Hyper-volumetric DDoS attacks skyrocket: Cloudflare’s 2025 Q2 DDoS threat report

2025-07-15

Omer Yoachimik Jorge Pacheco

15 min read

This post is also available in 简体中文, Deutsch, 日本語, 한국어, Español, Indonesia, Nederlands and 繁體中文.

Welcome to the 22nd edition of the Cloudflare DDoS Threat Report. Published quarterly, this report offers a comprehensive analysis of the evolving threat landscape of Distributed Denial of Service (DDoS) attacks based on data from the Cloudflare network. In this edition, we focus on the second quarter of 2025. To view previous reports, visit www.ddosreport.com.

June was the busiest month for DDoS attacks in 2025 Q2, accounting for nearly 38% of all observed activity. One notable target was an independent Eastern European news outlet protected by Cloudflare, which reported being attacked following its coverage of a local Pride parade during LGBTQ Pride Month.

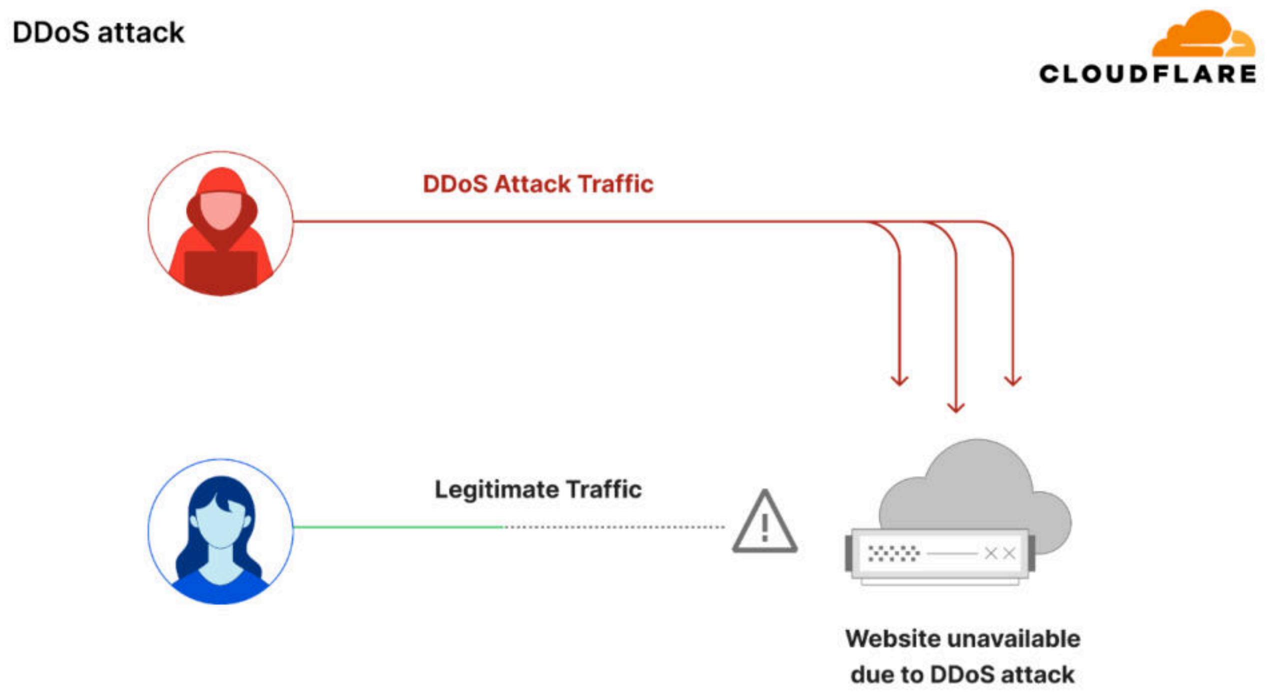
Key DDoS insights

- DDoS attacks continue to break records. During 2025 Q2, Cloudflare automatically blocked the largest ever reported DDoS attacks, peaking at 7.3 terabits per second (Tbps) and 4.8 billion packets per second (Bpps).

- Overall, in 2025 Q2, hyper-volumetric DDoS attacks skyrocketed. Cloudflare blocked over 6,500 hyper-volumetric DDoS attacks, an average of 71 per day.

- Although the overall number of DDoS attacks dropped compared to the previous quarter — which saw an unprecedented surge driven by a large-scale campaign targeting Cloudflare's network and critical Internet infrastructure protected by Cloudflare — the number of attacks in 2025 Q2 were still 44% higher than in 2024 Q2. Critical infrastructure continues to face sustained pressure, with the Telecommunications, Service Providers, and Carriers sector jumping again to the top as the most targeted industry.

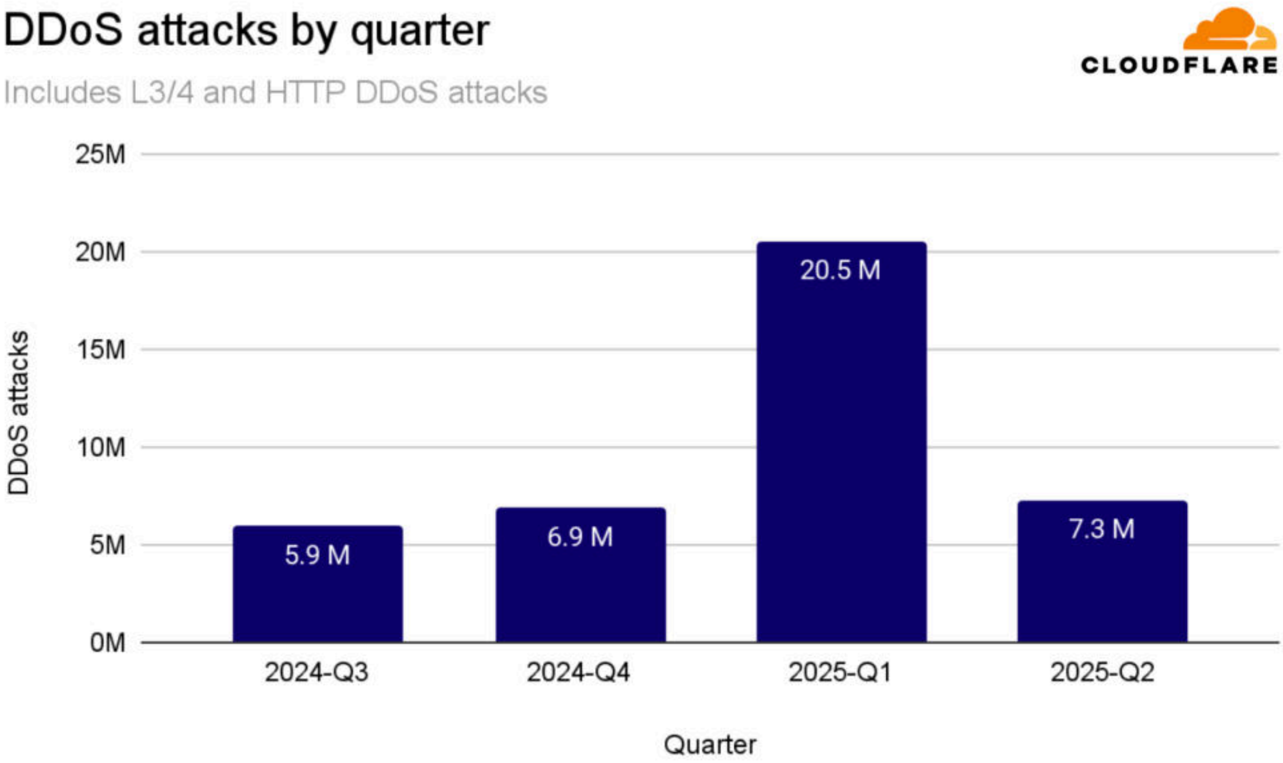
All the attacks in this report were automatically detected and blocked by our autonomous defenses.



To learn more about DDoS attacks and other types of cyber threats, refer to our Learning Center. Visit Cloudflare Radar to view an interactive version of this report where you can drill down further. Radar also offers a free API for those interested in investigating Internet trends. You can also learn more about the methodologies used in preparing these reports.

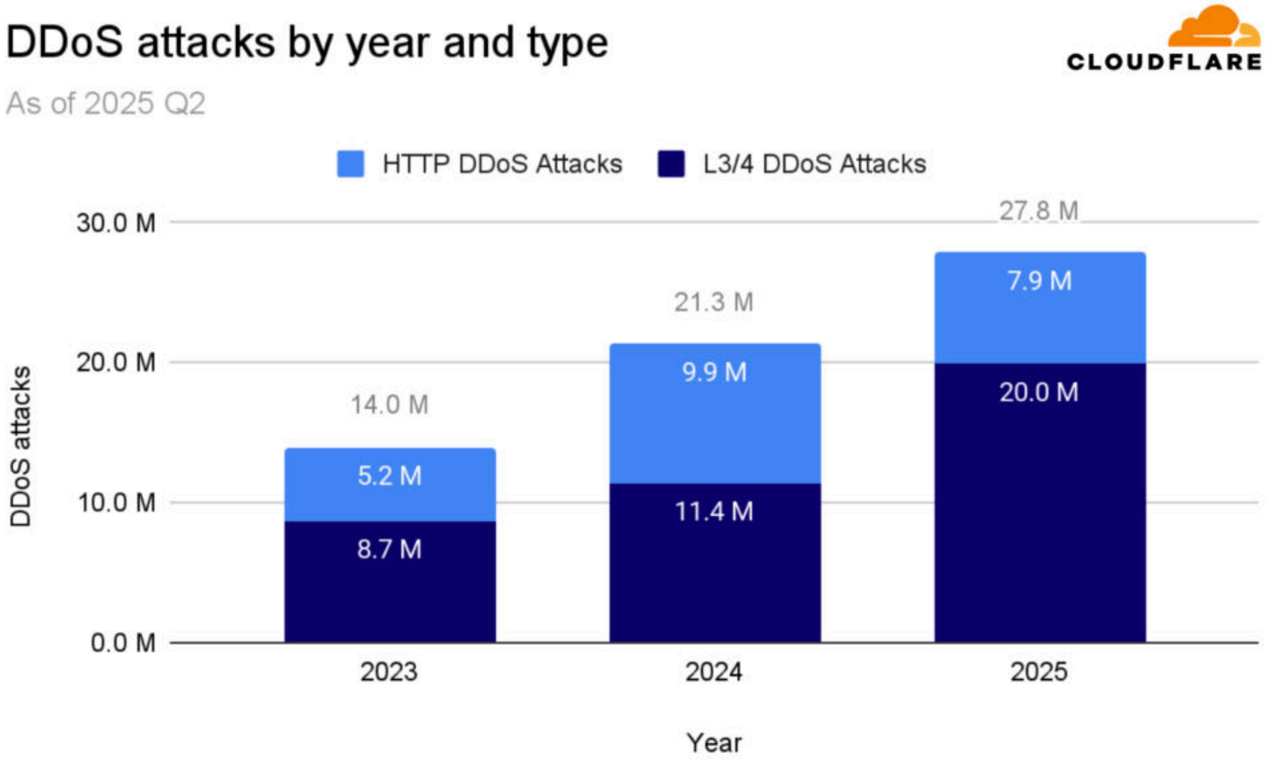
DDoS attacks in numbers

In 2025 Q2, Cloudflare mitigated 7.3 million DDoS attacks — down sharply from 20.5 million in Q1, when an 18-day campaign against Cloudflare's own and other critical infrastructure protected by Cloudflare, drove 13.5 million of those attacks.



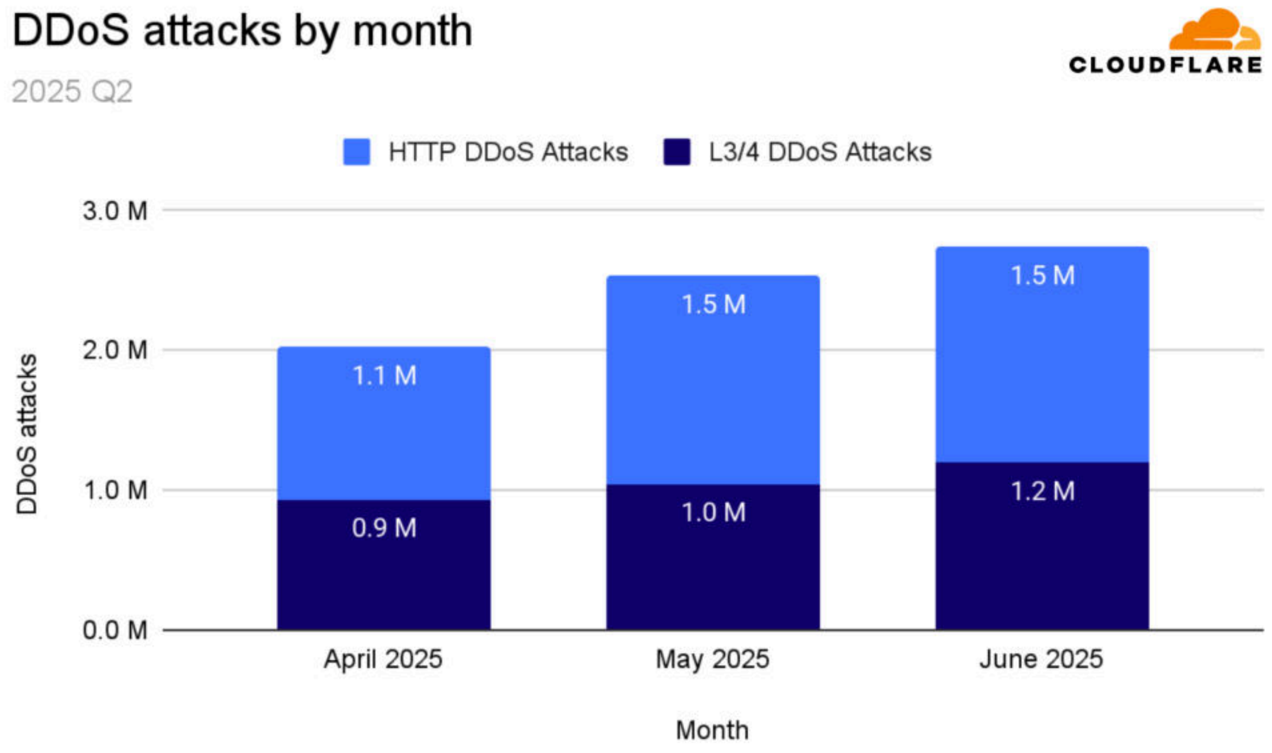
DDoS attacks by quarter

We've just crossed halfway through 2025, and so far Cloudflare has already blocked 27.8 million DDoS attacks, equivalent to 130% of all the DDoS attacks we blocked in the full calendar year 2024.



DDoS attacks by year

Breaking it down further, Layer 3/Layer 4 (L3/4) DDoS attacks plunged 81% quarter-over-quarter to 3.2 million, while HTTP DDoS attacks rose 9% to 4.1 million. Year-over-year changes remain elevated. Overall attacks were 44% higher than 2024 Q2, with HTTP DDoS attacks seeing the largest increase of 129% YoY.

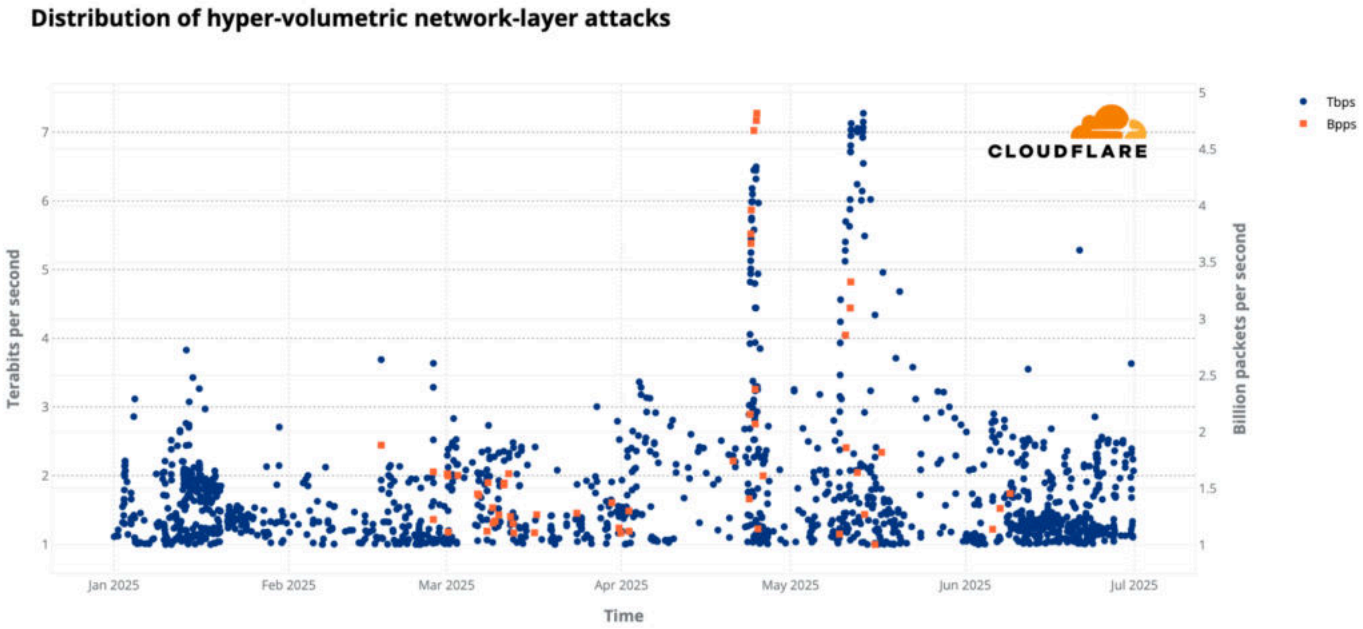


DDoS attacks by month

Hyper-volumetric DDoS attacks

In 2025 Q2, Cloudflare blocked over 6,500 hyper-volumetric DDoS attacks, averaging 71 hyper-volumetric attacks per day. Hyper-volumetric attacks include L3/4 DDoS attacks exceeding 1 Bpps or 1 Tbps, and HTTP DDoS attacks exceeding 1 million requests per second (Mrps).

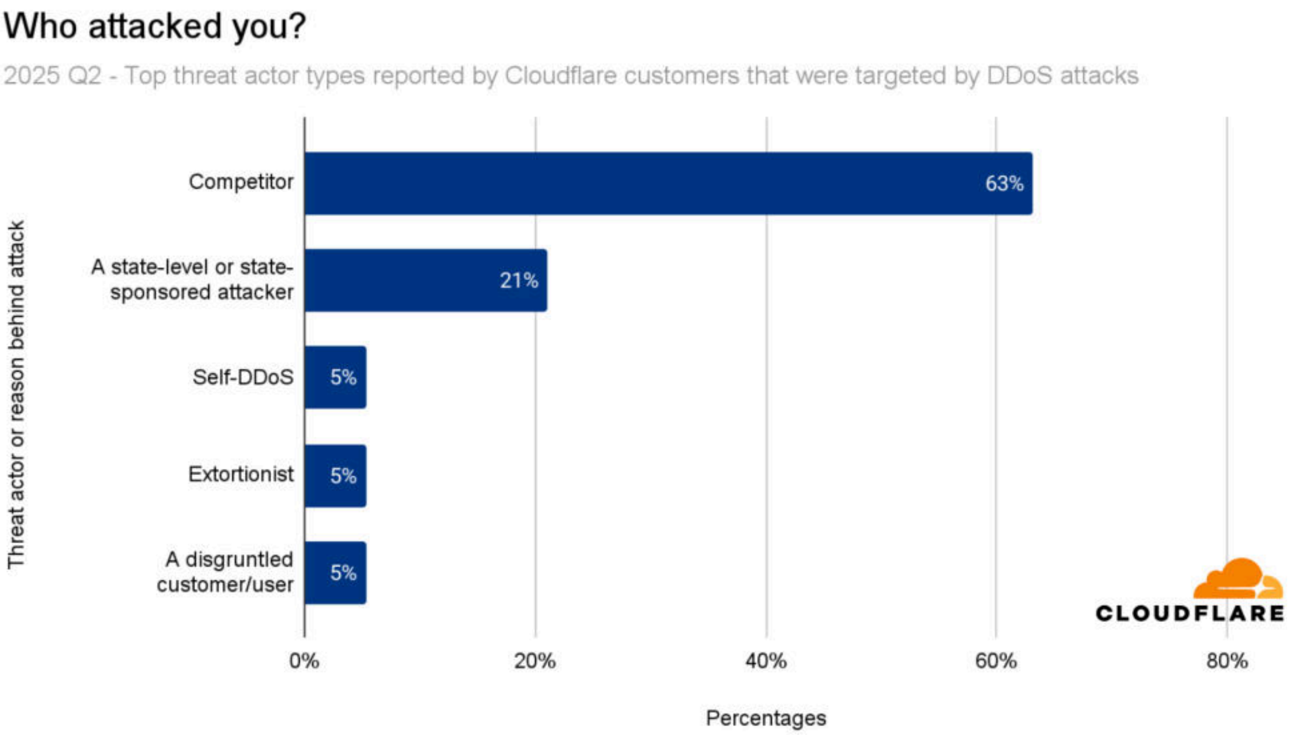
The number of hyper-volumetric DDoS attacks exceeding 100 million packets per second (pps) surged by 592% compared to the previous quarter, and the number exceeding 1 billion pps and 1 terabits per second (Tbps) doubled compared to the previous quarter. The number of HTTP DDoS attacks exceeding 1 million rps (rps) remained the same at around 20 million in total, an average of almost 220,000 attacks every day.



Hyper-volumetric DDoS attacks in 2025 Q2

Threat actors

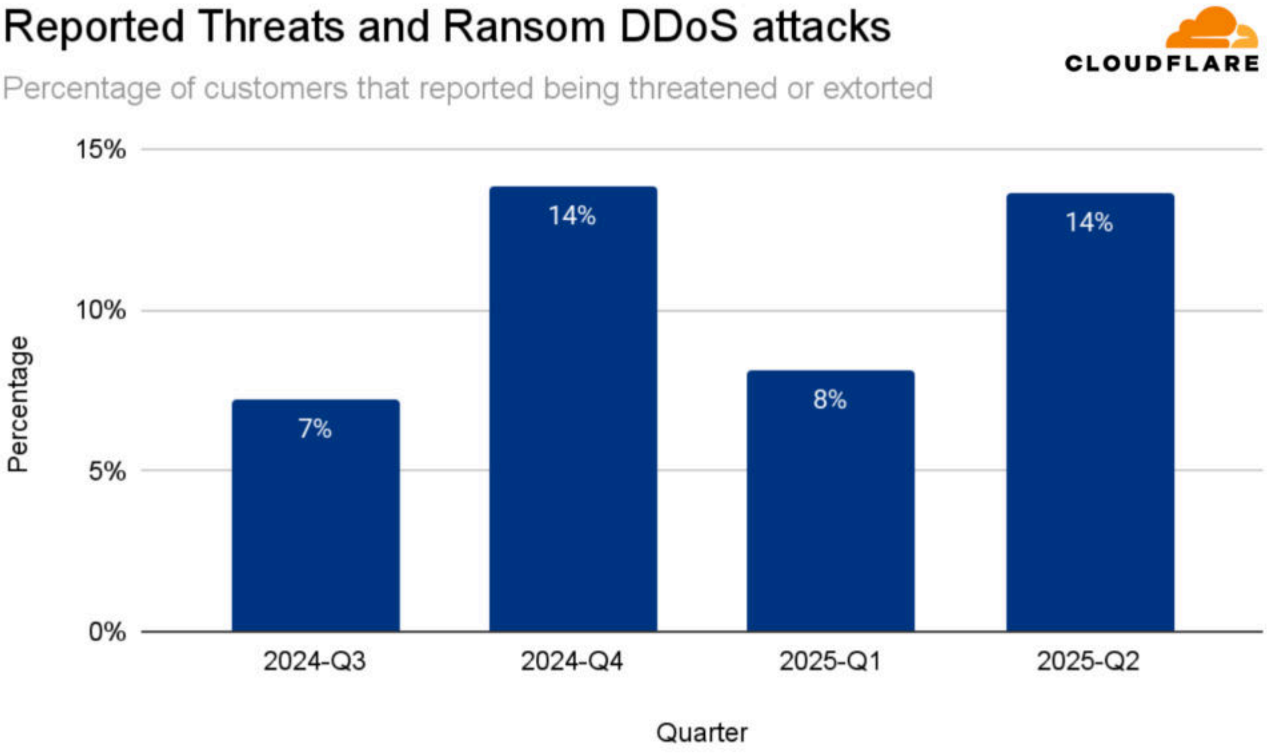
When asked who was behind the DDoS attacks they experienced in 2025 Q2, the majority (71%) of respondents said they didn’t know who attacked them. Of the remaining 29% of respondents that claimed to have identified the threat actor, 63% pointed to competitors, a pattern especially common in the Gaming, Gambling and Crypto industries. Another 21% attributed the attack to state-level or state-sponsored actors, while 5% each said they’d inadvertently attacked themselves (self-DDoS), were targeted by extortionists, or suffered an assault from disgruntled customers/users.



Top threat actors reported in 2025 Q2

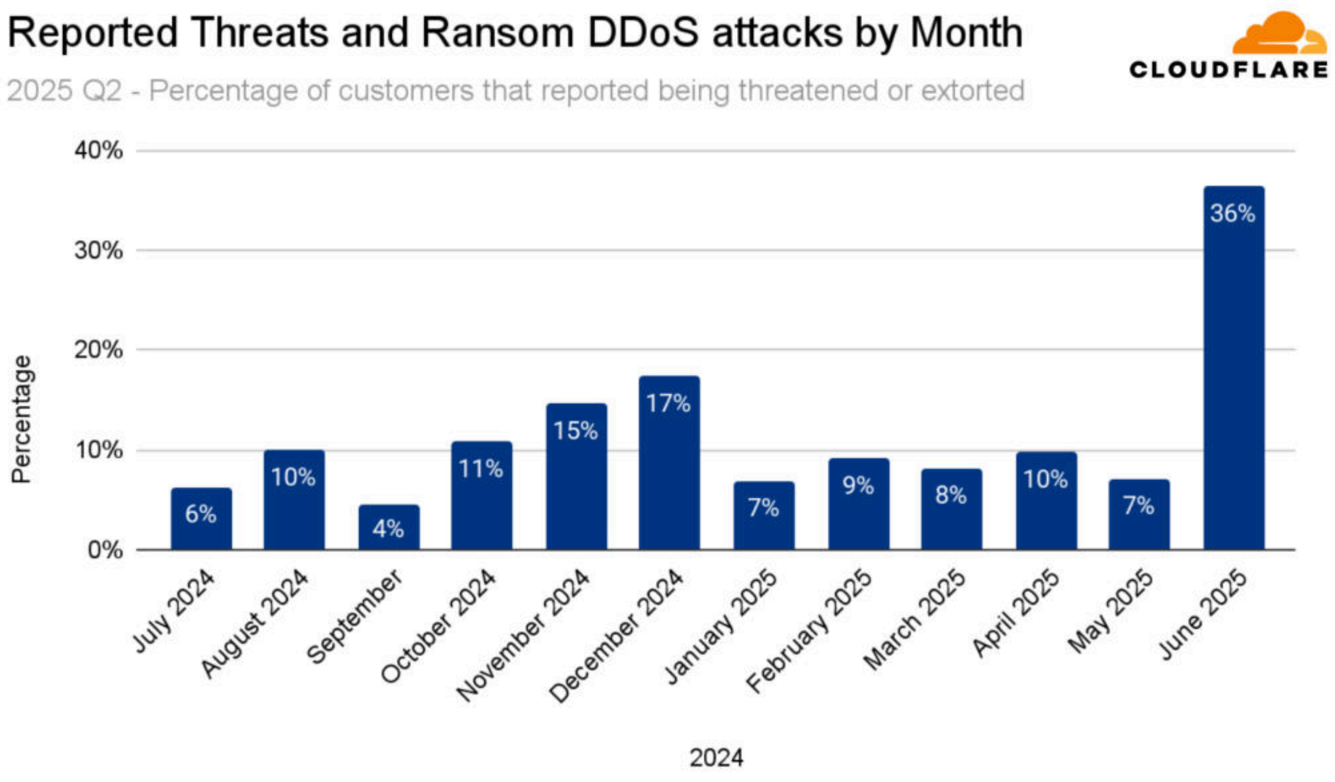
Ransom DDoS attacks

The percentage of attacked Cloudflare customers that reported being targeted by a Ransom DDoS attack or that were threatened increased by 68% compared to the previous quarter, and by 6% compared to the same quarter in 2024.



Ransom DDoS attacks by quarter 2025 Q2

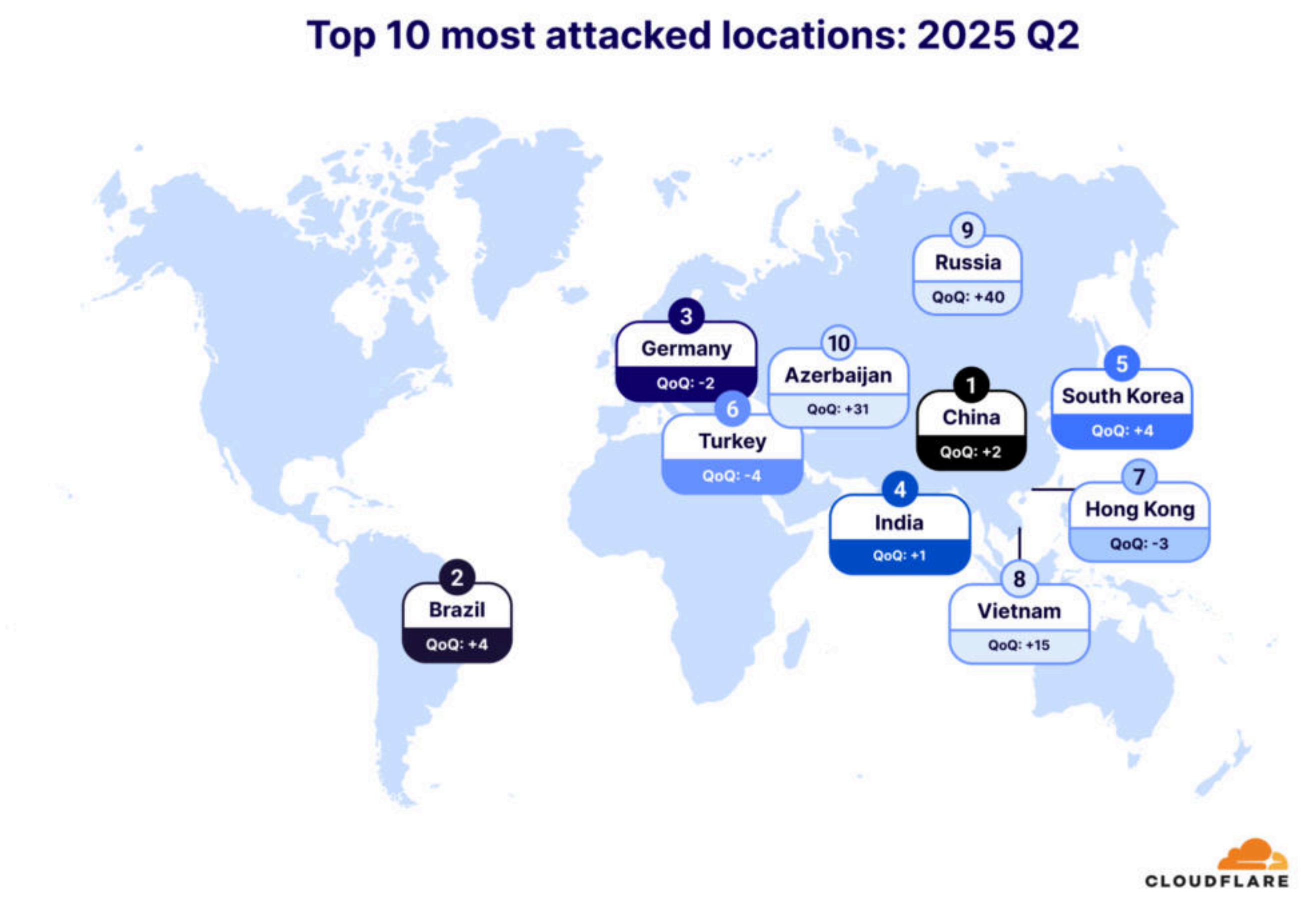
Diving deeper, Ransom DDoS attacks soared in June 2025. Around a third of respondents reported being threatened or subjected to Ransom DDoS attacks.



Ransom DDoS attacks by month 2025 Q2

Top attacked locations

The ranking of the top 10 most attacked locations in 2025 Q2 shifted significantly. China climbed two spots to reclaim first place, Brazil jumped four spots to second place, Germany slipped two spaces to third place, India edged up one to fourth, and South Korea rose four to fifth. Turkey fell four places to sixth, Hong Kong dropped three to seventh, and Vietnam vaulted an astonishing fifteen spots into eighth. Meanwhile, Russia rocketed forty places to ninth, and Azerbaijan surged thirty-one to round out the top ten.



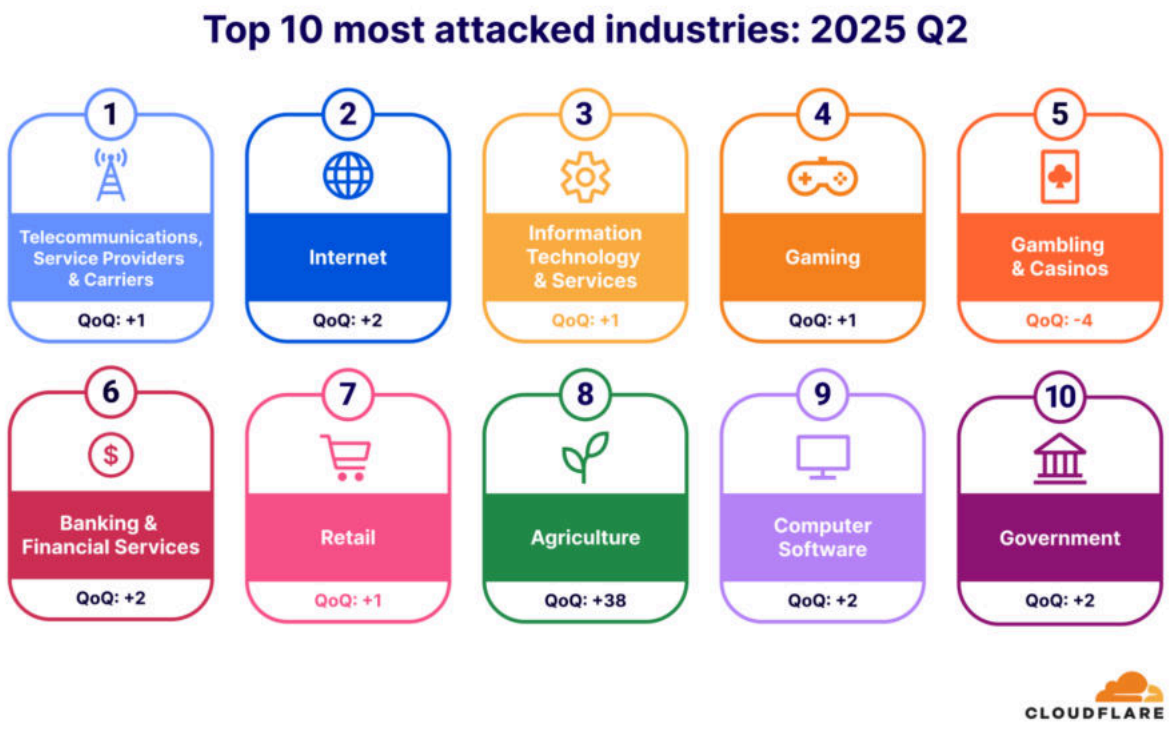
The locations most targeted by DDoS attacks for 2025 Q2

It’s important to note that these attacked locations are determined by the billing country of the Cloudflare customer whose services were targeted — not that those nations themselves are under attack. In other words, a high rank simply means more of our registered customers in that billing jurisdiction were targeted by DDoS traffic, rather than implying direct geopolitical targeting.

Top attacked industries

The ranking of the top 10 most attacked industries in 2025 Q2 also saw notable movement. Telecommunications, Service Providers and Carriers climbed one spot to claim first place, while the Internet sector jumped two spots to second place. Information Technology & Services held its placement as third most attacked, and Gaming rose one spot to fourth place. Gambling & Casinos slipped four spots to fifth place, and the Banking & Financial

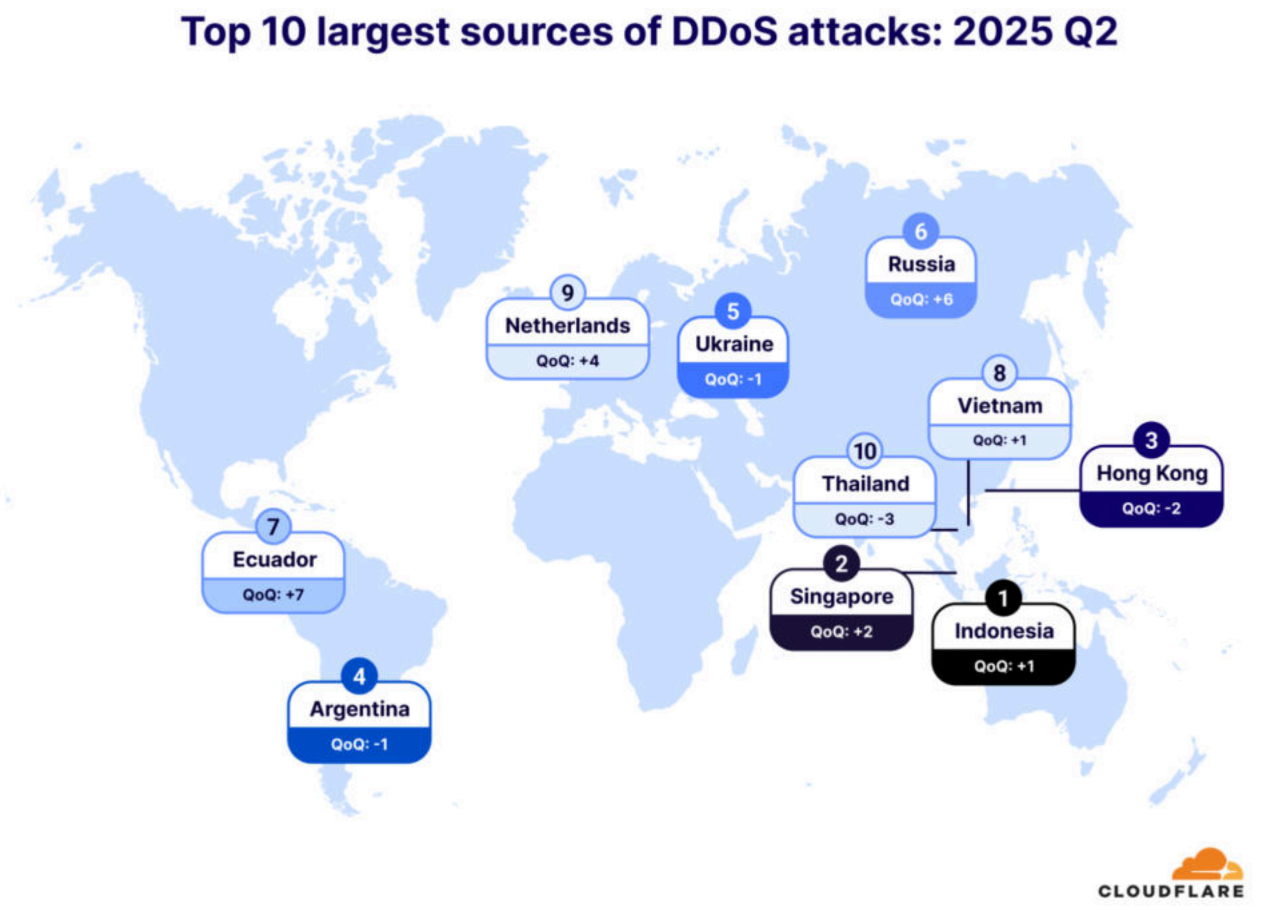
Services industry remained in sixth place. Retail inched up one spot to seventh place, and Agriculture made a dramatic 38-place leap into eighth. Computer Software climbed two spots to ninth place, and Government hopped two places to round out the top ten most attacked industries.



The top attacked industries of DDoS attacks for 2025 Q2

Top sources of DDoS attacks

The ranking of the top 10 largest sources of DDoS attacks in 2025 Q2 also saw several shifts compared to the previous quarter. Indonesia climbed one spot to claim the first place, Singapore jumped two places to second place, Hong Kong dropped two places to third, Argentina slipped one space as fourth and Ukraine held on as the fifth-largest source of DDoS attacks. Russia surged six spots as the sixth-largest source, followed by Ecuador who jumped seven places. Vietnam inched up one place as the eighth-largest source. The Netherlands moved up four places as the ninth-largest source, and Thailand fell three places as the tenth-largest source of DDoS attacks.



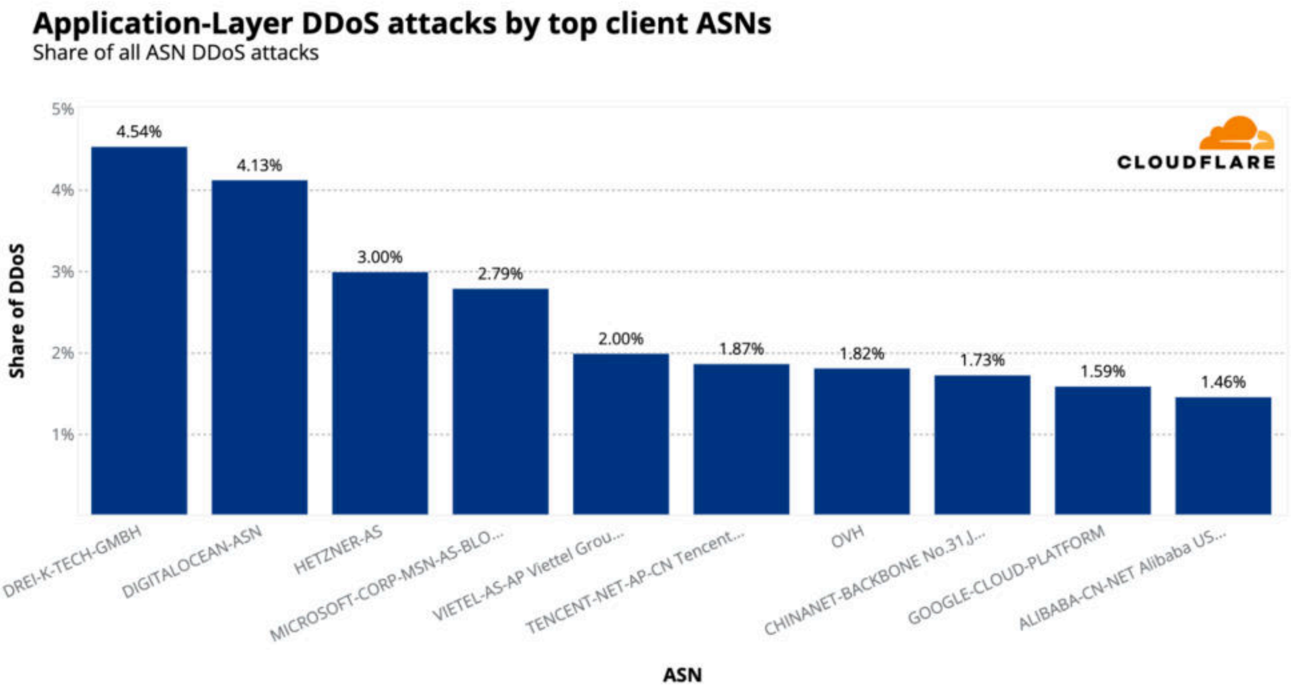
The top sources of DDoS attacks for 2025 Q2

It’s important to note that these “source” rankings reflect where botnet nodes, proxy or VPN endpoints reside — not the actual location of threat actors. For L3/4 DDoS attacks, where IP spoofing is rampant, we geolocate each packet to the Cloudflare data center that first ingested and blocked it, drawing on our presence in over 330 cities for truly granular accuracy.

Top source networks of DDoS attacks

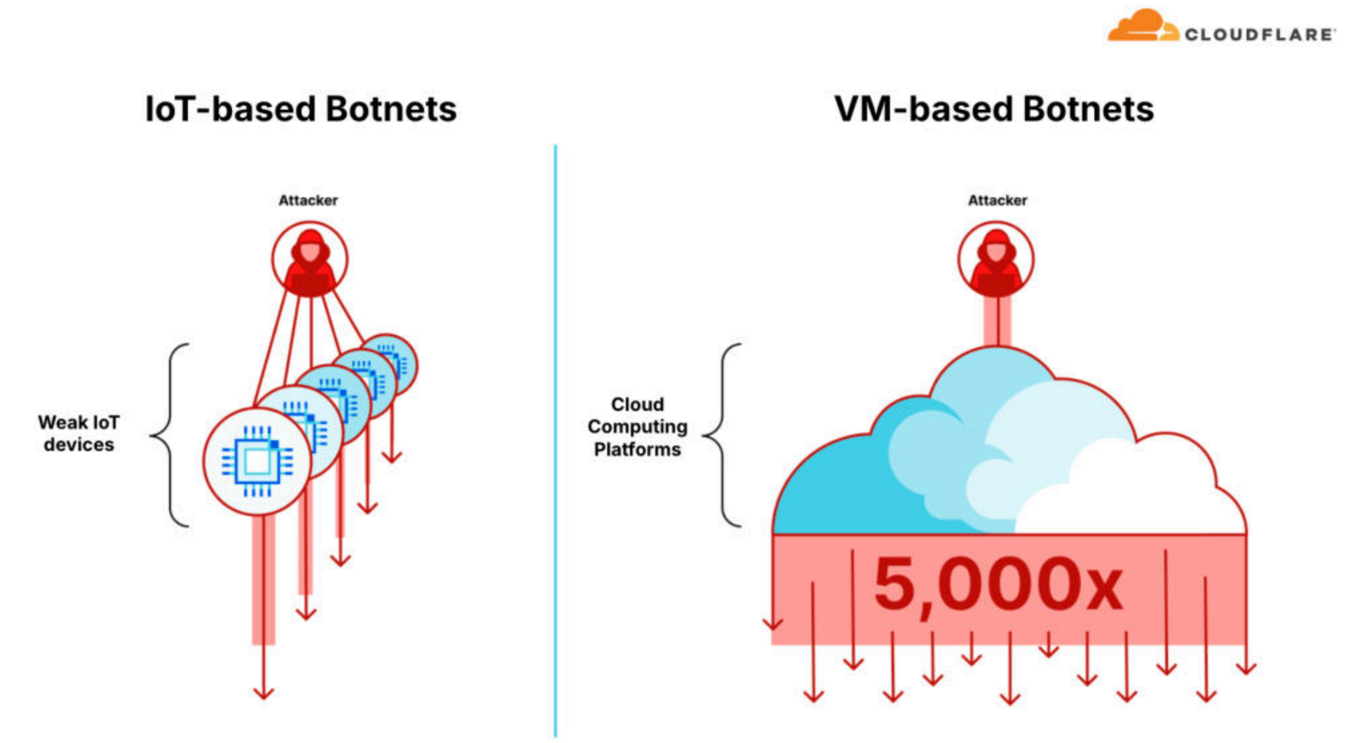
An ASN (Autonomous System Number) is a unique identifier assigned to a network or group of IP networks that operate under a single routing policy on the Internet. It’s used to exchange routing information between systems using protocols like BGP (Border Gateway Protocol).

For the first time in about a year, the German-based Hetzner (AS24940) network dropped from the first place as the largest source of HTTP DDoS attack to the third place. In its place, German-based Drei-K-Tech-GmbH (AS200373), also known as 3xK Tech, jumped 6 places as the number one largest source of HTTP DDoS attacks. The US-based DigitalOcean (AS14061) hopped one spot to the second place.



The top 10 ASN sources of HTTP DDoS attacks

As can be seen in the chart above, 8 out of 10 ASNs listed offer virtual machines (VMs), hosting, or cloud services which indicate the common use of VM-based botnets. These botnets are estimated to be 5,000x stronger than IoT-based botnets. Only Drei (AS200373) and ChinaNet Backbone (AS4134) are primarily ISPs or telecom carriers without significant public VM/cloud offerings.



IoT-based botnets versus VM-based botnets

To help hosting providers, cloud computing providers and any Internet service providers identify and take down the abusive accounts that launch these attacks, we leverage Cloudflare's unique vantage point to provide a free DDoS Botnet Threat Feed for Service Providers. Over 600 organizations worldwide have already signed up for this feed, and we've already seen great collaboration across the community to take down botnet nodes. This is possible thanks to the threat feed which provides these service providers a list of offending IP addresses from within their ASN that we see launching HTTP DDoS attacks. It's completely free and all it takes is opening a free Cloudflare account, authenticating the ASN via PeeringDB, and then fetching the threat intelligence via API.

With a simple API call, service providers can get a list of offending IPs from within their network. An example response is provided below.

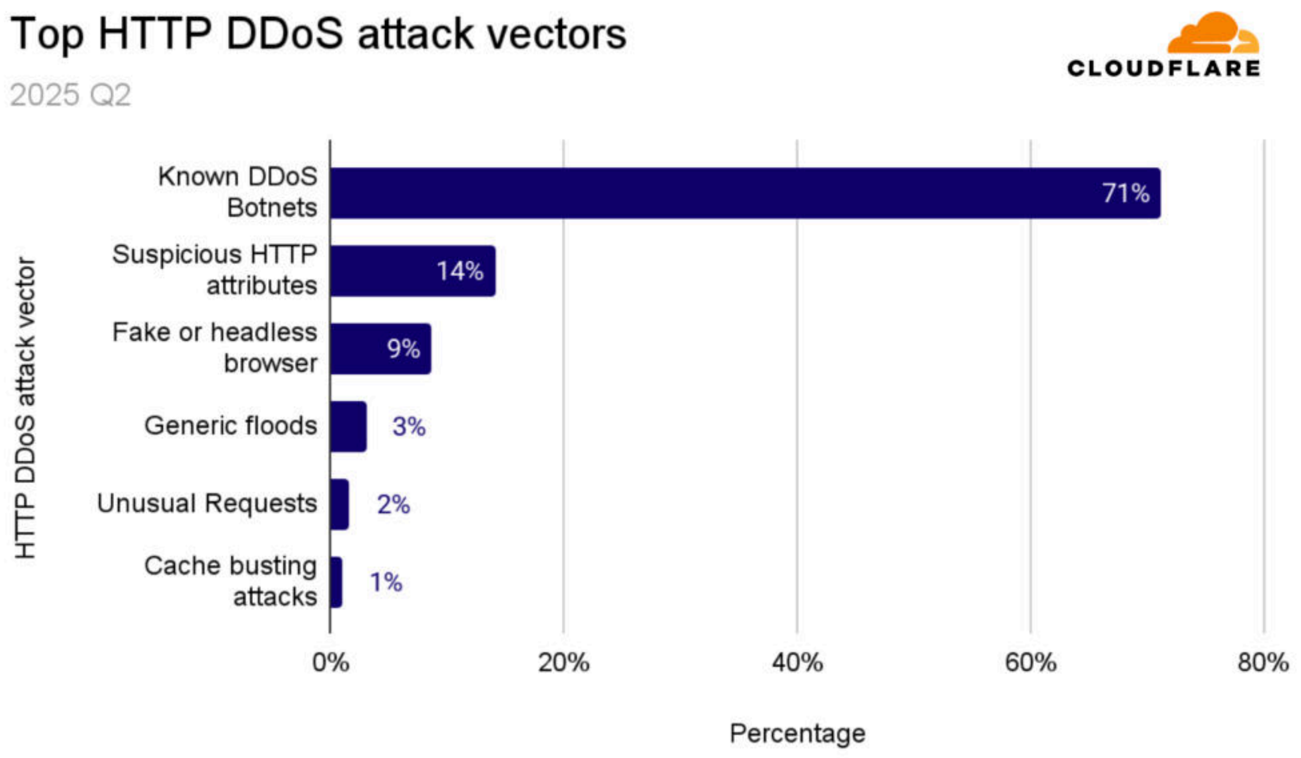
```
{
  "result": [
    {
      "cidr": "127.0.0.1/32",
      "date": "2024-05-05T00:00:00Z",
      "offense_count": 10000
    },
    // ... other entries ...
  ],
  "success": true,
  "errors": [],
  "messages": []
}
```

Example response from the free ISP DDoS Botnet Threat Feed API

Attack vectors

Defending against DDoS Botnets

In Q2 2025, the majority (71%) of HTTP DDoS attacks were launched by known botnets. Rapid detection and blocking of these attacks was possible as a result of operating a massive network and seeing many different types of attacks and botnets. By leveraging real-time threat intelligence, our systems are able to incriminate DDoS botnets very fast, contributing to a more effective mitigation. Even if a DDoS botnet has been incriminated while targeting only one website or IP address, our entire network and customer base is immediately protected against it. This real-time threat intelligence system adapts with botnets as they morph and change nodes.

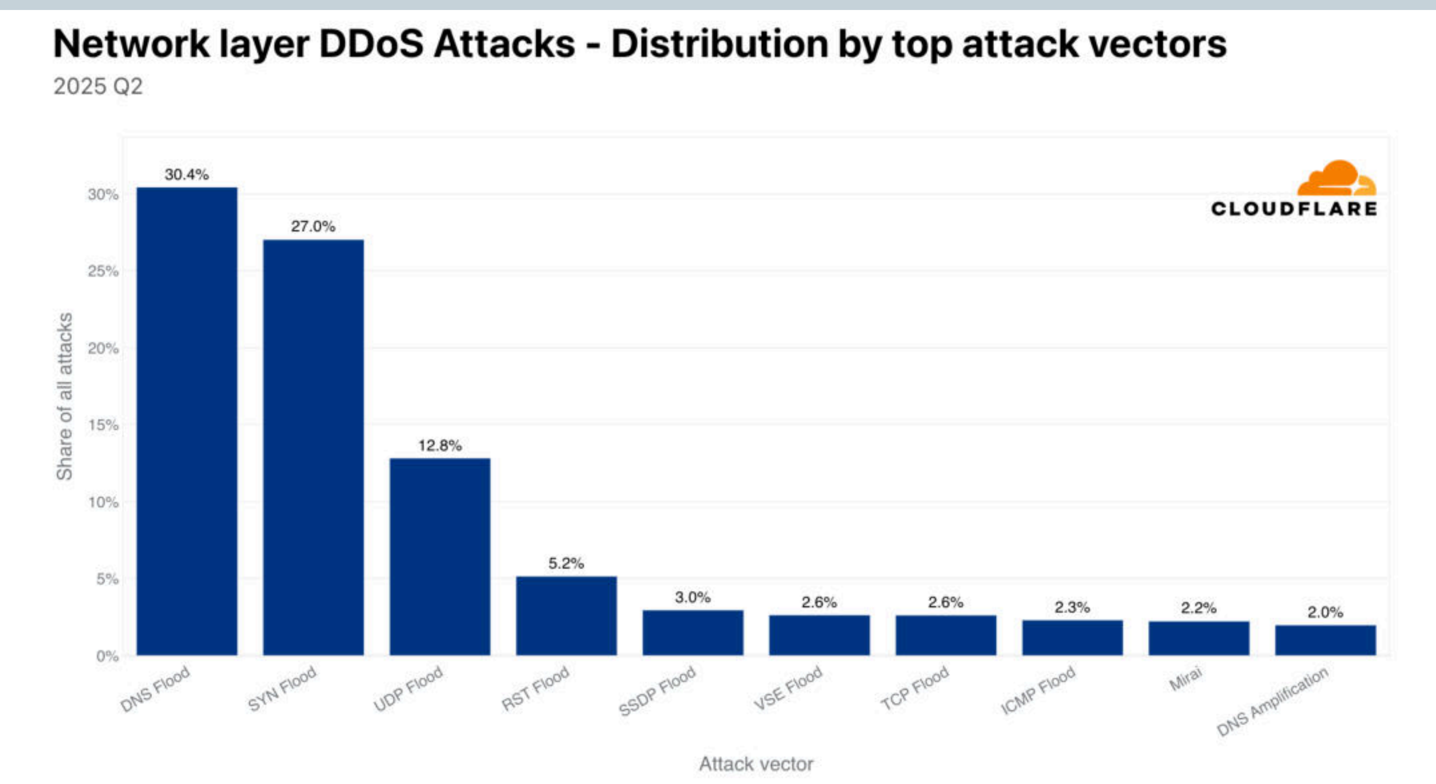


The top HTTP DDoS attack vectors for 2025 Q2

L3/4 attack vectors

In Q2 2025, DNS flood attacks were the top L3/4 attack vector accounting for almost a third of all L3/4 DDoS attacks. SYN floods was the second most common attack vector, dipping from 31% in Q1 to 27% in Q2.

In third place, UDP floods also grew meaningfully, rising from 9% in Q1 to 13% in Q2. RST floods, another form of TCP-based DDoS attacks, accounting for 5% of all L3/4 attacks, was the fourth most common vector. Rounding out the top five, SSDP floods edged into fifth place at 3% despite a decline from 4.3% last quarter, but enough to push the previously prevalent Mirai attacks (which fell from 18% in Q1 to just 2% in Q2) out of the top five altogether.



The top L3/4 DDoS attack vectors for 2025 Q2

Breakdown of the top 3 L3/4 DDoS attack vectors

Below are details about the top 3 most common L3/4 DDoS attacks. We provide recommendations on how organizations can avoid becoming a reflection and amplification element, and also recommendations on how to defend against these attacks whilst avoiding impact to legitimate traffic. Cloudflare's customers are protected against these attacks.

DNS Flood Attack

- **Type:** Flood
- **How it works:** A DNS flood aims to overwhelm a DNS server with a high volume of DNS queries—either valid, random, or malformed—to exhaust CPU, memory, or bandwidth. Unlike amplification attacks, this is a direct flood aimed at degrading performance or causing outages, often over UDP port 53, but sometimes over TCP as well (especially for DNS-over-TCP or DNSSEC-enabled zones).

- **How to defend against the attack:** Use Cloudflare DNS as primary or secondary, Cloudflare DNS Firewall and/or Cloudflare Magic Transit to absorb and mitigate query floods before they reach your origin. Cloudflare's global network handles tens of millions of DNS queries per second with built-in DDoS filtering and query caching, blocking malformed or excessive traffic while answering legitimate requests.

- **How to avoid unintended impact:** Avoid blocking all DNS traffic or disabling UDP port 53, which would break normal resolution. Rely on Cloudflare's DNS-specific protection such as the Advanced DNS Protection system, and deploy DNSSEC-aware protection to handle TCP-based query floods safely.

SYN Flood Attack

- **Type:** Flood

- **How it works:** In a SYN flood, threat actors send a large volume of TCP SYN packets—often with spoofed IP addresses—to initiate connections that are never completed. This leaves the target system with half-open connections, consuming memory and connection tracking resources, potentially exhausting server limits and preventing real clients from connecting.

- **How to defend against the attack:** Use Cloudflare Magic Transit to intercept and mitigate TCP SYN floods at the edge. Cloudflare leverages SYN cookies, connection tracking, and behavioral analysis to distinguish real clients from spoofed or malicious sources, ensuring legitimate TCP connections are completed successfully. Using Cloudflare's CDN/WAF services or Cloudflare Spectrum which are both reverse-proxy services for HTTP or TCP, respectively. Using a reverse-proxy basically eliminates the possible impact of TCP-based DDoS attacks.

- **How to avoid unintended impact:** Blocking all SYN traffic or applying aggressive timeouts can block real users. Instead, rely on Cloudflare's Advanced TCP protection system, which uses SYN rate shaping, anomaly detection, and spoofed-packet filtering to mitigate attacks without affecting genuine client connections.

UDP DDoS attack

- **Type**: Flood

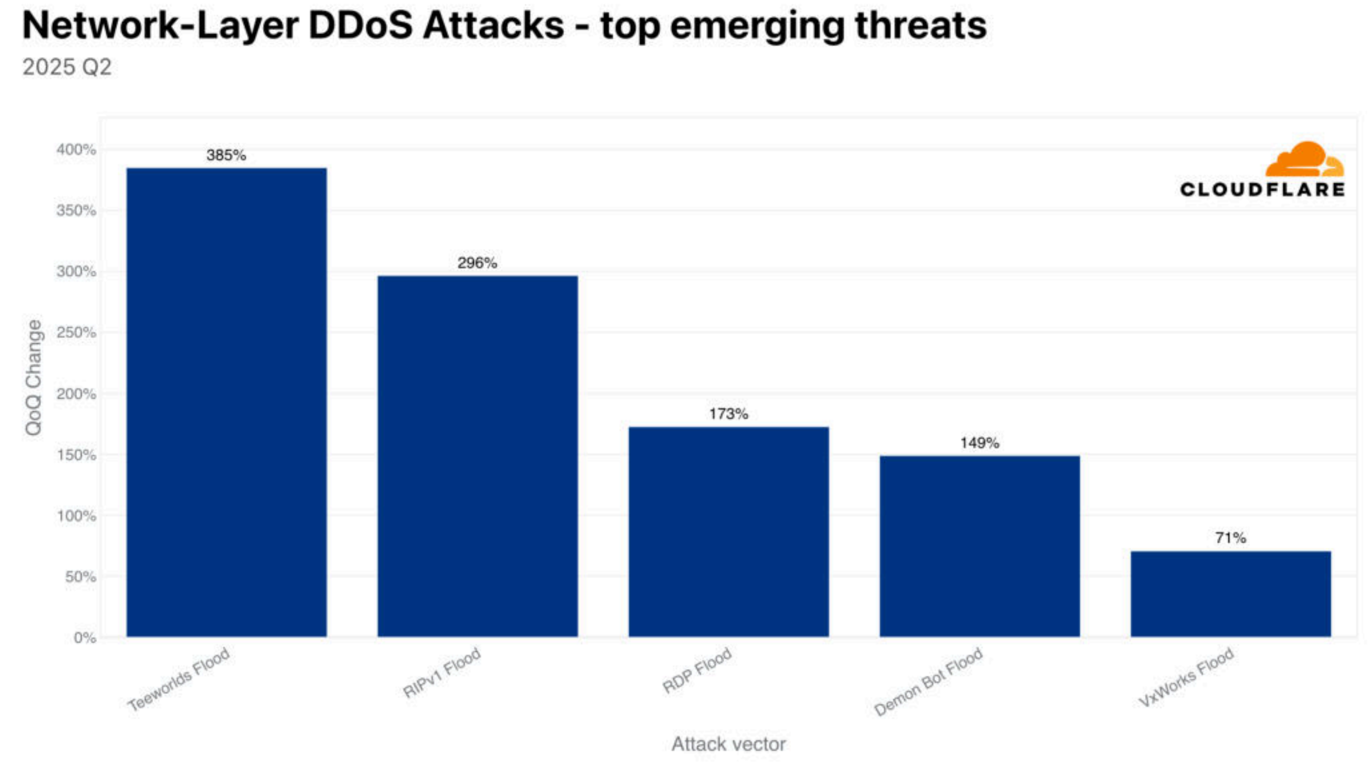
- **How it works**: A high volume of UDP packets is sent to random or specific ports on the target IP address(es). It may attempt to saturate the Internet link or overwhelm its in-line appliances with more packets than it can handle in order to create disruption or an outage.

- **How to defend against the attack**: Deploy cloud-based volumetric DDoS protection that can fingerprint attack traffic in real-time such as Cloudflare Magic Transit or Cloudflare Spectrum, apply smart rate-limiting on UDP traffic, and drop unwanted UDP traffic altogether with the Magic Firewall.

- **How to avoid unintended impact**: Aggressive filtering may disrupt legitimate UDP services such as VoIP, video conferencing, or online games. Apply thresholds carefully.

Emerging threats

Among emerging L3/4 DDoS threats in 2025 Q2, Teeworlds flood saw the biggest spike. These attacks jumped 385% QoQ, followed by the RIPv1 flood, which surged 296%. RDP floods climbed by 173%, and Demon Bot floods increased by 149%. Even the venerable VxWorks flood made a comeback, rising 71% quarter-over-quarter. These dramatic upticks highlight threat actors' ongoing experimentation with lesser-known and legacy protocols to evade standard defenses.



The top emerging threats for 2025 Q2

Breakdown of the top emerging threats

Below are details about the emerging threats for 2025 Q2, mostly recycling of very old attack vectors. We provide recommendations on how organizations can avoid becoming a reflection and amplification element, and also recommendations on how to defend against these attacks whilst avoiding impact to legitimate traffic. Cloudflare's customers are protected against these attacks.

Teeworlds DDoS Attack

- **Type:** Flood
- **How it works:** Teeworlds is a fast-paced, open-source 2D multiplayer shooter game that uses a custom UDP-based protocol for real-time gameplay. Threat actors flood the target’s game server with spoofed or excessive UDP packets that mimic in-game actions or connection attempts. This can overwhelm server resources and cause lag or outages.

- **How to defend against the attack:** Use Cloudflare Spectrum or Cloudflare Magic Transit to protect the servers. Cloudflare automatically detects and mitigates these types of attacks using real-time fingerprinting, blocking attack traffic while allowing real players through. Magic Transit also provides a packet-level firewall capability, the Magic Firewall which can be used to craft custom protection.

- **How to avoid unintended impact:** When crafting custom rules, avoid blocking or aggressively rate-limiting UDP port 8303 directly as it can disrupt overall gameplay. Instead, rely on intelligent detection and mitigation services to avoid affecting legitimate users.

Teeworlds Screenshot Jungle. Source: Wikipedia

RIPv1 DDoS attack

- **Type**: Reflection + (Low) Amplification

- **How it works**: Exploits the Routing Information protocol version 1 (RIPv1), an old unauthenticated distance-vector routing protocol that uses UDP/520. Threat actors send spoofed routing updates to flood or confuse networks.

- **How to prevent becoming a reflection / amplification element**: Disable RIPv1 on routers. Use RIPv2 with authentication where routing is needed.

- **How to defend against the attack**: Block inbound UDP/520 from untrusted networks. Monitor for unexpected routing updates.

- **How to avoid unintended impact**: RIPv1 is mostly obsolete; disabling it is generally safe. If legacy systems rely on it, validate routing behavior before changes.

RDP DDoS Attack

- **Type**: Reflection + Amplification

- **How it works**: The Remote Desktop Protocol (RDP) is used for remote access to Windows systems and typically runs over TCP port 3389. In some misconfigured or legacy setups, RDP can respond to unauthenticated connection attempts, making it possible to abuse for reflection or amplification. Threat actors send spoofed RDP initiation packets to exposed servers, causing them to reply to a victim, generating high volumes of unwanted traffic.

- **How to defend against the attack**: Use Cloudflare Magic Transit to protect your network infrastructure. Magic Transit provides L3/L4 DDoS protection, filtering out spoofed or malformed RDP traffic before it reaches your origin. For targeted application-layer abuse, Cloudflare Gateway or Zero Trust Network Access (ZTNA) can help secure remote desktop access behind authenticated tunnels.

- **How to avoid unintended impact**: Do not block TCP/3389 globally if RDP is actively used. Instead, restrict RDP access to known IPs or internal networks, or use Cloudflare Tunnel with Zero Trust Network Access (ZTNA) to remove public exposure altogether while maintaining secure access for legitimate users.

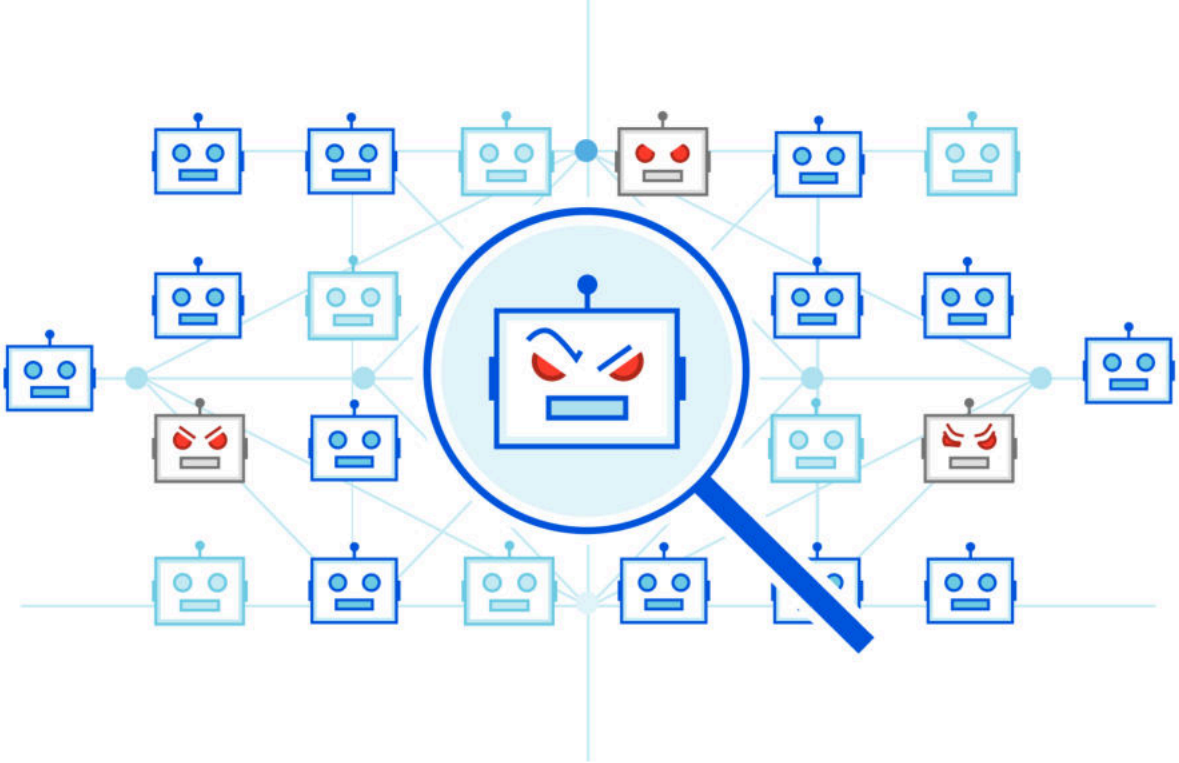
DemonBot DDoS Attack

- **Type**: Botnet-based Flood

- **How it works**: DemonBot is a malware strain that infects Linux-based systems—particularly unsecured IoT devices—via open ports or weak credentials. Once infected, devices become part of a botnet that can launch high-volume UDP, TCP, and application-layer floods. Attacks are typically command-and-control (C2) driven and can generate significant volumetric traffic, often targeting gaming, hosting, or enterprise services. To avoid infection, leverage antivirus software and domain filtering.

- **How to defend against the attack**: Use Cloudflare Magic Transit to absorb and filter large-scale network-layer floods before they reach your infrastructure. Cloudflare's real-time traffic analysis and signature-based detection neutralize traffic originating from DemonBot-infected devices. For application-layer services, Cloudflare DDoS protection and WAF can mitigate targeted HTTP floods and connection abuse.

- **How to avoid unintended impact**: Instead of broadly blocking traffic types or ports, rely on Cloudflare's adaptive mitigation to distinguish between legitimate users and botnet traffic. Combine with IP reputation filtering, geo-blocking, and rate limiting to reduce false positives and maintain service availability.

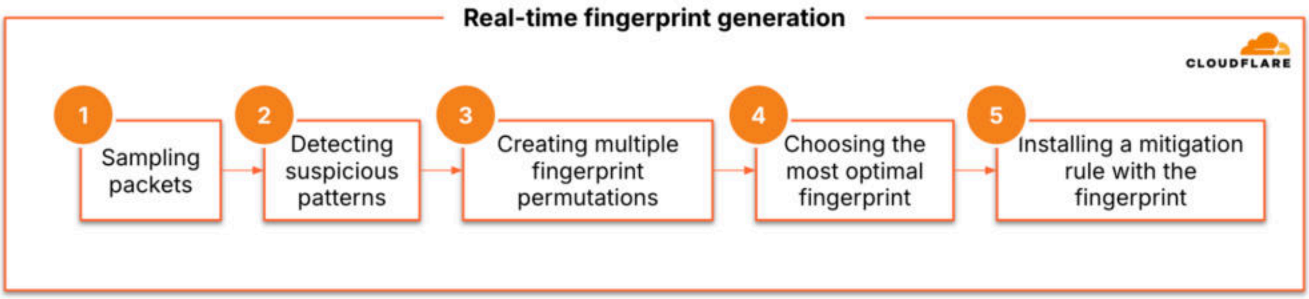


VxWorks Flood DDoS Attack

- ### Type: Flood (IoT-based)
- **How it works:** VxWorks is a real-time operating system (RTOS) used in millions of embedded and IoT devices (e.g., routers, industrial controllers). Devices running outdated or misconfigured versions of VxWorks can be compromised and used to launch DDoS attacks. Once infected—often via public exploits or weak credentials—they send high volumes of UDP, TCP, or ICMP traffic to overwhelm targets, similar to traditional IoT botnets.

- **How to defend against the attack:** Deploy Cloudflare Magic Transit to block volumetric traffic at the network edge. Cloudflare uses real-time fingerprinting and proprietary heuristics to identify traffic from compromised VxWorks devices and mitigate it in real-time. For application services, Cloudflare's DDoS mitigation and **Gateway services** provide additional protection against protocol-level abuse.

- **How to avoid unintended impact:** Avoid over-blocking UDP or ICMP traffic, as it may disrupt legitimate diagnostics or real-time services. Instead, use Cloudflare's intelligent filtering, rate limiting, and geo/IP reputation tools to safely mitigate attacks while avoiding impact to legitimate traffic.


Real-time fingerprint generation
CLOUDFLARE
1
Sampling packets
2
Detecting suspicious patterns
3
Creating multiple fingerprint permutations
4
Choosing the most optimal fingerprint
5
Installing a mitigation rule with the fingerprint

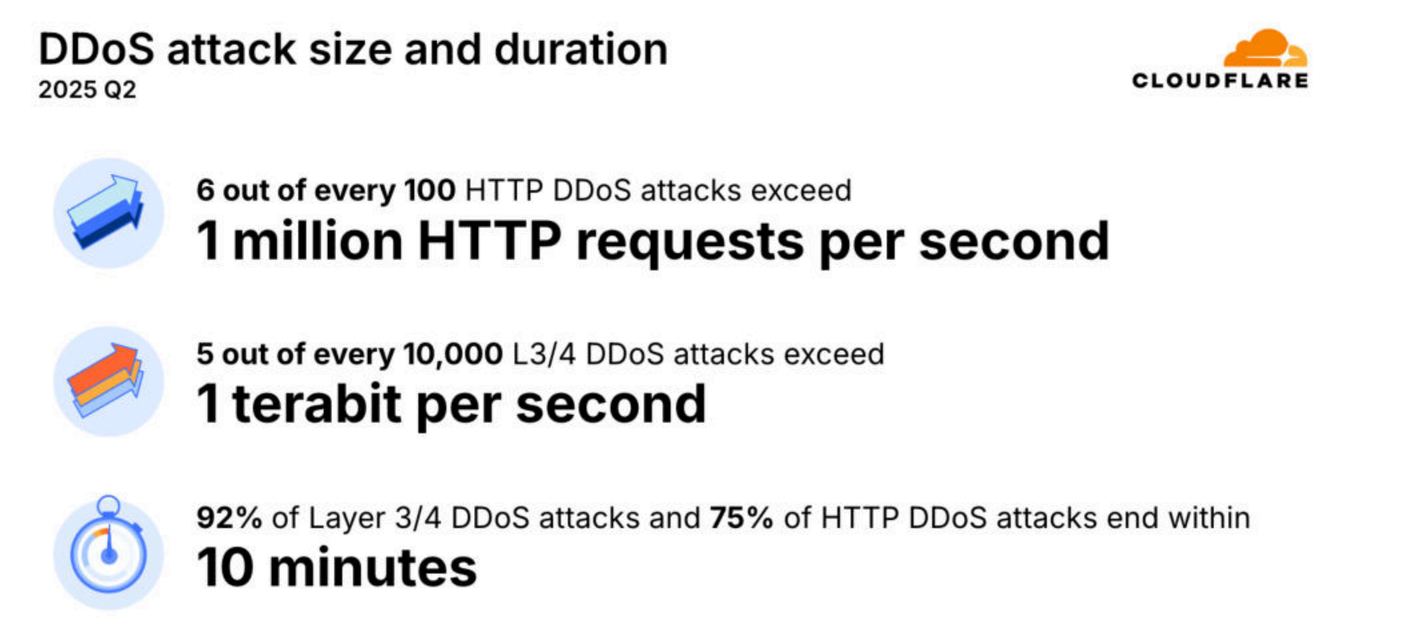
Cloudflare’s real-time fingerprint generation flow

Attack size & duration

Most DDoS attacks are small and short. In 2025 Q2, 94% of L3/4 DDoS attacks didn’t exceed 500 Mbps. Similarly, around 85% of L3/4 DDoS attacks didn’t exceed 50,000 pps. The majority of HTTP DDoS attacks are also small, 65% stay below 50K rps. “Small”, though, is a relative term.

An average modern server typically refers to a general-purpose physical or virtual machine with around 4–8 CPU cores (e.g. Intel Xeon Silver), 16–64 GB RAM, and a 1 Gbps NIC, running a Linux OS like Ubuntu or CentOS with NGINX or similar software. This setup can handle ~100,000–500,000 pps, up to ~940 Mbps throughput, and around 10,000–100,000 rps for static content or 500–1,000 rps for database-backed dynamic applications, depending on tuning and workload.

Assuming the server is unprotected by a cloud DDoS protection service, if it’s targeted by “small” DDoS attacks during peak time traffic rates, it is very likely that the server won’t be able to handle it. Even “small” DDoS attacks can cause significant impact to unprotected servers.



DDoS attack size and duration
2025 Q2

CLOUDFLARE

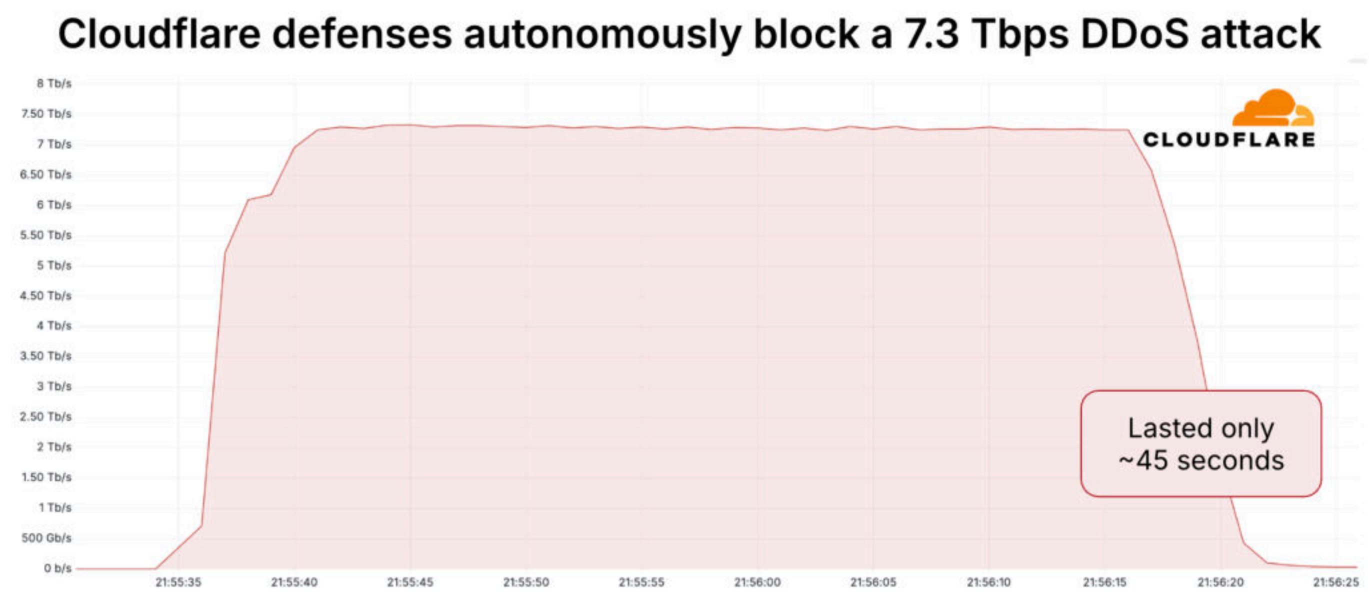
6 out of every 100 HTTP DDoS attacks exceed
1 million HTTP requests per second

5 out of every 10,000 L3/4 DDoS attacks exceed
1 terabit per second

92% of Layer 3/4 DDoS attacks and **75%** of HTTP DDoS attacks end within
10 minutes

DDoS attacks size and duration in 2025 Q2

While the majority of DDoS attacks are small, hyper-volumetric DDoS attacks are increasing in size and frequency. 6 out of every 100 HTTP DDoS attacks exceed 1M rps, and 5 out of every 10,000 L3/4 DDoS attacks exceed 1 Tbps — a 1,150% QoQ increase.



Lasted only ~45 seconds

The largest attack in the world: 7.3 Tbps

Most DDoS attacks are short in duration, even the largest and most intense ones. Threat actors often rely on brief bursts of concentrated traffic— sometimes lasting as little as 45 seconds as seen with the monumental 7.3

Tbps DDoS attack — in an attempt to avoid detection, overwhelm targets and cause maximum disruption before defenses can fully activate. This tactic of short, high-intensity bursts makes detection and mitigation more challenging and underscores the need for always-on, real-time protection. Thankfully, Cloudflare’s autonomous DDoS defenses kick in immediately.

Helping build a better Internet

At Cloudflare, we’re committed to helping build a better Internet. A part of that mission is offering free, unmetered DDoS protection regardless of size, duration and quantity. We don’t just defend against DDoS attacks. The best defense is a good offense, and using our free ISP Botnet Threat Feed, we contribute to botnet takedowns.

While many still adopt protection reactively or rely on outdated solutions, our data shows proactive, always-on security is far more effective. Powered by a global network with 388 Tbps capacity across 330+ cities, we provide automated, in-line, battle-proven defense against all types of DDoS attacks.