Cloudflare mitigates new record-breaking 22.2 Tbps DDoS attack

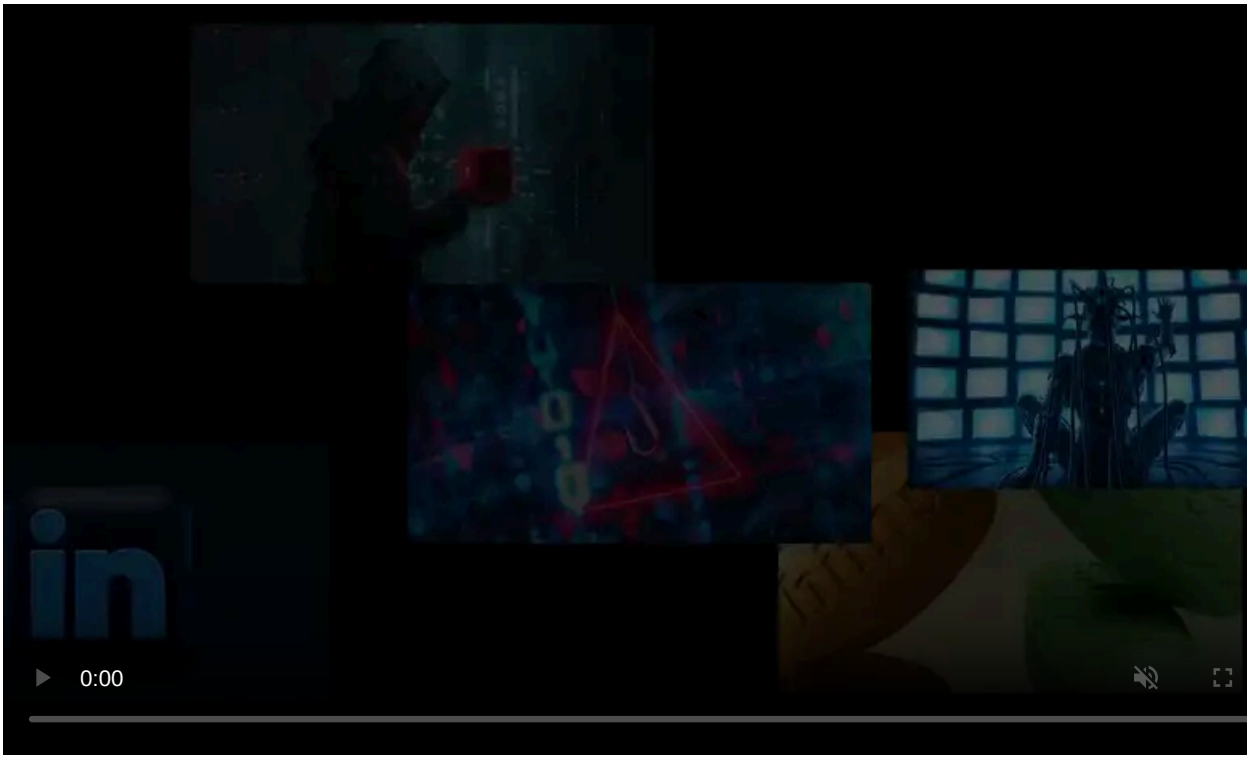
By Bill Toulas

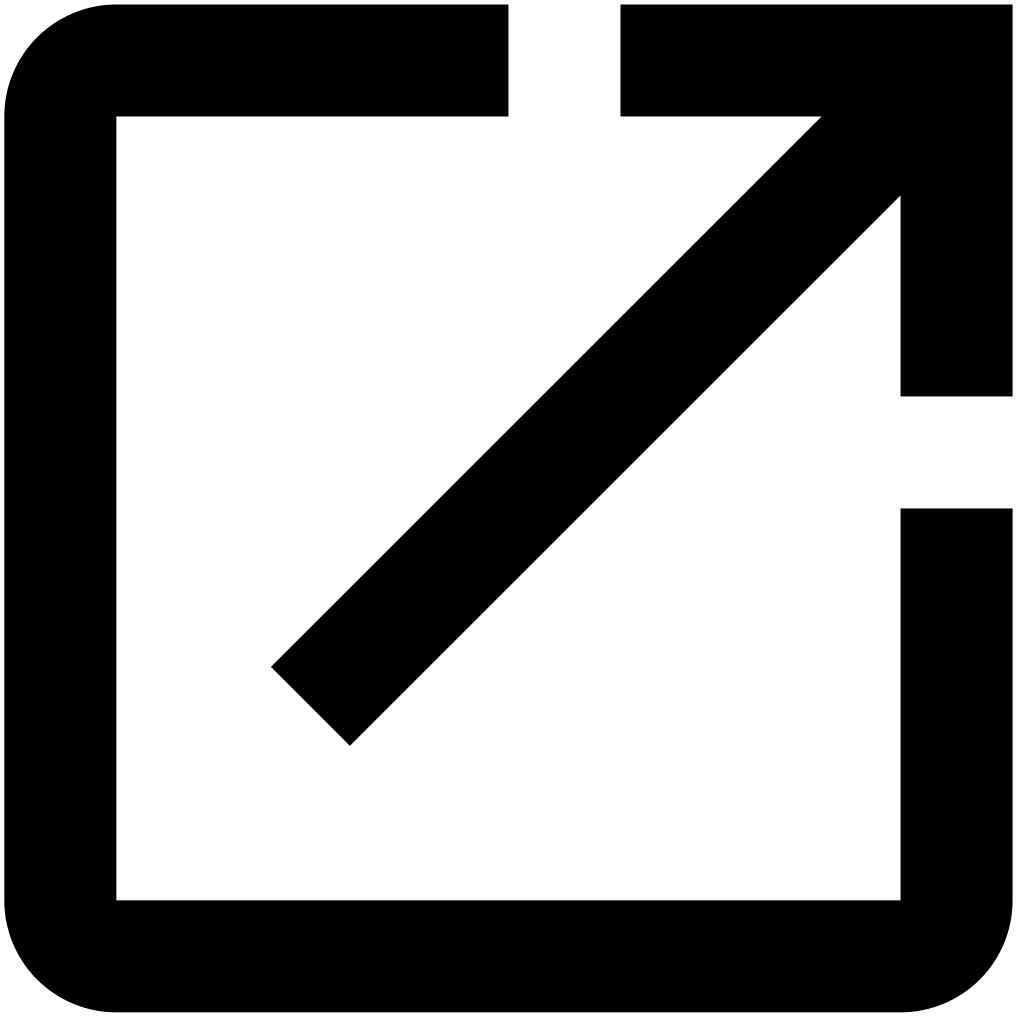
Published: 2025-09-23 · Archived: 2026-04-05 17:38:25 UTC

Cloudflare has mitigated a distributed denial-of-service (DDoS) attack that peaked at a record-breaking 22.2 terabits per second (Tbps) and 10.6 billion packets per second (Bpps).

DDoS attacks typically exhaust either system or network resources, aiming to make services slow or unavailable to legitimate users.

Record-breaking DDoS attacks are becoming more frequent, as just three weeks ago, Cloudflare disclosed that it mitigated a massive 11.5 Tbps and 5.1 Bpps attack, the largest publicly announced at the time.


0:00



Two months before that, the company dealt with another ecord attack that peaked at 7.3 Tbps. In April, the internet giant warned that it was dealing with a record number of DDoS attacks this year.

The latest DDoS incident, also volumentric, lasted 40 seconds and is by far the largest ever mitigated.

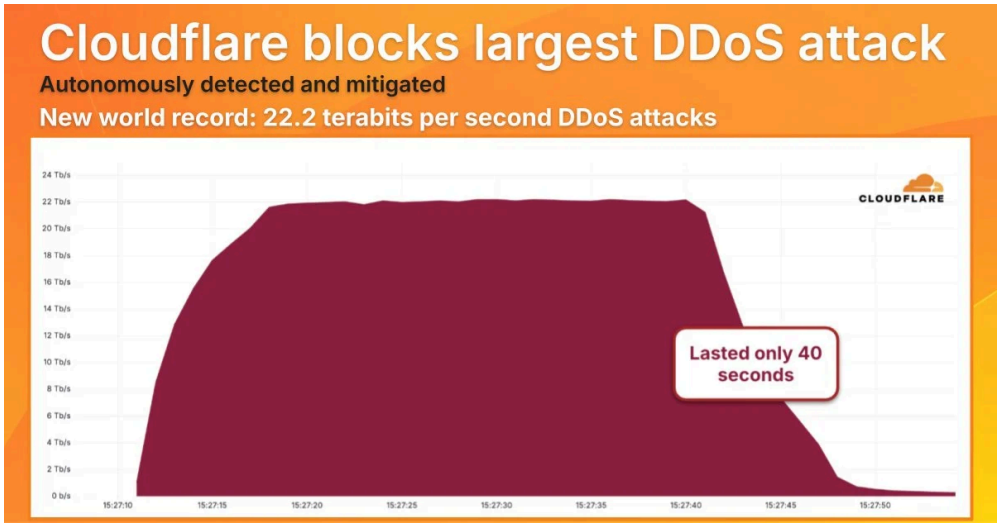


Diagram of the record-breaking attack

Source: Cloudflare

Despite the short assault period, the volume of traffic directed at the victim was enormous, roughly equivalent to streaming one million 4K videos simultaneously.

The packet rate of 10.6 Bpps can be translated to roughly 1.3 web page refreshes per second from every person on the planet.

The large volume of packets makes it particularly difficult for firewalls, routers, and load balancers to process the requests, even if the total bandwidth is manageable.

Although Cloudflare has not shared many details about the last two DDoS attacks, XLab research division at Chinese cybersecurity company Qi'anxin attributed an 11.5 Tb DDoS attack to the AISURU botnet.

According to the researchers, AISURU has infected more than 300,000 devices worldwide, with a sudden increase occuring in April 2025 after the compromise of a Totolink router firmware update server.

The botnet also targets vulnerabilities in IP cameras, DVRs/NVRs, Realtek chips, and routers from T-Mobile, Zyxel, D-Link, and Linksys.

Source: https://www.bleepingcomputer.com/news/security/cloudflare-mitigates-new-record-breaking-222-tbps-ddos-attack/