Analysis of Recent DDoS Attacks — Ethical Hacker GPT

AUTHOR: TOM SHINJO THOMAS

1) Cloudflare — 7.3 Tbps hyper-volumetric UDP flood (May 2025)

Cloudflare mitigated a 7.3 Tbps DDoS attack targeting a single IP. The attack used reflection and amplification via UDP services, lasting around 45 seconds. This demonstrated that massive short-burst attacks can still threaten availability without strong scrubbing infrastructure.

2) Cloudflare — 11.5 Tbps UDP flood (Sept 2025)

A 35-second UDP flood peaked at 11.5 Tbps (5.1 billion packets/sec), combining cloud and IoT sources. It was mitigated automatically by Cloudflare. The event reinforced the need for distributed filtering and global-scale detection.

3) Cloudflare — 22.2 Tbps 'record' attack (Sept 2025)

Another reported hyper-volumetric flood hit 22.2 Tbps and 10.6 billion pps, highlighting that attackers can sustain even higher burst traffic levels. Reflects rapid escalation in DDoS attack magnitude.

4) Gcore — 6 Tbps attack on gaming provider (Oct 2025)

A gaming host was hit with a 6 Tbps UDP flood, mitigated within 45 seconds. It used the Aisuru botnet, leveraging compromised IoT and cloud nodes. Such bursts are often reconnaissance for future campaigns.

5) Financial sector DDoS spike (Akamai/FS-ISAC, Oct 2024)

Financial institutions suffered a surge of targeted DDoS and API floods, causing partial outages. Multi-vector attacks targeted APIs, DNS, and application endpoints, demonstrating the evolution from volumetric floods to precision service disruption.

Detailed Investigation: Cloudflare 7.3 Tbps DDoS (May 2025)

Target

A Cloudflare customer's single IP address was targeted. Mitigation was handled through Cloudflare's edge scrubbing network.

Attack Technology

- UDP reflection/amplification using misconfigured internet services.

- Estimated 37.4 TB of traffic in 45 seconds.

- Likely combination of compromised IoT devices and abused cloud nodes.

Attacker Motive

- Likely testing or demonstrating botnet capacity.

- No confirmed ransom or extortion claims linked to this event.

Impact

- No service interruption reported for the victim.

- Demonstrated feasibility of >7 Tbps floods and the importance of distributed global mitigation.

Defensive Strategies

1. Use large-scale cloud-based DDoS mitigation services.

2. Employ anycast routing and global traffic scrubbing.

3. Rate-limit UDP and disable vulnerable reflection services.

4. Enforce BCP 38 (anti-spoofing) filtering.

5. Automate detection and response playbooks for hyper-burst floods.

6. Participate in ISAC/industry information-sharing for faster IOCs and blackholing coordination.

Defensive Lessons

- Traditional on-premises DDoS appliances cannot handle terabit-scale floods.

- Short-burst, high-pps attacks require pre-configured, automated mitigation.

- Cooperation with ISPs and global scrubbing providers is essential.

- Harden UDP services and remove amplification vectors.

- Sector-specific response coordination improves resilience.

References

1. Cloudflare DDoS Threat Reports (2025 Q1–Q3)

2. Gcore Radar and TechRadar (Oct 2025)

3. Akamai / FS-ISAC Financial Sector Threat Report (2024–2025)

4. Reuters, SecurityWeek, and TheHackerNews coverage of hyper-volumetric DDoS events