Steam, Riot Games, and PlayStation Network experienced login failures and latency due to severe network congestion.

2.2 Technology and Attack Vectors

- **Botnet-Driven Volumetric Flood:** A large botnet composed of compromised routers and IoT devices generated over 29.6 Tbps of traffic.
- **TCP Carpet-Bombing:** Attackers flooded networks with randomized TCP packets to exhaust bandwidth and overwhelm routers.
- **Direct Traffic (No Reflection):** Unlike traditional amplification attacks, this campaign used direct device-to-target flooding.

2.3 Attacker Motive

- **Disruption:** Likely intended to cause downtime and chaos for high-traffic gaming networks.
- **Botnet Testing:** The campaign may have been a stress test of Aisuru's growing infrastructure.
- **Possible Extortion:** While not confirmed, DDoS attacks of this scale often precede ransom demands.

2.4 Overall Impact

- **Service Outages:** Temporary disruption of login and gameplay services for millions of users.
- **Network Congestion:** Collateral bandwidth saturation across ISPs and cloud providers.
- **Economic Losses:** Increased operational and mitigation costs for service providers.

3. Defense Strategies and Mitigation Techniques

3.1 Network and Traffic Controls

- Deploy **Anycast-based CDN/DDoS scrubbing** to distribute attack load globally.
- Collaborate with ISPs for **BGP blackholing** and upstream filtering.
- Implement **rate limiting, SYN cookies, and connection caps** on public-facing servers.

3.2 IoT and Botnet Prevention

- Enforce **secure defaults** and automatic firmware updates for routers and IoT devices.
- Encourage ISPs to quarantine devices exhibiting DDoS traffic patterns.

3.3 Operational Preparedness

- Maintain **DDoS response playbooks** and conduct regular simulation exercises.
- Establish **real-time traffic monitoring** to detect anomalies early.
- Prepare **legal escalation and evidence logging** procedures for potential extortion cases.

3.4 Long-Term Resilience

- Use multiple cloud and CDN providers to prevent single points of failure.
- Ensure extra **network capacity and redundancy** in high-risk infrastructure.
- Harden control-plane systems (e.g., APIs, dashboards) to prevent internal outages.

4. Summary and Recommendations

The Aisuru 29.6 Tbps attack demonstrates the growing scale and danger of IoT-based botnets. Future defenses must combine **technical controls**, **ISP cooperation**, and **industry-wide IoT hardening**. Organizations—especially gaming and cloud providers—must adopt multi-layered defenses, continuous monitoring, and DDoS readiness planning to stay resilient.

Key References

1. FastNetMon Report on Aisuru Botnet (2025)
2. CSO Online: "Aisuru Botnet Overwhelms ISPs with 29.6 Tbps Flood"
3. KrebsOnSecurity (May 2025): Early Aisuru Activity
4. Cloudflare DDoS Mitigation Report (May 2025)
5. Gcore Security Blog (October 2025)
6. Microsoft Azure DDoS Protection Notes (2025)