TASK 7: Analyzing the Bimodal Threat of 2025 DDoS Attacks

Maheshwar Anup

Executive Summary

The DDoS threat landscape in 2025 has polarized into two critical, complementary extremes: **hyper-volumetric assaults** (Layer 3/4) that utilize massive, commercially-available IoT botnets like Aisuru to push record-breaking traffic (up to 22.2 Tbps [1]), and **hyper-surgical strikes** (Layer 7) that exploit subtle application protocol flaws (like HTTP/2 Rapid Reset) to achieve severe resource exhaustion with deceptive stealth.[3] This bimodal threat requires defense strategies to shift away from manual, reactive measures toward autonomous, AI-driven mitigation platforms supported by proactive architectural hardening and effective egress control.[5] The data suggests the primary objective has moved from mere random destruction to calculated disruption aimed at competitive advantage, financial extortion, and the strategic erosion of public trust [[21]],.

---

1. Analysis of Technological Trends: The Hyper-Scale and the Surgical Strike (Addressing Q1)

The comparison across the five incidents immediately reveals a fundamental shift away from "classic" DDoS—which often relied on easily blocked reflection or simple SYN floods—to a bimodal strategy prioritizing either protocol exploitation or hyper-volumetric evasion.[7] This evolution means defenders must simultaneously prepare for two fundamentally different types of siege: saturation and resource exhaustion.

Comparison Table: Technology and Critical Metrics

Incident	Target Sector	Primary Technology/Vector	Critical Performance Metric	Attacker Priority
#1 (Jan)	E-Commerce Retail	HTTP/2 Rapid Reset (L7)	6 Million RPS (Requests/Sec) over 2+ hours [4]	Stealthy, High Concurrency, Server Exhaustion
#2 (Feb)	Government Agency	HTTP/2 Rapid Reset (L7)	10 Million RPS for 14 hours	Endurance, Resource Exhaustion, Prolonged Disruption
#3 (Mar)	U.S. Beverage Co.	Rapid-Fire Botnet Requests (L7/L4)	13.5 Million RPS in 8 minutes [4]	Speed, "Flash DDoS" Effectiveness, Proof-of-Attack
#4 (May)	Hosting Provider	Multi-Vector (UDP, NTP, Mirai)	7.3 Tbps for 45 seconds [1]	Hyper-Volume, Protocol Diversity, Saturation
#5 (Sept)	Network Infra Co.	Aisuru-fueled UDP Carpet Bomb (L3/4)	22.2 Tbps & 10.6 Bpps (40 seconds) [1]	Scale, Evasion (47k ports) [1], Unprecedented Saturation

The Two Most Concerning Technological Trends

1. **Protocol Exploitation for Resource Exhaustion:** Incidents #1 and #2 demonstrate that high-impact attacks no longer require raw bandwidth to be successful. The HTTP/2 Rapid Reset technique exploits a flaw in the application protocol's logic (using RST_STREAM frames) to generate millions of requests from relatively few connections, consuming

disproportionately high CPU and thread pool resources on the origin server.[3] This vector is concerning because it mimics legitimate user behavior, challenging traditional rate-limiting and simple volumetric filtering heuristics.[9] The priority of modern botnet operators here is **concurrency and stealth**.

2. **Volumetric Evasion via Carpet Bombing:** Incident #5 epitomizes the hyper-volumetric threat (22.2 Tbps) [2], but its sophistication lies in its distribution: a **UDP Carpet Bomb** targeting up to 47,000 ports on a single IP.[1] This is designed to defeat legacy defenses.[11] By distributing the malicious load across a vast array of ports, the traffic volume on any single port often falls below the established local trigger thresholds for mitigation. The priority is **evasion and unprecedented scale** achieved by weaponizing compromised, high-bandwidth IoT devices.[10]

---

2. Analysis of Target Selection and Impact Profile (Addressing Q2)

The breadth of targets—from consumer e-commerce (#1), to government portals (#2), to network infrastructure (#5)—suggests there is no single "ideal" DDoS victim in 2025.[14] Instead, attackers target the most vulnerable **choke points** across the digital economy to maximize downstream disruption.[2]

Investigating Real-World Consequences

- **Incident #2 (Indonesian Government Agency):** The 14-hour siege on a public service portal, which citizens rely on for vital information, extends the impact far beyond technical downtime. The real-world consequence is a societal one: the **erosion of public trust and state legitimacy**,.[14] While direct economic losses are difficult to tally, the inability of citizens to access essential services (analogous to the airport disruptions seen in similar regional attacks) fuels social unrest and highlights governance concerns, particularly amid existing economic instability,. The prolonged duration forces the government into a state of continuous recovery, signifying operational failure.[4]
- **Incident #5 (European Network Infrastructure Company):** Although the 40-second attack was successfully mitigated [1], the potential real-world consequence was catastrophic: the **crippling of regional online platforms, financial systems, or utilities** reliant on the backbone provider's connectivity.[16] The attack's scale (22.2 Tbps) immediately underscores a gap in global preparedness [16] and creates a chill on market

confidence in cloud reliance.[2] The impact is an intangible one—fear—which forces global defense spending to accelerate.[17]

Destruction or Disruption?

The evidence suggests that modern DDoS attacks are primarily about **disruption**.[14]

- The hyper-volumetric bursts (#3, #4, #5) are designed to prove the capacity for **destruction** (saturation), but their short duration often minimizes total downtime.[18] This shock-and-awe tactic is used as leverage, not for simple annihilation.
- The prolonged L7 attacks (#1, #2) focus on sustained, crippling **disruption** to service availability and reputation [4], aiming to exhaust resources slowly over hours rather than seconds.[4]

The goal is to use the massive technical capability as a strategic tool to compel a reaction, whether that is a ransom payment, a loss of market share, or a political failure.[20]

---

3. Analysis of Motives and Attribution (Addressing Q3)

The common lack of public attribution in these 2025 cases, particularly for the record-breaking events, is a hallmark of the DDoS-as-a-Service (DaaS) model.[22] The monetization of massive IoT botnets like Aisuru has blurred the line between hacktivism, cybercrime, and state-sponsored activity.[15]

Attribution Challenges: The Rise of Aisuru

The Aisuru botnet (linked to Incidents #4 and #5, with capabilities derived from the Mirai lineage [13]) is the quintessential example of the commercialization of chaos.[15] Aisuru's massive power—estimated at over 300,000 compromised IoT devices worldwide [17]—is available for hire via platforms like Telegram.[15]

This democratization of massive attack power complicates traditional assumptions about

attribution.[23] The actual user commanding the 22.2 Tbps flood might be a competitor, a disgruntled customer, a hacktivist, or a state actor [20]—all paying the same DaaS operator for guaranteed volumetric service.

Motive Mapping for Specific Incidents

Incident	Most Likely Motive	Rationale and Context
#1 (French Retailer)	**Competitive Disruption** [21], [30],	The target is an e-commerce platform hit by a sophisticated L7 attack during peak operational hours.[4] This tactic aligns with competitive interests attempting to exhaust server resources, disrupt the shopping experience, and steal market share.[4]
#3 (U.S. Beverage Co.)	**Ransom DDoS (RDDoS)**, [31]	The intensity (13.5M RPS) and brevity (8-minute burst) is characteristic of a 'proof-of-attack' [4], typically sent to the victim as a precursor to an extortion demand, compelling the victim to pay a ransom (often in Bitcoin) to prevent a full-scale, crippling outage.

Hypothesis for Incident #5 (European Network Infrastructure)

Given the unprecedented, record-breaking scale (22.2 Tbps) [1] and the target being core

network plumbing, the most likely non-financial, strategic motive is **Botnet-as-a-Service (BaaS) Flexing and Strategic Testing**.[13]

The Aisuru operators, who have previously embedded "Easter egg" messages in their code [24] and engaged in public mockery [24], use these record-breaking events as a **high-profile, verifiable marketing demonstration** [15] to attract high-paying clients, including potentially state-aligned groups.[22] Hitting a core infrastructure target (unnamed European firm) allows the attacker to test the network capacity of a major global defense provider (Cloudflare), thus validating the botnet's 'guaranteed' power against the world's most hardened targets.[16]

---

4. Strategic Defensive Imperatives (Addressing Q4)

The 40-second duration of the 22.2 Tbps attack underscores a critical reality: human-paced defenses are obsolete.[5] Defense must be driven by machine-speed automation.

Three Non-Negotiable Architectural Requirements

1. **Global Anycast Routing and Massive Capacity Headroom:** To defend against the sheer scale of the May (7.3 Tbps) and September (22.2 Tbps) attacks, mitigation must occur at the edge, globally.[18] The **Anycast** routing technique is non-negotiable, as it disperses the monumental traffic load across multiple scrubbing sites, preventing the saturation of any single network link or data center.[25] Successful mitigation relies entirely on guaranteed *capacity headroom*.[17]
2. **AI-Driven Behavioral Scrubbing:** To counter the stealth and protocol exploitation of the January/February HTTP/2 attacks, detection must be autonomous.[18] AI/ML-driven anomaly detection is the only technology capable of identifying the subtle, malicious patterns of L7 resource abuse (like the zero-day logic of Rapid Reset) in real time, neutralizing the attack within seconds without human verification.[18]
3. **Proactive Egress Control and Micro-Segmentation:** Since major botnets like Aisuru primarily leverage compromised IoT devices within ISP and customer networks [13], defense must be proactive and internal.[6] **Egress control** via solutions like per-direction hostgroup thresholds [6] is necessary to monitor and automatically suppress malicious **outbound** traffic (the attack weapon) from the source before it impacts the wider internet.[6] This aligns with Zero Trust principles, where **micro-segmentation** contains threats and prevents compromised internal devices from launching large-scale attacks.[27]

CISO Investment Strategy for the Indonesian Government Agency (#2)

If I were the CISO for the Indonesian Government Agency, my first $1 million would be invested in **Reactive Mitigation via a Third-Party Cloud Service (DDoS Scrubbing Center)**.

Justification: The 14-hour siege demonstrates a sustained, specialized Layer 7 threat that leverages protocol flaws (HTTP/2 Rapid Reset).[4] While long-term infrastructure hardening is crucial, a government agency's core mandate is **immediate service continuity** to maintain public trust. Internal IT departments typically lack the specialized, T-level capacity, the global Anycast routing necessary to absorb massive floods, and the AI/ML application intelligence required to defeat stealthy L7 protocol attacks.[25] Outsourcing to a hyperscale cloud scrubbing service provides instant, elastic capacity and machine-speed L7 expertise that the agency cannot build in-house, offering immediate and guaranteed resilience against both the scale of the February attack and the potential future jump to multi-Tbps floods.[4]

Low-Cost, High-Impact Mitigation for Incident #2

A specific, low-cost, high-impact mitigation strategy to reduce the duration of the 14-hour Indonesian Government attack (Incident #2) would be **Adaptive Session-Based Rate Limiting combined with a Non-Intrusive JavaScript Challenge**.[22]

The HTTP/2 Rapid Reset attack works by rapidly creating and resetting thousands of streams within a single, persistent connection.[3] Instead of relying on crude IP-based limits (which fail if the botnet is distributed), the mitigation would be:

1. **Rate-Limit Streams per Connection:** Enforce an extremely aggressive limit on the number of new HTTP/2 streams that can be opened and reset within a short window (e.g., 50 streams/second) from a single TCP connection.
2. **Challenge High-RPS Sources:** Any source IP or connection that violates the stream threshold is immediately subjected to a **JavaScript-based challenge** (or similar proof-of-work puzzle). A legitimate browser solves this challenge instantly and transparently; a high-volume botnet script (which is programmed only for the protocol exploit) would either fail to execute the JavaScript or be prohibitively resource-intensive to run at 10 million RPS simultaneously.[4] This surgical approach breaks the automated

script's logic, effectively throttling the attack without blocking legitimate citizen access.

Works cited

1. Record-Breaking DDoS Attack Peaks at 22 Tbps and 10 Bpps - SecurityWeek, accessed October 19, 2025, https://www.securityweek.com/record-breaking-ddos-attack-peaks-at-22-tbps-and-10-bpps/
2. Hyper-Volumetric DDoS Attack Sets New Benchmark at 22.2 Tbps - CircleID, accessed October 19, 2025, https://circleid.com/posts/hyper-volumetric-ddos-attack-sets-new-benchmark-at-22.2-tbps
3. What Is a Denial of Service (DoS) Attack? - Palo Alto Networks, accessed October 19, 2025, https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos
4. Early 2025 DDoS Attacks Signal a Dangerous Trend in Cybersecurity - Imperva, accessed October 19, 2025, https://www.imperva.com/blog/early-2025-ddos-attacks-signal-a-dangerous-trend-in-cybersecurity/
5. Cloudflare Fends Off Record 22.2 Tbps DDoS Attack With Zero Downtime - SQ Magazine, accessed October 19, 2025, https://sqmagazine.co.uk/cloudflare-record-ddos-22-2-tbps-blocked/
6. DDoS botnet Aisuru drives record outbound floods from infected ISP-hosted IoT, accessed October 19, 2025, https://fastnetmon.com/2025/10/15/ddos-botnet-aisuru-drives-record-outbound-floods-from-infected-isp-hosted-iot/
7. DDoS Attack Statistics: 20.5M Attacks Blocked in Q1 2025 - DeepStrike, accessed October 19, 2025, https://deepstrike.io/blog/ddos-attack-statistics
8. Classification of DDoS attacks: every modern DDoS attack vector explained - FastNetMon, accessed October 19, 2025, https://fastnetmon.com/2025/07/25/classification-of-ddos-attacks-every-modern-ddos-attack-vector-explained/
9. Five Most Famous DDoS Attacks and Then Some | A10 Networks, accessed October 19, 2025, https://www.a10networks.com/blog/5-most-famous-ddos-attacks/
10. Airport attack suspect arrested, DDoS hits new record, BRICKSTORM backdoor steals IPs, accessed October 19, 2025, https://cisoseries.com/cybersecurity-news-suspect-arrested-over-airport-attack-ddos-attack-hits-new-record-brickstorm-backdoor-steals-ips/
11. 2023 DDoS Statistics and Trends - Vercara - DigiCert, accessed October 19, 2025, https://vercara.digicert.com/resources/2023-ddos-statistics-and-trends
12. A Deep Dive into DDoS Carpet-Bombing Attacks - NSFocus, accessed October 19, 2025, https://nsfocusglobal.com/a-deep-dive-into-ddos-carpet-bombing-attacks/

13. DDoS Botnet Aisuru Blankets US ISPs in Record DDoS - Krebs on Security, accessed October 19, 2025, https://krebsonsecurity.com/2025/10/ddos-botnet-aisuru-blankets-us-isps-in-record-ddos/
14. What is a DDoS attack and how to defend against it in 2025 - Sycope, accessed October 19, 2025, https://www.sycope.com/post/what-is-a-ddos-attack-and-how-to-defend-against-it-in-2025
15. Aisuru Ascending: The Near-Record Attack on Krebs and What It Means for You - Vercara, accessed October 19, 2025, https://vercara.digicert.com/resources/aisuru-ascending-the-near-record-attack-on-krebs-and-what-it-means-for-you
16. Cloudflare Mitigates Record 22.2 Tbps DDoS Attack from Aisuru Botnet - WebProNews, accessed October 19, 2025, https://www.webpronews.com/cloudflare-mitigates-record-22-2-tbps-ddos-attack-from-aisuru-botnet/
17. Cloudflare Mitigated Record-Breaking 22.2 Tbps DDoS Attack - CyberInsider, accessed October 19, 2025, https://cyberinsider.com/cloudflare-mitigated-record-breaking-22-2-tbps-ddos-attack/
18. 22.2 Terabit-Per-Second DDoS Attack Establishes New Global Record, accessed October 19, 2025, https://cyberpress.org/22-2-terabit-per-second-ddos-attack/
19. Massive 22.2 Tbps DDoS Attack Sets New World Record - GBHackers, accessed October 19, 2025, https://gbhackers.com/massive-22-2-tbps-ddos-attack/
20. DDoS Attack Motivations Abound | NETSCOUT, accessed October 19, 2025, https://www.netscout.com/blog/ddos-attack-motivations-abound
21. Why do DDoS attacks happen? Top motivations behind DDoS cybercrime - FastNetMon, accessed October 19, 2025, https://fastnetmon.com/2025/08/27/why-do-ddos-attacks-happen-top-motivations-behind-ddos-cybercrime/
22. DDoS Trends & Predictions For 2025 - Cyber Security Intelligence, accessed October 19, 2025, https://www.cybersecurityintelligence.com/blog/ddos-trends-and-predictions-for-2025-8350.html
23. High-Speed Network DDoS Attack Detection: A Survey - PMC, accessed October 19, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC10422513/
24. The Most Powerful Ever? Inside the 11.5Tbps-Scale Mega Botnet AISURU - 奇安信 X 实验室, accessed October 19, 2025, https://blog.xlab.qianxin.com/super-large-scale-botnet-aisuru-en/
25. Mitigating DDoS using an anycast playbook - APNIC Blog, accessed October 19, 2025, https://blog.apnic.net/2023/03/28/mitigating-ddos-using-an-anycast-playbook/
26. Top 7 DDoS Types in 2025 and How to Prevent Them - Radware, accessed October 19, 2025, https://www.radware.com/cyberpedia/ddos-attacks/top-7-ddos-types-in-2025/

27. Secure networks with SASE, Zero Trust, and AI - Microsoft Learn, accessed October 19, 2025, https://learn.microsoft.com/en-us/security/zero-trust/deploy/networks
28. Connected Communities Guidance - Zero Trust to Protect Interconnected Systems - CISA, accessed October 19, 2025, https://www.cisa.gov/sites/default/files/2024-08/Connected%20Communities%20Guidance%20-%20Zero%20Trust%20to%20Protect%20Interconnected%20Systems%20%28508%29.pdf
29. DNS Security 2022 - Best Practices to Prevent DDoS Attacks - DigiCert, accessed October 19, 2025, https://www.digicert.com/blog/dns-security-2022-best-practices-and-solutions
30. DDoS – Motivations for the Madness, Part 1 - NSFOCUS, Inc., a global network and cyber security leader, protects enterprises and carriers from advanced cyber attacks., accessed October 19, 2025, https://nsfocusglobal.com/ddos-motivations-madness-part-1/
31. Hyper-volumetric DDoS attacks skyrocket: Cloudflare's 2025 Q2 DDoS threat report, accessed October 19, 2025, https://blog.cloudflare.com/ddos-threat-report-for-2025-q2/