Athira Biju
Amal Jyothi College of Engineering

An Investigation of Five Major Distributed Denial of Service (DDoS) Incidents (2024-2025)

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

Target:

A European network infrastructure company, critical for regional internet services.

Technology Used:
A massive volumetric flood reaching 22.2 Tbps and 10.6 billion packets per second, executed in a short burst lasting about 40 seconds. The attack was distributed across 404,000+ non-spoofed IPs, primarily from the Aisuru botnet which commandeers over 300,000 IoT devices.

Attacker's Motive:
Primarily commercial—to demonstrate and advertise DDoS-for-hire services—and for notoriety among hacking groups.

Overall Impact:
Cloudflare successfully mitigated the attack, preventing service disruption. However, this attack set a new scale benchmark and stressed global defense planning capacities.

Defensive Strategies:
Cloud scrubbing with anycast architecture to absorb massive volumes; real-time botnet fingerprinting; industry-wide IoT security improvements[PDF].

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

Target:

Undisclosed, but the attack was launched from both compromised IoT devices and commercial cloud infrastructure.

Technology Used:
Hybrid UDP flood reaching 11.5 Tbps at 5.1Bpps, lasting approximately 35 seconds. Utilized hijacked Google Cloud resources alongside consumer IoT botnets.

Attacker's Motive:
Likely a demonstration of capability or a distraction accompanying a more stealthy intrusion; may be linked to ransom DDoS campaigns.

Overall Impact:
Attack was neutralized without outage but exposed the threat of abusing legitimate cloud platforms for massive DDoS.

Defensive Strategies:
Behavior and pattern-based filtering beyond IP blacklisting, combined on-premise and cloud-based defenses.

Incident 3: The 7.3 Tbps Hosting Provider Assault (May 2025)
Target:
A hosting provider safeguarded by Cloudflare Magic Transit.

Technology Used:
Multi-vector attack primarily UDP flood (99.996%), including NTP amplification; 37.4 TB data over 45 seconds; sources spanned 161 countries.

Attacker's Motive:
Disruption aiming for collateral damage, with possible geopolitical or extortion-driven goals.

Overall Impact:
Mitigated with no service disruption; highlighted vulnerability in supply chain infrastructure.

Defensive Strategies:
Global anycast distribution of traffic, multi-vector autonomous mitigation platforms.

Incident 4: Taiwan Election Campaign (2024)
Target:
Taiwanese government institutions, telecoms, and financial organizations during the January 2024 presidential elections.

Technology Used:
Sustained hybrid warfare combining DDoS, cyber espionage, and disinformation campaigns; daily attacks averaging 2.4 million attempts.

Attacker's Motive:
Geopolitical interference attributed to PRC-aligned groups aiming to intimidate voters and undermine political stability.

Overall Impact:
Did not change election outcome but demonstrated the power of combined cyber and information warfare.

Defensive Strategies:
Coordinated national real-time threat intelligence sharing, public-private partnerships, defense-in-depth measures including DDoS mitigation and public awareness.

Incident 5: Anonymous Sudan Financial Sector Campaign (2024-2025)
Target:
Banks and financial institutions primarily in Kenya and other affected regions.

Technology Used:

Sophisticated Layer 7 HTTP floods using rented server infrastructures, with botnets like Skynet and Godzilla.

Attacker's Motive:
Blend of political hacktivism and financially motivated cybercrime through DDoS-for-hire and ransom DDoS services.

Overall Impact:
Caused prolonged disruption in banking and government services, showcasing professional criminal operations masked by political narratives.

Defensive Strategies:
Advanced Layer 7 protection using Web Application Firewalls, API security, behavioral analysis, and clear RDDoS incident response playbooks.