Owasp x µLearn Bootcamp Task 7

DDoS Incident Analysis Report

Name: Ajay M Nambiar

Date: 30/09/2025

Assessment Type: DDoS Incident Analysis

Objective :

The goal of this assessment is to analyze five recent, seminal Distributed Denial-of-Service (DDoS) incidents that define the threat landscape of late 2024 and 2025. The process involves investigating each chosen attack to prepare a summary covering the target, the technology used, the attacker's motive, the overall impact, and the defensive strategies that could have mitigated it.

Information Sources

- Cloudflare Threat Reports
- NETSCOUT Threat Intelligence Reports
- Public cybersecurity news outlets and publications

Methodology & Execution

Task 1: Incident Analysis - The 22.2 Tbps Volumetric Siege (September 2025)

- **Target:** The target of this historic attack was a European network infrastructure company.[1] Directing an attack of this magnitude at a core infrastructure provider indicates an intent to cause widespread, regional disruption, potentially impacting internet connectivity and services for a large population of downstream users and businesses.
- **Technology Used:** The attack was a massive volumetric flood that reached a peak of **22.2 Tbps** and a packet rate of **10.6 billion packets per second (Bpps)**, making it the largest DDoS attack publicly recorded to date.[2] The assault was executed as a short, intense burst, lasting only approximately 40 seconds.[3] This "hit-and-run" methodology is a deliberate tactic designed to overwhelm defenses before they can fully react.[5] The attack was attributed to the

Aisuru botnet, estimated to control over 300,000 infected IoT devices, with a particular focus on vulnerable internet routers.[2] The 22.2 Tbps attack itself was highly distributed, originating from over 404,000 unique, non-spoofed IP addresses.[1]

- **Attacker's Motive:** The motive appears to be primarily commercial, intertwined with a desire for notoriety. The creators of the Aisuru botnet operate a commercial enterprise, selling access to their DDoS capabilities on platforms like Telegram.[1] Executing a record-shattering attack serves as a powerful advertisement for their services. Additionally, members of the Aisuru group exhibit a culture of launching highly destructive attacks "for fun" or for "bragging rights".[1]
- **Overall Impact:** The attack was successfully mitigated by Cloudflare's autonomous systems, preventing any service disruption.[3] However, the strategic impact is profound. This incident demonstrates that botnets capable of generating over 20 Tbps of attack traffic are no longer theoretical, forcing a complete recalibration of defensive capacity planning for major internet providers and large enterprises.
- **Defensive Strategies:** Mitigation requires a massive-scale, globally distributed cloud scrubbing service with an anycast network architecture. Proactive defense relies on automated, real-time botnet fingerprinting to identify and surgically drop malicious packets.[6] The long-term strategy must address the root cause of insecure IoT devices through industry-wide pressure on manufacturers and end-user education.[3]

Task 2: Incident Analysis - The 11.5 Tbps Multi-Source Flood (September 2025)

- **Target:** The specific target of the 11.5 Tbps attack was not publicly disclosed.
- **Technology Used:** The attack was a high-intensity **UDP flood** that peaked at **11.5 Tbps** with a packet rate of **5.1 Bpps**.[7] It was a short-burst "hit-and-run" attack, lasting only about

35 seconds.[7] The most critical aspect was its hybrid source, a coordinated assault from a "combination of several IoT and cloud providers," with Google Cloud being just one of many sources.[7] This demonstrates the ability to orchestrate massive traffic flows simultaneously from compromised consumer-grade IoT devices and hijacked, high-bandwidth commercial cloud infrastructure.

- **Attacker's Motive:** Plausible motives include a capability demonstration for a DDoS-for-hire service, a distraction to cover for a more stealthy intrusion attempt [7], or an unpublicized Ransom DDoS (RDDoS) campaign.
- **Overall Impact:** The attack was successfully neutralized by Cloudflare's autonomous defenses.[7] The broader impact is the confirmation of large-scale, coordinated abuse of legitimate cloud infrastructure as a primary DDoS weapon. This tactic complicates defense, as security teams cannot simply block large IP ranges belonging to major cloud providers without blocking legitimate traffic.

- **Defensive Strategies:** Defenses must move beyond IP blocklisting toward granular, behavior-based filtering capable of deep packet inspection. Robust internal monitoring and abuse detection from cloud providers themselves are essential.[7] A hybrid defense model combining on-premise network monitoring with cloud-based scrubbing services is necessary to counter such threats.

Task 3: Incident Analysis - The 7.3 Tbps Hosting Provider Assault (May 2025)

- **Target:** The target was a **hosting provider** protected by Cloudflare's Magic Transit service.[6] By attacking a foundational piece of internet infrastructure, adversaries aim to create a significant blast radius of collateral damage, potentially causing cascading service failures for thousands of businesses and applications that rely on the provider.
- **Technology Used:** The incident was a multi-vector attack that peaked at **7.3 Tbps** and delivered 37.4 terabytes of malicious data in just **45 seconds**.[6] The attack blended a primary

UDP flood (99.996% of traffic) with secondary reflection and amplification attacks, including **NTP reflection**.[6] The attack was massively distributed, originating from a botnet of over 122,000 unique source IP addresses across 161 countries.[6]

- **Attacker's Motive:** The motive is systemic infrastructure disruption to inflict maximum collateral damage and create widespread chaos. This can be driven by anti-competitive aims, geopolitical goals, or as a precursor to a large-scale extortion campaign.
- **Overall Impact:** The attack was successfully mitigated with no reported service impact on the hosting provider or its customers.[6] The incident serves as a critical case study on the vulnerability of the internet's supply chain and the systemic risk posed by attacks on foundational providers.
- **Defensive Strategies:** The cornerstone of the successful defense was an **anycast network architecture**, which distributed the 7.3 Tbps load across a global network, mitigating the attack close to its source.[6] An automated multi-vector mitigation platform capable of autonomously detecting and blocking multiple, simultaneous attack vectors was also essential. This incident proves that foundational internet companies must adopt robust, large-scale DDoS protection for their own infrastructure.

Task 4: Incident Analysis - The Taiwan Election Campaign (2024)

- **Target:** The targets were a broad set of Taiwanese institutions, including **government systems, telecommunications firms, and financial institutions**, with activity escalating around the January 13, 2024 presidential elections.[10]

- **Technology Used:** This was a **sustained, multi-faceted campaign of hybrid warfare**. The daily volume of cyberattacks from Chinese-attributed groups doubled to an average of 2.4 million attempts per day.[11] The campaign blended

DDoS attacks to disrupt service availability, **cyber espionage** to steal sensitive data, and **disinformation** to undermine public trust in the democratic process.[11] DDoS attacks were specifically launched against transportation and financial institutions, timed to coincide with Chinese military drills to intensify intimidation.[12]

- **Attacker's Motive:** The motive was explicitly **geopolitical interference**. The campaign, widely attributed to actors aligned with the People's Republic of China, was designed to intimidate the Taiwanese populace and undermine support for the Democratic Progressive Party (DPP).[10]
- **Overall Impact:** While the campaign did not prevent the election or change the outcome, it provided a clear public demonstration of a state-level hybrid warfare capability.[15] It serves as a blueprint for future election interference operations globally, showcasing how cyber, military, and information operations can be orchestrated to exert political pressure.
- **Defensive Strategies:** Defense requires a coordinated, national-level effort involving real-time threat intelligence sharing between government agencies, military cyber commands, and private-sector cybersecurity firms. Public-private partnerships are essential, as is a defense-in-depth posture that includes scalable DDoS mitigation, advanced endpoint detection, and public awareness campaigns to build resilience against disinformation.[18]

Task 5: Incident Analysis - Anonymous Sudan's Financial Sector Campaign (2024-2025)

- **Target:** The hacktivist group Anonymous Sudan has conducted a wide-ranging campaign, with a significant and consistent focus on the **financial sector**, including major banks and financial service providers.[19]
- **Technology Used:** The group prefers sophisticated **Layer 7 (application-layer) DDoS attacks**, such as HTTP floods, which target application logic with seemingly legitimate but resource-intensive requests.[19] Instead of a traditional IoT botnet, Anonymous Sudan primarily uses clusters of

rented servers to launch attacks, giving them access to high-bandwidth infrastructure.[19] Their toolkit includes platforms such as the "Skynet Botnet" and "Godzilla".[19]

- **Attacker's Motive:** The group operates with a **blended motive** of political hacktivism and professional cybercrime for financial gain. They publicly claim

political or religious motivations for attacks [19], while simultaneously operating a commercial

DDoS-for-hire (DDoSaaS) service and engaging in **Ransom DDoS (RDDoS)**, where they demand payment to stop an attack.[19]

- **Overall Impact:** Anonymous Sudan has proven its ability to cause significant and sustained disruption to major organizations, including Microsoft and Scandinavian Airlines.[19] Their campaign against Kenyan infrastructure successfully disrupted banks, hospitals, and government services.[20] The primary impact is the successful demonstration of a professionalized cybercrime model that leverages a political narrative as both a weapon and a business strategy.
- **Defensive Strategies:** Countering this threat requires advanced Layer 7 protection, such as a modern Web Application Firewall (WAF) that can perform deep analysis of HTTP/S traffic and use behavioral analysis to distinguish malicious bots from legitimate users. Dedicated API security is also critical.[23] Organizations must develop a pre-defined incident response playbook for handling RDDoS threats, establishing a clear policy on ransom payments and outlining communication strategies.[25]

Results

The analysis of these five incidents reveals several key strategic takeaways for developing a modern defensive posture:

- A resilient architecture must be built for the hyper-volumetric era, prioritizing globally distributed, cloud-native DDoS mitigation services with massive scrubbing capacity.
- Threat intelligence must be integrated into real-time defense, using automated botnet fingerprinting and adaptive, heuristic-based analysis to counter evolving threats.
- Defenses must be hardened against sophisticated application-layer (L7) attacks by deploying modern Web Application Firewalls (WAFs) and dedicated API security gateways.
- Incident response plans must be updated to account for blended threats, treating DDoS attacks as potential smokescreens for other intrusions and developing specific playbooks for Ransom DDoS (RDDoS) scenarios.