Analysis of Recent DDoS Attacks

Prepared by**:** Shifna N
Date**:** August 2025

●Introduction

A Distributed Denial of Service (DDoS) attack happens when many computers or devices send a large amount of traffic to a target, making it very slow or even causing it to stop working. These attacks are becoming more common and stronger. They are often used to disturb online services, ask for ransom, or make a political point. This report looks at five recent DDoS attacks and gives a closer study of one main attack, covering its target, method, reason, effect, and possible defenses.

●Recent DDoS attacks

1. Cloudflare 7.3 Tbps / 4.8 Bpps attack (May / June 2025)

Cloudflare automatically blocked a record-breaking, hyper-volumetric attack that peaked at 7.3 terabits per second (Tbps) and 4.8 billion packets per second (Bpps). The attack was a very short, extremely intense flood aimed at a hosting provider's IP address and was stopped by Cloudflare's global defenses.

2. Cloudflare 6.5 Tbps attack (April 2025)

In April 2025 Cloudflare mitigated a separate hyper-volumetric attack that reached 6.5 Tbps (and very large packet rates). Security analysts linked it to large IoT/cloud-VM botnets (reported as “Eleven11bot” and similar botnets composed of compromised cameras and VMs).

3. X (formerly Twitter) nationwide outages from DDoS (March 2025)

X experienced repeated worldwide outages that day. A hacktivist group called Dark Storm Team publicly claimed the DDoS, while independent researchers found evidence of large botnet traffic (many IoT devices). The outages were intermittent but affected many users.

4. Coordinated hacktivist DDoS surge against U.S. businesses (June 2025)

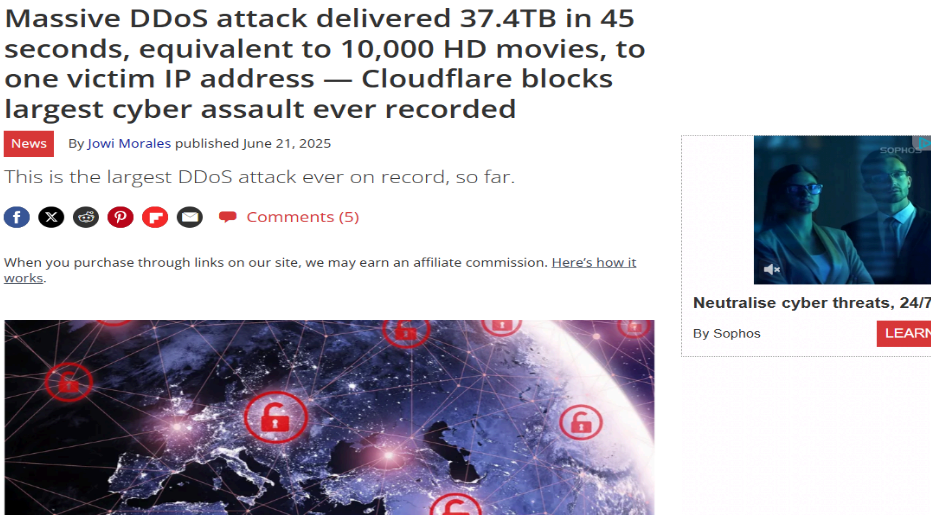
Following geopolitical events, multiple hacktivist groups launched a coordinated surge of DDoS attacks over 24 hours that targeted military/aerospace manufacturers, financial institutions and government agencies causing wide but varied disruption.

5. DDoS scrubbing service targeted (September 2025)

A DDoS “scrubbing” provider (a company that filters DDoS traffic) itself was hit by a very large attack that peaked at about 1.5 billion packets per second, coming from over 11,000 networks showing even defenders can be targeted. (reported in Tom's Hardware / FastNetMon).

✦Cloudflare — 7.3 Tbps / 4.8 Bpps attack

- Target



Massive DDoS attack delivered 37.4TB in 45 seconds, equivalent to 10,000 HD movies, to one victim IP address — Cloudflare blocks largest cyber assault ever recorded

News By Jowi Morales published June 21, 2025

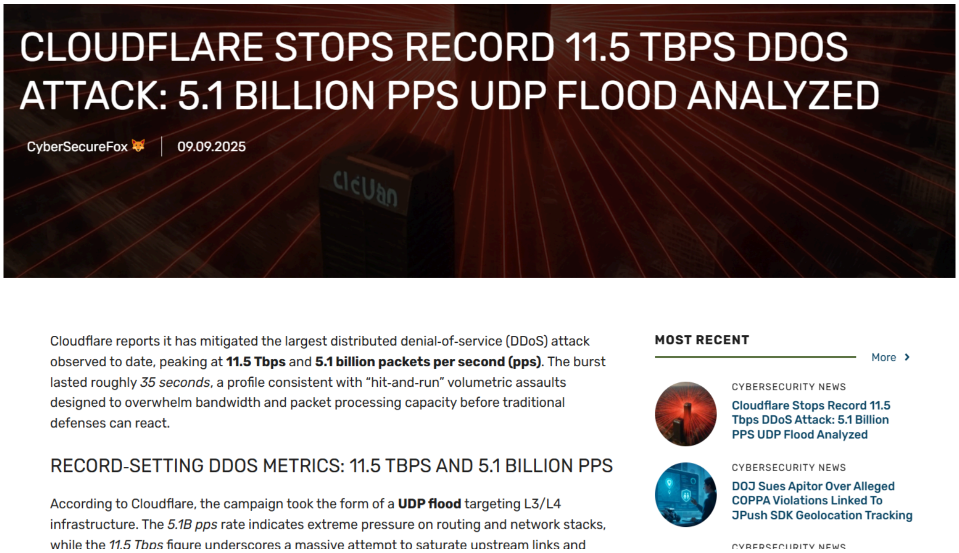
This is the largest DDoS attack ever on record, so far.

Comments (5)

When you purchase through links on our site, we may earn an affiliate commission. Here's how it works.

The visible target was a single IP address owned by a hosting provider (the victim's server IP). Cloudflare's systems observed the attack as a flood of traffic aimed at that IP and its multiple destination ports. Cloudflare's global network automatically intercepted and blocked the malicious traffic before it reached customers.

- Technology used



CLOUDFLARE STOPS RECORD 11.5 TBPS DDOS ATTACK: 5.1 BILLION PPS UDP FLOOD ANALYZED

CyberSecureFox 🦊 | 09.09.2025

Cloudflare reports it has mitigated the largest distributed denial-of-service (DDoS) attack observed to date, peaking at **11.5 Tbps** and **5.1 billion packets per second (pps)**. The burst lasted roughly *35 seconds*, a profile consistent with "hit-and-run" volumetric assaults designed to overwhelm bandwidth and packet processing capacity before traditional defenses can react.

RECORD-SETTING DDOS METRICS: 11.5 TBPS AND 5.1 BILLION PPS

According to Cloudflare, the campaign took the form of a **UDP flood** targeting L3/L4 infrastructure. The *5.1B pps* rate indicates extreme pressure on routing and network stacks, while the *11.5 Tbps* figure underscores a massive attempt to saturate upstream links and

MOST RECENT

More ›

CYBERSECURITY NEWS

Cloudflare Stops Record 11.5 Tbps DDoS Attack: 5.1 Billion PPS UDP Flood Analyzed

CYBERSECURITY NEWS

DOJ Sues Apitor Over Alleged COPPA Violations Linked To JPush SDK Geolocation Tracking

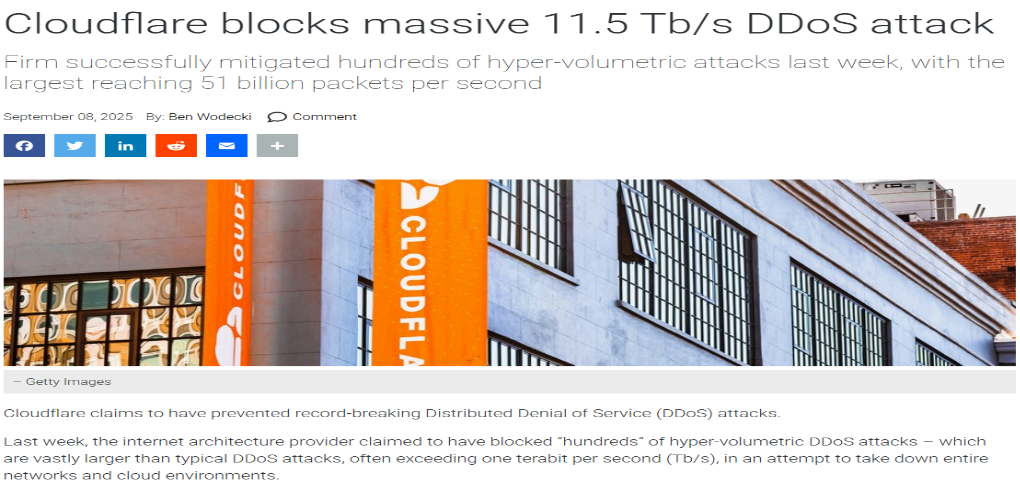
CYBERSECURITY NEWS

- Hyper-volumetric UDP floods and multi-vector traffic: Cloudflare reported this was a very large, high-speed flood measured in terabits per second and billions of packets per second, the attackers used network-layer floods (UDP/packet floods) and many destination ports to overwhelm infrastructure quickly.
- Botnets of compromised devices: The attack traffic came from a huge number of IP addresses across many countries. These botnets are made by infecting many devices (IoT cameras, DVRs, home routers, or cloud VMs) and commanding them to send traffic at once. Some prior attacks in 2025 were linked to botnets like “Eleven11bot” (many compromised cameras) or VM-based botnets.
- Short, intense bursts: Attackers used very short bursts (tens of seconds) at extremely high rates that are intended to overwhelm links/routers before defenders can react. Cloudflare said the 7.3 Tbps peak lasted only about 45 seconds.

●Attacker's motive

- Testing or showing capability: Some attackers launch record attacks to test their botnets or to show power.
- Extortion or disruption: DDoS attacks may be used to pressure victims (threaten downtime for ransom) or just to cause disruption. Ransom DDoS activity rose in 2025.
- Political/hacktivist reasons: Some attacks are politically motivated (to punish or disrupt certain targets). Cloudflare’s reports show different sectors and regions are targeted for varied motives.

●Impact



Cloudflare blocks massive 11.5 Tb/s DDoS attack

Firm successfully mitigated hundreds of hyper-volumetric attacks last week, with the largest reaching 51 billion packets per second

September 08, 2025 By: Ben Wodecki Comment

– Getty Images

Cloudflare claims to have prevented record-breaking Distributed Denial of Service (DDoS) attacks.

Last week, the internet architecture provider claimed to have blocked “hundreds” of hyper-volumetric DDoS attacks – which are vastly larger than typical DDoS attacks, often exceeding one terabit per second (Tb/s), in an attempt to take down entire networks and cloud environments.

- Potential to saturate network links: An unprotected hosting provider or ISP could have had its uplinks saturated, causing websites and services to go offline for customers. The actual victim avoided prolonged outage because Cloudflare mitigated the traffic.
- Short burst, high damage risk: Even when short, these bursts can cause packet loss, increased latency, and service dropouts for legitimate users if they hit unprotected infrastructure. Cloudflare reported the attack delivered ~37.4 TB in 45 seconds to the target IP (illustrating the volume).

- Industry-wide signal: These record attacks raise costs for defenders and show that attackers can combine millions of devices to hit terabit scales — increasing the need for always-on protection.

●Defensive strategies

- Always-on cloud DDoS protection (CDN / scrubbing networks)
- Use providers like Cloudflare, Akamai, or other DDoS mitigation services that can absorb huge volumes across many data centers. These services distribute and filter attack traffic before it reaches the origin server. Cloudflare's global network was what blocked the 7.3 Tbps flood.
- Put origin servers behind a protected edge and avoid exposing real IPs
- Don't expose the real IP addresses of your servers to the internet. Place servers behind reverse proxies/CDNs and use strict firewall rules so attackers can't hit the origin directly. (In X's March incident, exposed origin servers were a factor.)
- ISP and backbone filtering / coordination
- Work with ISPs to filter spoofed traffic and block known attack sources close to the network edge. For very large volumetric attacks, ISP-level filtering (null-routes, sinkholing) is vital to protect downstream networks. Cloudflare and others provide threat feeds for ISPs to help.
- Rate limiting and intelligent traffic shaping
- At the application level, use rate limiting, challenge pages (CAPTCHA), and progressive throttling so bots can't send millions of requests to the same endpoint. This reduces effect of HTTP layer floods.
- Multi-layer defense (cloud + on-prem appliances + threat intel)
- Combine cloud scrubbing with on-prem firewalls/edge appliances and use shared threat intelligence so defenders can block known bad IP ranges faster. Cloudflare's free threat feeds for ISPs are an example of shared intel.
- Harden IoT and public devices (long-term prevention)
- Since many attacks use compromised IoT devices, manufacturers and ISPs should push firmware updates, harden default passwords, and block dangerous services at the network edge to reduce the pool of devices an attacker can recruit. Regulators and ISPs help by limiting open reflectors/amplifiers.
- Prepare an incident plan and test it
- Have playbooks for failover, communication, and emergency routes when attack traffic starts. Run tabletop exercises so the team can quickly trigger protections, contact CDNs/ISPs, and switch traffic if needed. (Best practice from industry reports.)

●Conclusion

- The 7.3 Tbps Cloudflare attack shows how DDoS has become a hyper-volumetric problem — attackers can create gigantic, short bursts of traffic from huge botnets. The good news is cloud defenses and coordinated ISP action can stop most of these attacks today, but long-term reductions require better device security, threat sharing, and preparedness.

●References

Cloudflare — *DDoS Threat Report for 2025 Q2* (Cloudflare blog).
Cloudflare — *How Cloudflare blocked a monumental 7.3 Tbps DDoS* (Cloudflare technical post).
The Hacker News — *Massive 7.3 Tbps DDoS Attack Delivers 37.4 TB in 45 seconds.*
Tom's Hardware — *DDoS scrubbing service ironic target… (1.5B pps).*
Cloudflare Q1 report and related write-ups on the 6.5 Tbps & 4.8 Bpps attacks.
Wired / Cyberscoop / Malwarebytes coverage — *X outages and March 10, 2025 DDoS (Dark Storm Team)*.
TeckPath — *June 2025 DDoS surge of hacktivist attacks (June 21–22, 2025)*.