Aisuru DDoS Campaign: Threat Intelligence Assessment

By heavyscientist

Archived: 2026-04-05 16:59:46 UTC

Executive Summary

What's Happening:

- Gaming platforms (Steam, Riot Games, PlayStation Network) experienced major disruptions October 6-7, 2025, suspected but NOT confirmed as DDoS attacks
- The widely-circulated 29.69 Tbps claim is **UNCONFIRMED**—appears only in social media, no mitigation vendor verification
- Confirmed: 22.2 Tbps attack on September 22, 2025 (Cloudflare), largest verified DDoS on record, suspected Aisuru involvement
- Confirmed: 11.5 Tbps attack early September 2025 (Cloudflare), definitively attributed to Aisuru botnet by XLab researchers
- Aisuru: ~300,000-node IoT botnet, capable of sustained multi-terabit attacks, operated by three-person group

Key Findings:

- Attack durations: 35-65 seconds (too short for manual mitigation)
- Dominant vectors: UDP floods (99%+), TCP carpet bombing across IP ranges, short hyper-volumetric bursts
- Mitigation reality: At 20-30 Tbps, only always-on cloud scrubbing with global anycast has proven effective
- Infection vector breakthrough: April 2025 Totolink router firmware supply-chain compromise grew botnet from <100k to 300k+ nodes
- Game publishers face unique challenge: Zero downtime tolerance vs. infrastructure protection trade-offs

Critical Assessment: October 6-7 gaming disruptions are real but lack official DDoS confirmation from victims or mitigation providers. The 29.69 Tbps figure should be treated as unsubstantiated speculation until verified by tier-1 vendors.

Incident Timeline: Last 10 Days

Date (UTC)	Target	Peak Bandwidth	Peak Bpps	Duration	Vectors	Status	Source
Sept 22, 2025	European network infrastructure company	**22.2 Tbps**	**10.6 Bpps**	40 sec	UDP carpet bomb (31,000-47,000 ports/sec)	CONFIRMED	Cloudflare official
Early Sept 2025	Undisclosed (Cloudflare customer)	**11.5 Tbps**	**5.1 Bpps**	35 sec	UDP flood, multi-	CONFIRMED, Aisuru attributed	Cloudflare + XLab

Date (UTC)	Target	Peak Bandwidth	Peak Bpps	Duration	Vectors	Status	Source
					source (IoT + cloud)		
Oct 6, ~00:00 UTC	Steam, Riot Games, PSN, Xbox, Epic, AWS	**29.69 Tbps (UNVERIFIED)**	Unknown	Unknown	TCP carpet bomb (reported)	SUSPECTED, NO official confirmation	Social media only
Oct 6-7, 2025	Riot Games (all platforms)	Unknown	Unknown	36+ hours intermittent	Unknown	Disruption CONFIRMED, DDoS unconfirmed	Riot Games official statement
Oct 6-7, 2025	Steam/Valve	Unknown	Unknown	Intermittent	Unknown	Disruption reported, NO official statement	DownDetector, community reports

Key Context (Just Prior):

- **May 2025**: 7.3 Tbps attack (Cloudflare), 45 seconds, 37.4 TB delivered, 99.996% UDP floods
- **May 12, 2025**: KrebsOnSecurity 6.3 Tbps attack, Google Shield mitigation, confirmed Aisuru by Google

---

Confidence Assessment Table

Claim	Bandwidth	Source	Attribution	Confidence Level	Evidence
29.69 Tbps attack	29.69 Tbps	Social media (X/Reddit)	Aisuru suspected	**UNCONFIRMED**	FastNetMon: "figures remain unverified"; NO vendor confirmation; Cybernews cites "early reports from cybersecurity community"
22.2 Tbps attack	22.2 Tbps	Cloudflare official (X/Twitter)	Aisuru suspected	**CONFIRMED (attack), LIKELY (attribution)**	Cloudflare: "twice as large as anything seen"; SecurityWeek: Cloudflare "believes it may have been powered by Aisuru"; XLab attribution analysis
11.5 Tbps attack	11.5 Tbps	Cloudflare official	Aisuru confirmed	**CONFIRMED**	Cloudflare announcement + XLab detailed technical report with C2 tracking;

Claim	Bandwidth	Source	Attribution	Confidence Level	Evidence
					404,000+ source IPs verified
Oct 6-7 gaming outages	Unknown	Riot Games, community	Unknown	**CONFIRMED (outages), UNCONFIRMED (DDoS cause)**	Riot Games: "intermittent network issues"; NO vendor confirmation of DDoS; NO official statements from Steam, PSN, Xbox
Botnet size: 300k nodes	N/A	XLab CTIA + leaked panels	Aisuru	**CONFIRMED**	XLab telemetry data corroborated with anonymous insider + leaked panel screenshots showing 340k nodes
Totolink supply-chain breach	N/A	XLab + anonymous insider	Aisuru operator "Tom"	**CONFIRMED**	XLab report with technical details; domain updatetoto[.]tw reached Tranco 672,588; malicious script t.sh verified
Cambium cnPilot 0-day	N/A	XLab report (June 2024)	Aisuru exploitation	**CONFIRMED**	XLab contacted vendor with no response; Snort detection rule provided; ongoing exploitation verified

---

Technical Analysis: Aisuru Botnet

Architecture & Composition

Malware Base: Mirai-variant with sophisticated enhancements (Malpedia classification)
Variants: AISURU (Aug 2024) → kitty (Oct 2024) → AIRASHI (Nov 2024-present)
Current Scale: ~300,000 compromised devices (XLab CTIA tracking + leaked panel verification)

Device Infrastructure:

- **Primary (90%+):** Consumer routers (Totolink, D-Link, Linksys, Zyxel), IP cameras, DVRs/NVRs
- **Secondary:** Limited cloud instances (Google Cloud confirmed in 11.5 Tbps attack but "not majority")
- **Geographic concentration:** Brazil, Russia, Vietnam, Indonesia (compromised devices); China, USA, Germany, UK (attack targets)

Infection Vectors

PRIMARY: Supply-Chain Compromise (April 2025)

- **Target:** Totolink router firmware update server

- **Method:** Operator "Tom" compromised update URL, injected malicious script (t.sh)
- **Domain:** updatetoto[.]tw (reached Tranco rank 672,588 within one month)
- **Impact:** Any router performing automatic updates infected; botnet grew <100k → 300k+ nodes
- **Status:** Patched; operators posted "RIP TOTOLINK 2025-2025"

SECONDARY: Exploitation

- **Zero-day:** Cambium Networks cnPilot routers (exploited since June 2024, still active)
- **N-days:** 15+ CVEs spanning 2013-2024 including CVE-2023-28771 (Zyxel ATP), CVE-2023-50381 (Realtek SDK), CVE-2024-3721 (TBK DVR)
- **Credential attacks:** Telnet brute-force with 60+ default credential pairs

Command & Control

C2 Method: DNS TXT record resolution with encrypted payloads
Encryption: Base64 + XOR (key: `ca fe ba be`); earlier versions used Base64 + ChaCha20
Protocol: HMAC-SHA256 + ChaCha20 encryption (AIRASHI variant); custom RC4 variant (key: `PJbiNbbeasddDfsc`)
Infrastructure: 60+ C2 IPs across 19 countries, 10+ ASNs; GRE tunneling via 151.242.2.22-25

Example C2 Domains (mocking security researchers):

- xlabresearch[.]ru, xlabsecurity[.]ru, foxthreatnointel[.]africa, ilovegaysex[.]su

Attack Tactics & Capabilities

Dominant Vectors:

- **UDP floods** (99.996% of 7.3 Tbps attack)—primary weapon for record-breaking attacks
- **TCP SYN floods** (270.52 Mpps observed)
- **DNS amplification** (NTP, QOTD, Echo, RIPv1 reflection/amplification as secondary vectors)
- **TCP carpet bombing** (October 2025, new tactic reported by TCPShield)

"Carpet Bombing" Technique:

- Distributes attack across wide IP ranges (/24, /20, /16 CIDR blocks) simultaneously
- Evades per-host detection thresholds (e.g., 10-50 Mbps per IP × 1000 IPs = 10-50 Gbps aggregate)
- 7.3 Tbps attack: Average 21,925 destination ports/sec, peak 34,517 ports/sec
- **Prevalence:** 75% of all DDoS attacks in 2024 used carpet bombing (Vercara data)

Attack Characteristics:

- **Duration:** 35-65 seconds (hyper-volumetric "hit-and-run" bursts)
- **Frequency:** Several hundred targets hit daily (XLab tracking)
- **Packet rates:** Up to 10.6 Bpps confirmed (22.2 Tbps attack)
- **No industry targeting:** Indiscriminate across gaming, hosting, ISPs, financial services

Demonstrated Capacity:

- **Stable operational:** 1-3 Tbps (advertised on Telegram)
- **Record attacks:** 11.5 Tbps confirmed; 22.2 Tbps suspected; 29.69 Tbps unverified

Operator Profile

Group Structure (XLab anonymous insider):

- **Snow:** Botnet development, malware coding
- **Tom:** Vulnerability research, exploitation (responsible for Totolink breach)
- **Forky:** Business operations, DDoS-for-hire sales

Operational Behavior:

- "Flamboyant" style with taunting messages embedded in malware
- Mock security researchers with C2 domain names
- Attack ISPs "for fun" under ideological pretexts
- DDoS-as-a-Service pricing: $150/day, $600/week (Aug 2024 Telegram)
- New revenue: Residential proxy service (high-bandwidth nodes identified via speed tests)

Evasion & Persistence

Anti-Analysis:

- Detects VMs (VMware, VirtualBox, KVM, QEMU), analysis tools (tcpdump, wireshark)—terminates if found
- Writes `-1000` to `/proc/self/oom_score_adj` (evades Linux OOM Killer)
- Renames binary to `libcow.so`, process to system daemons (telnetd, dhclient, lighttpd)
- Maps shared libraries to resist rival botnet "killer" scripts

Persistence:

- Modifies `/etc/rc.local` for boot persistence
- Does NOT delete binary after execution (unlike typical Mirai variants)

Per-Region Patterns

Attack Sources (7.3 Tbps attack):

- 122,145 source IPs from 5,433 ASNs across 161 countries
- Top sources: Brazil (Telefonica Brazil, 10.5%), Vietnam (Viettel Group, 9.8%), China (China Unicom, 3.9%)
- Near 50% combined from Brazil and Vietnam

Attack Targets:

- Primary: China, USA, Germany, UK, Hong Kong
- AIRASHI variant: Poland, Russia also targeted heavily

Hyperscale Mitigation Playbook (≥20 Tbps, ≥5 Bpps)

Upstream/CDN Layer

What Works at 20-30 Tbps:

Anycast Network Architecture ⭐ PROVEN

- **Capacity requirement:** 200-300+ Tbps total across 200+ PoPs (10x largest expected attack)
- **Deployment:** Already active if pre-deployed; 6-12 months + $10M+ for new infrastructure

- **Real-world proof:** Cloudflare 22.2 Tbps (40 sec), 7.3 Tbps (45 sec)—fully autonomous mitigation
- **First 15 minutes (always-on):** No action needed; monitor dashboards only
- **Trade-offs:** Cloud service $10K-500K/mo vs. self-built (6-12 months, $10M+ capex)

Scrubbing Center Design

- **Always-on cloud scrubbing:** Detection <1 sec, mitigation 0-3 sec ✅ **MANDATORY for 20-30 Tbps**
- **On-demand scrubbing:** 2-5 min activation ❌ **TOO SLOW** (attacks last 40-65 sec)
- **Capacity:** 500 Gbps-1 Tbps per center; need 30-40+ centers for 20+ Tbps aggregate
- **Architecture:** GRE tunnels or anycast symmetric routing
- **First 15 minutes (on-demand):** Initiate BGP route advertisement if not automated
- **Pitfall:** Not testing BGP announcements before attack; incorrect GRE MTU causing fragmentation

Dynamic Routing & Traffic Engineering

- **BGP route control:** Anycast withdrawal, traffic concentration, /24-/26 route specificity
- **Automated vs. manual:** <10 sec automated vs. 30-120 sec manual (manual IMPOSSIBLE at 40-sec attack duration)
- **Prerequisites:** Pre-defined policies triggered on attack signatures

Inter-Provider Signaling

- **BGP communities:** `65535:666` (RTBH blackhole RFC 7999), custom communities per provider
- **FlowSpec:** BGP SAFI 133 for granular filtering rules
- **Limitations:** Requires pre-established relationships; not all providers support customer-triggered RTBH

Network Layer

BGP FlowSpec ⭐ EFFECTIVE FOR UDP/TCP VOLUMETRIC

- **Capabilities:** 12 filter types (source/dest IP, protocol, ports, TCP flags, packet length, DSCP, fragments)
- **When effective:** ✅ UDP floods (DNS, NTP, QOTD), TCP SYN floods; ❌ L7 attacks, encrypted payload inspection
- **Deployment:** 1-3 weeks initial setup; <60 sec rule activation if automated
- **First 15 minutes:** Deploy via FastNetMon, Arbor ATLAS, or custom automation
- **Vendor support:** Cisco ASR/NCS, Juniper MX/PTX, Arista 7500R/7280R, Nokia SR-series
- **Example rule (DNS amplification):**

```
 match: dest 203.0.113.1/32, protocol UDP/17, dest-port 53
action: drop (rate 0)
```

- **Critical pitfall:** Not validating BGP community filters → customers can blackhole entire networks

Remotely Triggered Black Hole (RTBH)

- **Mechanism:** Advertise /32 with BGP community, edge routers rewrite next-hop to null0
- **When effective:** ✅ Single-target volumetric overwhelming transit (buys time for scrubbing setup); ❌ Multi-service hosts (collateral damage), critical always-on services
- **Deployment:** 30-90 sec automated; 5-15 min manual
- **First 15 minutes:** Should auto-trigger via monitoring
- **Critical limitation:** "Success = achieving attacker's goal" (service offline); drops ALL traffic

- **Game publisher vs. ISP:** Publishers use as last resort only (unacceptable downtime); ISPs use commonly (protects infrastructure)

Unicast Reverse Path Forwarding (uRPF)

- **Purpose:** Anti-spoofing, verify source IP legitimacy
- **Modes:** Strict (source reachable via same interface), loose (source exists in routing table)
- **When effective:** ✅ Preventing reflection/amplification FROM your network; ❌ Not effective for attacks targeting you
- **Deployment:** 1-2 weeks (test asymmetric routing), 2-5% CPU increase
- **Best practice:** Loose mode at customer edges, strict mode at single-homed connections

Carpet Bombing Defenses ⭐ CRITICAL FOR 2024-2025 THREAT LANDSCAPE

- **Detection challenge:** Traditional per-host thresholds (25-50 Mbps) don't trigger; 10 Mbps × 1000 IPs = 10 Gbps aggregate
- **What works:**
  - ✅ Context-based detection: Monitor individual IPs AND subnet aggregates simultaneously
  - ✅ Managed Object Misuse alerts: Detect total DDoS across network segment
  - ✅ Precise Protection Prefixes: Divert /25, /26, /27 (not entire /24) to scrubbing
  - ✅ Known Attacker Detection: Block IPs from threat intelligence feeds
- **NETSCOUT/Arbor solution:** Carpet bombing alert thresholds on total misuse, auto-redirect most-specific subnets
- **FlowSpec approach:** Can filter specific vectors (UDP/53 across subnet) but doesn't solve detection
- **Deployment:** 24 hours-30 days for baseline tuning; 5-10 min manual response if pre-tuned

---

L4/L7 Application Layer

SYN Cookies & TCP Hardening

- **Performance:** Handles 1M+ SYN/sec
- **When effective:** ✅ SYN floods <100K SYN/sec; ❌ Not effective for 20-30 Tbps volumetric (bandwidth exhaustion, not state table)
- **Deployment:** Linux `net.ipv4.tcp_syncookies = 1` (default); should already be enabled
- **First 15 minutes:** Pre-configured, no action needed
- **Advanced (Cloudflare):** Statistical analysis of connection patterns, automatic challenge-response

UDP & QUIC Protocol Hardening

- **Challenge:** UDP stateless (no handshake), QUIC encrypted (limited inspection)
- **Defenses:**
  - Rate limiting per source: 100-1000 pps (general), 10K pps (game servers), 1K pps (DNS)
  - Connection limiting: Max concurrent sessions per IP
  - Challenge gates: Probe packet, require response before state allocation
- **QUIC-specific:** Validate connection IDs, rate-limit Initial packets, limit response size until handshake complete

Game Protocol Rate Limiting & Challenge Gates

- **Multi-layer defense:**
  - Connection establishment: 1-5 new connections per IP/minute, require challenge-response before gameplay, exponential backoff

    - In-game rate limiting: 10-100 commands/sec (game-dependent), packet size limits, state validation
    - Burst handling: Allow 5-10 packet bursts, surge queues buffer 100-1000 packets
- **First 15 minutes:**
    1. Increase rate limits 20-50% (accommodate legitimate spikes)
    2. Enable aggressive filtering
    3. Activate standby servers
    4. Geo-block non-player regions

Circuit Breakers & Surge Queues

- **Circuit breaker pattern:** Closed (normal) → Half-Open (testing recovery) → Open (reject new requests)
- **Surge queue:** 1000-10000 request capacity, 5-30 sec timeout, prioritize authenticated > anonymous
- **Game publisher specific:** Match service circuit breaker, login queue during auth floods, asset servers via CDN mandatory

---

Organizational Preparedness

Peering Strategy

- **Multi-homing minimum:** 3 upstreams (2 transit + 1 IXP); best: 5-10 upstreams including Tier 1; hyperscale: 50-100+ peering
- **Capacity planning:** Each link 50-75% of total traffic (N+1 redundancy); example: 100 Gbps normal → 4×50G links (200G capacity)
- **First 15 minutes:** Single link saturated: Emergency AS-prepending; multi-homed: Natural distribution (no action if capacity OK)

Multi-CDN Architecture

- **Strategy:** Primary CDN 70-80% traffic, secondary 20-30% (hot standby), DNS failover 60-300 sec TTL
- **Game publishers:** Static content multi-CDN for patches; dynamic/game single provider (low latency critical); regional optimization

Out-of-Path Scrubbing Model Comparison

Model	Monthly Cost	Activation	Effectiveness at 20-30 Tbps
Always-On Cloud	$10K-500K	Instant	✅ **PROVEN** (22.2 Tbps)
On-Demand	$5K-50K + fees	2-5 min	❌ Too slow (40-65 sec attacks)
Hybrid (on-prem + cloud)	$20K-100K	<100Gbps instant, >100Gbps 2-5min	✅ Works if below threshold
DIY Self-hosted	$50K-200K	N/A	❌ Insufficient capacity

Recommendation: Always-on cloud scrubbing is the **ONLY** viable option for 20-30 Tbps defense.

Incident Runbooks & First 15 Minutes

Time	Action	Owner
0:00	Alert triggered	Automated
0:01	Confirm attack	NOC Tier 1
0:02	Activate automated mitigation	NOC/Security
0:03	Notify Security lead	NOC
0:05	Assess effectiveness	Security team
0:10	Escalate to provider if needed	Security lead
0:10	Begin customer communication	Comms team
0:15	Document in incident log	NOC

Communication Templates:

- Internal: "DDoS attack detected, traffic X% above baseline"
- Customer/Players: "Connectivity issues due to external attack, teams working to resolve"
- Upstream providers: "Under attack, requesting RTBH for [IPs]"

Quarterly Drills:

- Tabletop exercise (decision tree walkthrough)
- Technical drill (test BGP announcements with test prefixes)
- Communication drill (customer/stakeholder messaging)

Game Publisher vs. ISP/CDN Response Differences

Aspect	Game Publisher	ISP/CDN Provider
Downtime tolerance	**0 seconds** (players quit immediately)	Minutes acceptable if infrastructure protected
RTBH usage	**Last resort only**	Commonly used
Mitigation priority	**Precision** (don't block legitimate players)	**Speed** (protect infrastructure)
Typical capacity	10-100 Gbps	1-20+ Tbps
Latency requirements	<50ms critical	<200ms acceptable
Best approach	**Always-on cloud mandatory**	Multiple options viable

---

Priority Implementation Roadmap

Immediate (24 Hours):

- Sign up for cloud DDoS protection (Cloudflare/Akamai/AWS Shield)
- Enable SYN cookies and kernel hardening (`net.ipv4.tcp_syncookies = 1`)
- Configure NetFlow/sFlow exports to monitoring platform

Week 1:

- Establish traffic baselines (Mbps per host, per subnet, total ingress)
- Configure initial FlowSpec rules (test with dry-run mode)
- Test BGP announcements using test prefixes (DO NOT test with production IPs)
- Create communication templates (internal, customer, upstream)

Month 1:

- Deploy always-on scrubbing OR configure on-demand triggers with automation
- Implement automated alerting (per-host 25-100 Mbps, per-subnet 1-5 Gbps, total ingress 75%+ link)
- Conduct first DDoS drill (tabletop exercise)
- Document procedures in incident runbook

Quarter 1:

- Expand to multi-CDN architecture (static content distribution)
- Deploy advanced monitoring (carpet bombing detection, subnet aggregates)
- Conduct technical drill (test BGP failover with non-production prefixes)
- Establish upstream DDoS contacts (get direct phone numbers, escalation paths)

What FAILS at 20-30 Tbps

❌ **Manual intervention:** Attack duration (40-65 sec) < human reaction time → **Solution:** Autonomous detection/mitigation only
❌ **Single-location scrubbing:** Transit saturates before reaching scrubber → **Solution:** Distributed anycast scrubbing
❌ **On-premises appliances:** Typical capacity 10-100 Gbps → **Solution:** Cloud scrubbing or hybrid with overflow
❌ **Static defenses:** Modern attacks shift vectors every 10-30 seconds → **Solution:** Dynamic fingerprinting, adaptive rules
❌ **Reactive scaling:** Auto-scaling takes 3-10 minutes (attack over) → **Solution:** Always-on over-provisioned capacity

---

Key Operational Pitfalls

1. Not testing BGP failover → Manual errors under pressure
2. Insufficient NetFlow sampling → Missed/late detection
3. No baseline traffic profiles → False positive overload
4. Forgetting to document blackholes → Services stay offline
5. Provider doesn't support FlowSpec → Discovered during attack
6. GRE tunnel MTU issues → Fragmentation degrades performance
7. No pre-established provider contacts → Wasting time escalating
8. Assuming long attacks → Missing 60-second attacks
9. Rate limits too aggressive → Blocking legitimate users
10. No carpet bombing playbook → Treating as multiple small attacks

---

Gaps & Unknowns: What to Watch

Critical Information Gaps

October 6-7, 2025 Gaming Incidents:

- **No official DDoS confirmation** from any affected company (Steam, Riot, PSN, Xbox, Epic, AWS)
- **No mitigation vendor data** published by Cloudflare, Akamai, Radware, NETSCOUT
- **29.69 Tbps figure** appears nowhere in official channels—likely exaggerated, aggregated across targets, or fabricated
- **Root cause unknown:** Could be infrastructure issues, routing problems, or smaller-scale DDoS handled internally
- **Riot Games statement:** Acknowledged "intermittent network issues" and "challenges to network stability" but did NOT confirm DDoS

Attribution Uncertainties:

- **22.2 Tbps attack:** Cloudflare "believes it may have been" Aisuru but "yet to determine" definitively
- **October 6-7 incidents:** Aisuru attribution based purely on speculation and timing, no technical fingerprinting published

Technical Unknowns:

- **Exact Cambium cnPilot 0-day details:** XLab withheld to prevent further abuse
- **Full extent of cloud infrastructure usage:** Google Cloud confirmed but proportion unclear
- **TCP carpet bombing by Aisuru:** October 2025 tactic new, technical details limited (reported by TCPShield only)
- **Botnet command structure:** Relationship between operators Snow/Tom/Forky and attack customer selection unknown

What to Monitor Next

Short-Term (Days-Weeks):

- **Vendor disclosures:** Watch for delayed incident reports from Cloudflare, Akamai, AWS Shield Q4 2025 reports (expected Oct-Nov)
- **Victim statements:** Monitor Valve/Steam, Sony, Microsoft investor relations for security incident disclosures
- **XLab updates:** Aisuru attribution analysis for October incidents
- **Botnet size:** Track if Aisuru growth continues post-Totolink patch

Medium-Term (Months):

- **Q3 2025 DDoS reports:** Cloudflare, Akamai, NETSCOUT quarterly threat intelligence (October-November release)
- **New infection vectors:** Watch for additional supply-chain compromises or 0-day exploitation
- **Attack evolution:** Monitor for sustained attacks (>5 minutes) vs. continued short-burst strategy
- **Operator activity:** Telegram DDoS-for-hire channels for Aisuru pricing/capability updates

Likely Next Targets:

- **ISPs and hosting providers:** Aisuru operators stated they attack ISPs "for fun"
- **Financial services:** Emerging target sector in Q2 2025 per Cloudflare
- **Telecommunications:** Most-attacked industry in Q2 2025
- **Gaming platforms:** If October incidents were Aisuru, expect continued targeting

Indicators to Watch:

- **Botnet growth signals:** Tranco rank spikes for suspicious domains (like updatetoto[.]tw jump to 672,588)
- **IoC emergence:** New C2 domains matching xlabresearch[.]ru pattern (mocking security researchers)
- **Vendor firmware compromises:** Similar supply-chain attacks on other router manufacturers
- **Attack size escalation:** 22.2 Tbps is 4x larger than 2024 record (5.6 Tbps)—trend suggests 30+ Tbps attacks feasible

Detection Recommendations

Network-Level Monitoring:

- DNS TXT record queries with Base64 content + XOR key `ca fe ba be`
- GRE tunnel establishment to specific C2 IPs (151.242.2.22-25)
- Short-duration, high-intensity traffic bursts (30-65 seconds)
- UDP flood patterns with port-based carpet bombing (20K-35K ports/sec)

Host-Based Detection (IoT/Router):

- OOM score adjustments to -1000 (`/proc/self/oom_score_adj`)
- Process renames to system daemons (telnetd, dhclient, lighttpd) with binary `libcow.so`
- Speedtest API queries from IoT devices (identifying high-bandwidth nodes for proxy assignment)
- Suspicious network connections to known C2 infrastructure

Threat Intelligence Feeds:

- AISURU IoC tracking: C2 domains, sample hashes, source IP ranges
- Carpet bombing signatures: Subnet-level traffic distribution patterns
- Botnet size tracking: Monitor for growth beyond 300k nodes

References

Primary Authoritative Sources

Cloudflare (DDoS Mitigation Vendor):

- Cloudflare Q2 2025 DDoS Trends Report—7.3 Tbps attack technical details, Q2 statistics
- Cloudflare X/Twitter Official: 22.2 Tbps attack announcement (September 22, 2025)
- Cloudflare Q1 2025 Report: 6.5 Tbps attack, 4.8 Bpps campaign data

XLab/Qianxin (Threat Research):

- XLab Blog: "The Most Powerful Ever? Inside the 11.5Tbps-Scale Mega Botnet AISURU"—Comprehensive technical analysis, C2 infrastructure, operator profiles
- XLab Blog: "Botnets Never Die: An Analysis of the Large Scale Botnet AIRASHI"—AIRASHI variant analysis, Cambium 0-day, encryption protocols

Security Vendors & Threat Intelligence:

- SecurityWeek (Eduard Kovacs, Ionut Arghire): Cloudflare statements on 22.2 Tbps, Aisuru attribution
- KrebsOnSecurity: 6.3 Tbps attack on site, Google Shield mitigation details
- Vercara/DigiCert: "Aisuru Ascending: The Near-Record Attack on Krebs"—Geographic distribution analysis
- NETSCOUT ASERT: Carpet bombing technique analysis (2016-present)
- Malpedia (Fraunhofer FKIE): Aisuru malware family classification

Affected Platforms & Victims:

- Riot Games Official Status Pages: October 6-7 network issues confirmation
- PC Gamer: Riot Games spokesperson Joe Hixson statement ("challenges to network stability")

- DownDetector: October 6 outage spike data for Steam, PSN, Xbox, Epic

Technical Documentation & Standards:

- RFC 5635: Remotely Triggered Black Hole (RTBH) Filtering
- RFC 8955: BGP FlowSpec Dissemination of Flow Specification Rules
- RFC 7999: BLACKHOLE BGP Community for Blackholing
- MANRS (Mutually Agreed Norms for Routing Security): Anti-spoofing best practices

DDoS Mitigation Platforms:

- Akamai Prolexic: 20+ Tbps scrubbing capacity documentation
- AWS Shield Advanced: Hyperscale DDoS protection technical guides
- FastNetMon: Open-source DDoS detection, October 6 unverified 29.69 Tbps note
- NETSCOUT/Arbor ATLAS: Global DDoS threat intelligence, carpet bombing detection

Research & Analysis:

- USENIX Security 2022: "Anycast Agility" research on BGP routing for DDoS mitigation
- NANOG (Network Operators Group): Presentations on hyperscale DDoS defense
- Cybernews, BleepingComputer, The Hacker News, Dark Reading: Secondary reporting on confirmed attacks

Outage Tracking & Community

- DownDetector: Real-time outage reports and user-submitted data
- TCPShield: TCP carpet bomb attack reports (October 6)
- Gaming community forums and subreddits: Symptom reports (login failures, disconnections)

Final Assessment

Confirmed Facts:

- Aisuru is a 300,000-node IoT botnet capable of 11.5+ Tbps attacks (verified)
- 22.2 Tbps attack on September 22, 2025 is largest on record (Cloudflare official)
- Attack durations 35-65 seconds require autonomous mitigation (manual impossible)
- Always-on cloud scrubbing with global anycast is the ONLY proven defense at 20-30 Tbps

High-Confidence Assessments:

- October 6-7 gaming disruptions are real but DDoS cause unconfirmed
- 29.69 Tbps claim is unsubstantiated speculation until vendor verification
- Aisuru likely involved in 22.2 Tbps attack based on fingerprints but not definitively attributed
- Carpet bombing is dominant tactic (75% of 2024 attacks) requiring subnet-level detection

Recommendations:

- **Immediate:** Deploy always-on cloud DDoS protection if not already active
- **Short-term:** Tune carpet bombing detection (subnet aggregates, not just per-host)
- **Ongoing:** Monitor vendor Q4 reports for October incident disclosures, track XLab Aisuru updates
- **Strategic:** Accept that 30+ Tbps attacks are feasible and plan capacity accordingly

---

Complete Citation List

Primary Sources - Cloudflare (Mitigation Vendor)

1. Cloudflare. (2025, September 22). "Cloudflare mitigates new record-breaking 22.2 Tbps DDoS attack." Cloudflare Blog. https://blog.cloudflare.com/
2. Cloudflare. (2025, July). "Defending the Internet: How Cloudflare blocked a monumental 7.3 Tbps DDoS attack." Cloudflare Blog. https://blog.cloudflare.com/defending-the-internet-how-cloudflare-blocked-a-monumental-7-3-tbps-ddos/
3. Cloudflare. (2025, July). "Hyper-volumetric DDoS attacks skyrocket: Cloudflare's 2025 Q2 DDoS threat report." Cloudflare Blog. https://blog.cloudflare.com/ddos-threat-report-for-2025-q2/
4. Cloudflare. (2025). "DDoS threat report for 2025 Q2." Cloudflare Radar. https://radar.cloudflare.com/reports/ddos-2025-q2
5. Cloudflare. (2024). "How Cloudflare auto-mitigated a world record 3.8 Tbps DDoS attack." Cloudflare Blog. https://blog.cloudflare.com/how-cloudflare-auto-mitigated-world-record-3-8-tbps-ddos-attack/
6. Cloudflare. (2025). "Famous DDoS attacks | Biggest DDoS attacks." Cloudflare Learning Center. https://www.cloudflare.com/learning/ddos/famous-ddos-attacks/
7. Cloudflare. (2025). "What is a distributed denial-of-service (DDoS) attack?" Cloudflare Learning Center. https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

Primary Sources - XLab/Qianxin (Threat Research)

8. XLab Threat Intelligence Center. (2025). "The Most Powerful Ever? Inside the 11.5Tbps-Scale Mega Botnet AISURU." Qianxin XLab Blog. https://blog.xlab.qianxin.com/super-large-scale-botnet-aisuru-en/
9. XLab Threat Intelligence Center. (2025). "Botnets Never Die: An Analysis of the Large Scale Botnet AIRASHI." Qianxin XLab Blog. https://blog.xlab.qianxin.com/large-scale-botnet-airashi-en/
10. APNIC Blog. (2025, March 13). "Botnets never die." Asia-Pacific Network Information Centre. https://blog.apnic.net/2025/03/13/botnets-never-die/

Security News & Analysis - Tier 1

11. Kovacs, E. (2025, September). "Record-Breaking DDoS Attack Peaks at 22 Tbps and 10 Bpps." SecurityWeek. https://www.securityweek.com/record-breaking-ddos-attack-peaks-at-22-tbps-and-10-bpps/
12. Arghire, I. (2025, September). "Cloudflare mitigates new record-breaking 22.2 Tbps DDoS attack." BleepingComputer. https://www.bleepingcomputer.com/news/security/cloudflare-mitigates-new-record-breaking-222-tbps-ddos-attack/
13. BleepingComputer. (2025, September). "Cloudflare blocks largest recorded DDoS attack peaking at 11.5 Tbps." https://www.bleepingcomputer.com/news/security/cloudflare-blocks-record-breaking-115-tbps-ddos-attack/
14. Krebs, B. (2025, May 12). "KrebsOnSecurity Hit With Near-Record 6.3 Tbps DDoS." Krebs on Security. https://krebsonsecurity.com/2025/05/krebsonsecurity-hit-with-near-record-6-3-tbps-ddos/

15. The Hacker News. (2025, September). "Tech Overtakes Gaming as Top DDoS Attack Target, New Gcore Radar Report Finds." https://thehackernews.com/2025/09/tech-overtakes-gaming-as-top-ddos.html

Security News & Analysis - Tier 2

16. CyberSecureFox. (2025, September). "Cloudflare Thwarts Record 22.2 Tbps DDoS As Botnet Firepower Surges." https://cybersecurefox.com/en/cloudflare-thwarts-record-22-2-tbps-ddos-aisuru-botnet/

17. CyberInsider. (2025, September). "Cloudflare Mitigated Record-Breaking 22.2 Tbps DDoS Attack." https://cyberinsider.com/cloudflare-mitigated-record-breaking-22-2-tbps-ddos-attack/

18. Cyber Security News. (2025, September). "22.2 Tbps DDoS Attack Breaks Internet With New World Record." https://cybersecuritynews.com/ddos-attack-world-record/

19. Cyber Security News. (2025, September). "AISURU Botnet With 300,000 Hijacked Routers Behind The Recent Massive 11.5 Tbps DDoS Attack." https://cybersecuritynews.com/aisuru-botnet-with-300000-hijacked-routers/

20. GBHackers. (2025, September). "AISURU Botnet Fuels Record-Breaking 11.5 Tbps DDoS Attack With 300,000 Hijacked Routers." https://gbhackers.com/aisuru-botnet/

21. GBHackers. (2025, September). "Massive 22.2 Tbps DDoS Attack Sets New World Record." https://gbhackers.com/massive-22-2-tbps-ddos-attack/

22. Security Affairs. (2025, September). "Cloudflare mitigates largest-ever DDoS attack at 22.2 Tbps." https://securityaffairs.com/182521/security/cloudflare-mitigates-largest-ever-ddos-attack-at-22-2-tbps.html

23. Security Online. (2025). "AISURU Botnet: From Record-Breaking DDoS to Residential Proxy Empire." https://securityonline.info/aisuru-botnet-from-record-breaking-ddos-to-residential-proxy-empire/

24. Cyber Press. (2025). "AISURU's 300,000 compromised routers unleashed an 11.5 Tbps global DDoS storm." https://cyberpress.org/aisuru-ddos-attack/

25. NPAV Security Blogs. (2025). "Unveiling AISURU: The 11.5 Tbps Mega Botnet Behind Record-Breaking DDoS Attacks and Totolink Router Compromise." https://blogs.npav.net/blogs/post/unveiling-aisuru-the-115-tbps-mega-botnet-behind-record-breaking-ddos-attacks-and-totolink-router-co

Gaming Industry & Affected Platforms

26. Marshall, C. (2025, October 7). "Today's Steam outage may have been part of a massive DDoS attack targeting Xbox, PlayStation, Riot, and other game companies." PC Gamer. 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/

27. Cybernews. (2025, October 6). "Major gaming platforms hit by disruptions: unprecedented DDoS suspected." https://cybernews.com/security/steam-riot-gaming-services-hit-by-disruptions-ddos-suspected/

28. GosuGamers. (2025, October 6). "Steam, PlayStation, Xbox, Riot Games and Epic outage sparks concerns of coordinated DDoS attack." https://www.gosugamers.net/entertainment/news/77434-steam-playstation-xbox-riot-games-and-epic-outage-sparks-concerns-of-coordinated-ddos-attack

29. FastNetMon. (2025, October 8). "Another record-breaking DDoS? Aisuru botnet suspected behind 29.69 Tbps gaming outages." https://fastnetmon.com/2025/10/08/another-record-breaking-ddos-aisuru-botnet-suspected-behind-29-69-tbps-gaming-outages/

30. PlayStation LifeStyle. (2025, September 4). "PSN Partially Down for Some Users." https://www.playstationlifestyle.net/2025/09/04/psn-outage-september-4-2025/

DDoS Mitigation Vendors & Technical Analysis

31. Vercara/DigiCert. (2025, May). "Aisuru Ascending: The Near-Record Attack on Krebs and What It Means for You." https://vercara.digicert.com/resources/aisuru-ascending-the-near-record-attack-on-krebs-and-what-it-means-for-you

32. Vercara/DigiCert. (2024). "2024: Year of the Carpet Bomb in DDoS." https://vercara.digicert.com/resources/2024-year-of-the-carpet-bomb-in-ddos

33. NETSCOUT ASERT. (2024). "Carpet-Bombing." NETSCOUT Blog. https://www.netscout.com/blog/asert/carpet-bombing

34. NETSCOUT. (2024). "Carpet Bombing DDoS Protection." NETSCOUT Solutions. https://www.netscout.com/solutions/carpet-bombing-protection

35. NSFOCUS Global. (2024). "A Deep Dive into DDoS Carpet-Bombing Attacks." https://nsfocusglobal.com/a-deep-dive-into-ddos-carpet-bombing-attacks/

36. Tata Communications. (2024). "Rise of Carpet Bombing Attacks: DDoS Threats and Defense." https://www.tatacommunications.com/knowledge-base/ddos/rise-of-carpet-bombing-attacks

37. Akamai. (2025). "What Is Blackhole (RTBH) Routing? | How Does Blackholing Work?" Akamai Glossary. https://www.akamai.com/glossary/what-is-blackhole-routing

BGP FlowSpec & Network Mitigation

38. Kentik. (2025). "What Is Adaptive Flowspec and Does It Solve the DDoS Problem?" Kentik Blog. https://www.kentik.com/blog/what-is-adaptive-flowspec-and-does-it-solve-the-ddos-problem/

39. FastNetMon. (2025, February 10). "BGP Flow Spec for DDoS Mitigation." https://fastnetmon.com/2025/02/10/bgp-flow-spec-for-ddos-mitigation/

40. FastNetMon. (2024, December 7). "BGP Blackhole Automation for DDoS mitigation." https://fastnetmon.com/2024/12/07/bgp-blackhole-automation-for-ddos-mitigation/

41. FastNetMon. (2025). "FlowSpec DDoS Mitigation with FastNetMon." https://fastnetmon.com/flowspec-ddos-mitigation/

42. Equinix. (2025). "Offload DDoS mitigation to your provider's high-capacity network with BGP Flowspec." https://deploy.equinix.com/blog/how-to-use-bgp-flowspec-to-filter-and-mitigate-ddos-attacks/

43. Noction. (2025). "DDoS Mitigation and BGP Flowspec." https://www.noction.com/blog/ddos-mitigation

44. Cisco Blogs. (2025). "DDoS Mitigation for Modern Peering." https://blogs.cisco.com/sp/ddos-mitigation-for-modern-peering

45. NANOG. (2014). "DDoS Mitigation Using BGP Flowspec." Presentation Archive. https://archive.nanog.org/sites/default/files/tuesday_general_ddos_ryburn_63.16.pdf

46. Kentik. (2025). "How to Configure Remotely Triggered Black-Hole Routing with Kentik Detect." Kentik Blog. https://www.kentik.com/blog/how-to-rtbh-with-kentik-detect/

47. A10 Networks. (2025). "Remotely Triggered Black Hole Routing." https://www.a10networks.com/resources/videos/remotely-triggered-black-hole-routing/

48. SENKI. (2025). "Remote Triggered Black Hole (RTBH) Filtering." https://www.senki.org/operators-security-toolkit/remote-triggered-black-hole-rtbh-filtering/

Technical Standards & RFCs

49. IETF. (2009). "RFC 5635 - Remote Triggered Black Hole Filtering with Unicast Reverse Path Forwarding (uRPF)." https://datatracker.ietf.org/doc/html/rfc5635

50. IETF. (2010). "RFC 8955 - Dissemination of Flow Specification Rules." https://datatracker.ietf.org/doc/html/rfc8955

51. IETF. (2016). "RFC 7999 - BLACKHOLE BGP Community for Blackholing." https://datatracker.ietf.org/doc/html/rfc7999

Malware Analysis & Threat Intelligence

52. Malpedia (Fraunhofer FKIE). (2025). "Aisuru (Malware Family)." https://malpedia.caad.fkie.fraunhofer.de/details/elf.aisuru

53. Wikipedia. (2025). "Mirai (malware)." https://en.wikipedia.org/wiki/Mirai_(malware)

54. Owlysec. (2024). "Hackers Leverage Undisclosed Zero-Day Flaw in cnPilot Routers to Propagate AIRASHI DDoS Botnet." https://owlysec.com/vulnerabilities/hackers-leverage-undisclosed-zero-day-flaw-in-cnpilot-routers-to-propagate-airashi-ddos-botnet

55. FastNetMon. (2025, January 24). "Cybercriminals Leverage Zero-Day Vulnerability to Launch AIRASHI DDoS Botnet." https://fastnetmon.com/2025/01/24/cybercriminals-leverage-zero-day-vulnerability-to-launch-airashi-ddos-botnet/

56. Hackread. (2025, May). "KrebsOnSecurity Hit with 6.3 Tbps DDoS Attack via Aisuru Botnet." https://hackread.com/krebsonsecurity-6-3-tbps-ddos-attack-aisuru-botnet/

Cloud Provider & CDN Services

57. Global Secure Layer. (2025). "DDoS Protection." https://globalsecurelayer.com/ddos-protection

58. Medium (Tillu, J.). (2024). "How AWS Shield Protects You From DDoS?" https://jaytillu.medium.com/how-aws-shield-protects-you-from-ddos-94bd3d933d6d

Additional Industry Sources

59. Tom's Hardware. (2025, September). "Cloudflare blocks record-setting 11.5Tbps DDoS attack two months after the previous record-setting DDoS attack." https://www.tomshardware.com/tech-industry/cyber-security/cloudflare-blocks-record-setting-11-5tbps-ddos-attack-two-months-after-the-previous-record-setting-ddos-attack

60. TechRadar. (2025, September). "Cloudflare blocked massive 22.2Tbps DDoS attack, surpassing 11.5Tbps record set just weeks earlier." https://www.techradar.com/pro/security/cloudflare-says-it-has-once-again-blocked-the-largest-ever-ddos-attack-in-history

61. PC Gamer. (2025, September). "Cloudflare mitigates yet another record-breaking DDoS attack—which, at 22.2 Tbps, makes it nearly twice as big as the last hyper-volumetric attack." https://www.pcgamer.com/hardware/cloudflare-mitigates-yet-another-record-breaking-ddos-attack-which-at-22-2-tbps-is-nearly-twice-as-big-as-the-last-hyper-volumetric-attack/

62. HotHardware. (2025, September). "Cloudflare Blocks Massive 22.2 Tbps DDoS Attack Twice As Big As Anything Seen Before." https://hothardware.com/news/cloudflare-blocks-massive-222-tbps-ddos-attack

63. Slashdot. (2025, May). "KrebsOnSecurity Hit With Near-Record 6.3 Tbps DDoS." https://tech.slashdot.org/story/25/05/20/2215258/krebsonsecurity-hit-with-near-record-63-tbps-ddos

64. Fullerton College Cybersecurity Center. (2025, May 20). "KrebsOnSecurity Hit With Near-Record 6.3 Tbps DDoS." https://cybersecurity.fullcoll.edu/2025/05/20/krebsonsecurity-hit-with-near-record-6-3-tbps-ddos/

65. 0xzx. (2025, May). "IoT Botnet Aisuru Exploits Recent Records to Launch DDoS Attack on Krebsonsecurity Website." https://0xzx.com/en/20250522001455234O2.html

---

Report Compiled: October 9, 2025
Intelligence Assessment Level: MEDIUM-HIGH CONFIDENCE (Confirmed attacks, unconfirmed attributions)
Next Review: October 15, 2025 (Post-vendor Q3 report releases)
