Report on Aisuru / October 6, 2025 gaming outages

Title Page

- Prepared for: Mulearn Bootcamp
- Prepared by: Jaseel K
- Date: 2025-10-23

Introduction

This report analyzes the large-scale distributed denial-of-service (DDoS) attack on major gaming networks in early October 2025, attributed to the Aisuru botnet. The purpose is to understand how the attack unfolded, its technical characteristics, potential motives, impact on users and businesses, and effective defensive strategies.

Timeline & targets (what happened)

Around Oct 6–7, 2025, players worldwide reported simultaneous connection and login problems across Steam, Riot Games (League/Valorant), PlayStation Network, Epic Games and others. Downdetector spikes and vendor status pages reflected widespread issues. Reports and threat intel linked these disruptions to a massive DDoS campaign attributed to the Aisuru botnet.

Technical profile (how the attack worked)

Botnet origin & family: Aisuru is described as a Mirai-descended IoT botnet that recruits routers, consumer NAT devices and some cloud instances. Attackers used large numbers of compromised endpoints to generate carpet-bombing TCP/UDP floods and high-pps bursts. Some suppliers reported the attack flowing through ISP backbones with extremely high packet rates. Reported peaks varied across sources (vendor mitigation vs open telemetry): some claims of tens of Tbps appeared in early reporting but those figures are not uniformly corroborated by all mitigators.

Vectors: mixed volumetric UDP/TCP floods, likely including spoofed sources and reflection/amplification where possible; very short duration but very intense “smash-and-grab” bursts consistent with modern DDoS trends.

Likely motive & attribution

Public reporting frames the incident as disruption and capability demonstration rather than a known state-sponsored campaign. The botnet looks criminally operated (Mirai variants are

typically criminal), possibly for bragging, testing, or to prepare for future extortion (ransom DDoS). No credible public attribution to a nation-state at the time of reporting.

Impact (business + user)

User impact: millions of players experienced disconnects, login failures, and disabled ranked play in some titles.

Business impact: reputational harm, potential revenue loss during peak hours, increased mitigation costs and potential compensations to users. ISPs and hosting providers saw backbone stress and had to implement emergency filtering

What mitigations helped or were missing

What worked

- Large DDoS mitigation providers (Cloudflare, Gcore, AWS Shield, etc.) and ISPs used anycast scrubbing, automated signatures, and traffic engineering to absorb/redirect the floods — limiting long outages. Vendor coordination reduced the overall damage.

What could improve

- ISP egress/ingress filtering (BCP 38): reduce spoofing and reflection amplification opportunities. Widespread adoption would limit effectiveness of reflection vectors.
- IoT hardening at scale: manufacturers and ISPs should enforce secure defaults (no default credentials, automatic updates, disable UPnP by default) to shrink botnet recruitment grounds.
- Per-customer layered protection & pricing: game companies should combine regional scrubbing, SYN/UDP cookie protections, and per-session anomaly detection to spot carpet bombs quickly.
- Cross-provider threat intel sharing: faster sharing of malicious IP ranges and behavioral signatures so edge providers can preemptively block.

Concrete defensive checklist for gaming platforms / ISPs

- Provision capacity with multiple upstream scrubbing partners (anycast + on-demand scrubbing).
- Implement adaptive rate limiting and per-session heuristics (drop very high-pps flows, challenge suspicious UDP handshake patterns).
- Use behavioral ML to detect sudden shifts in packet sizes/pps distinct from normal game traffic.

- Enforce BCP 38 across ISP customers and run sinkholing/blackholing playbooks when necessary.
- Collaborate with other major providers (cloud, CDN, ISPs) for coordinated filtering during hyper-volumetric events.

Conclusion

The Aisuru attack demonstrated how botnets built from insecure IoT devices can disrupt large-scale online platforms despite advanced defenses. Continuous IoT hardening, ISP-level filtering, and global cooperation remain essential to reduce the frequency and intensity of such incidents in the future.

References

1. https://www.pcgamer.com/games/todays-steam-outage-may-have-been-part-of-a-massive-ddos-attack-targeting-xbox-playstation-riot-and-other-game-companies/
2. https://www.csoonline.com/article/4071594/aisurus-30-tbps-botnet-traffic-crashes-through-major-us-isps.html
3. https://fastnetmon.com/2025/10/08/another-record-breaking-ddos-aisuru-botnet-suspected-behind-29-69-tbps-gaming-outages