4.2 Tbps of bad packets and a whole lot more: Cloudflare's Q3 DDoS report

2024-10-23

 Omer Yoachimik  Jorge Pacheco

9 min read

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

Welcome to the 19th edition of the Cloudflare DDoS Threat Report. Released quarterly, these reports provide an in-depth analysis of the DDoS threat landscape as observed across the Cloudflare network. This edition focuses on the third quarter of 2024.

With a 296 Terabit per second (Tbps) network located in over 330 cities worldwide, Cloudflare is used as a reverse proxy by nearly 20% of all websites. Cloudflare holds a unique vantage point to provide valuable insights and trends to the broader Internet community.

Key insights

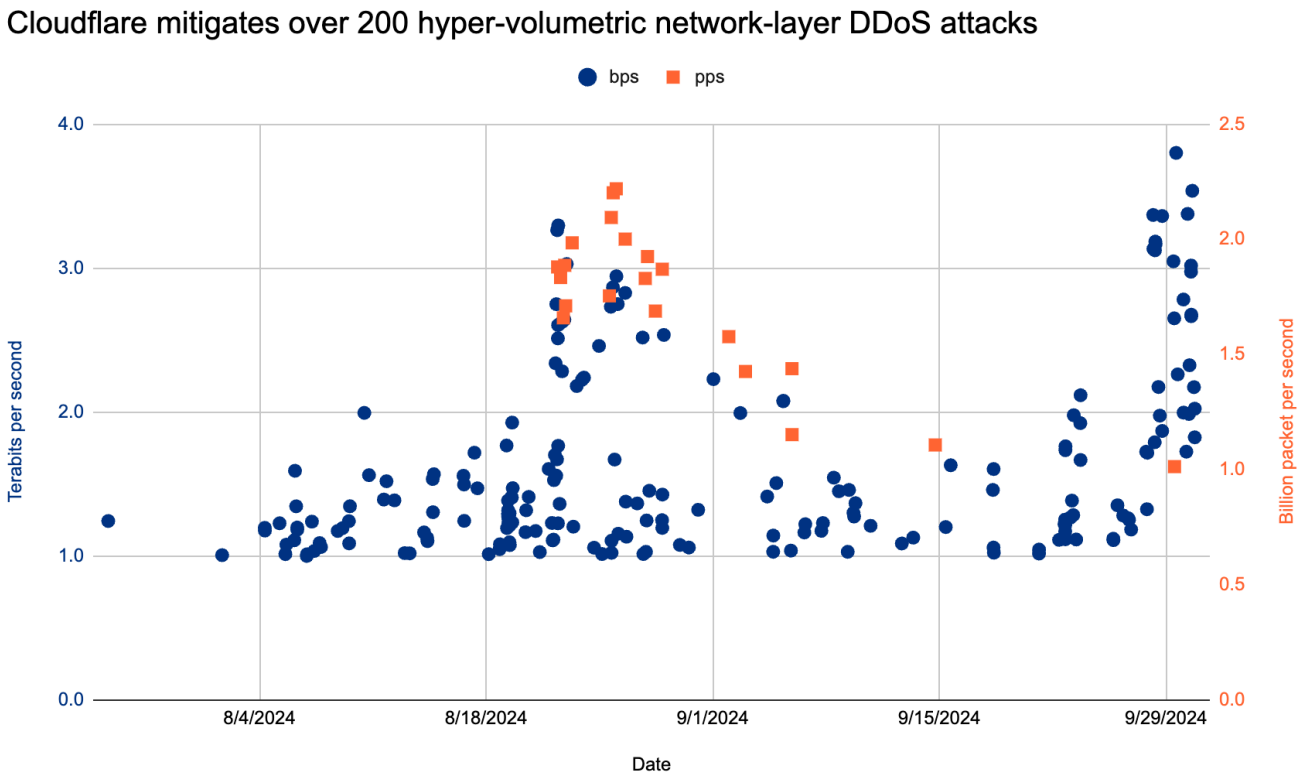
- The number of DDoS attacks spiked in the third quarter of 2024. Cloudflare mitigated nearly 6 million DDoS attacks, representing a 49% increase QoQ and 55% increase YoY.
- Out of those 6 million, Cloudflare's autonomous DDoS defense systems detected and mitigated over 200 hyper-volumetric DDoS attacks exceeding rates of 3 terabits per second (Tbps) and 2 billion packets per second (Bpps). The largest attack peaked at 4.2 Tbps and lasted just a minute.
- The Banking & Financial Services industry was subjected to the most DDoS attacks. China was the country most targeted by DDoS attacks, and Indonesia was the largest source of DDoS attacks.

To learn more about DDoS attacks and other types of cyber threats, visit our Learning Center, access previous DDoS threat reports on the Cloudflare blog, or visit our interactive hub, Cloudflare Radar. There's also a free API for those interested in investigating these and other Internet trends. You can also learn more about the methodologies used in preparing these reports.

Hyper-volumetric campaign

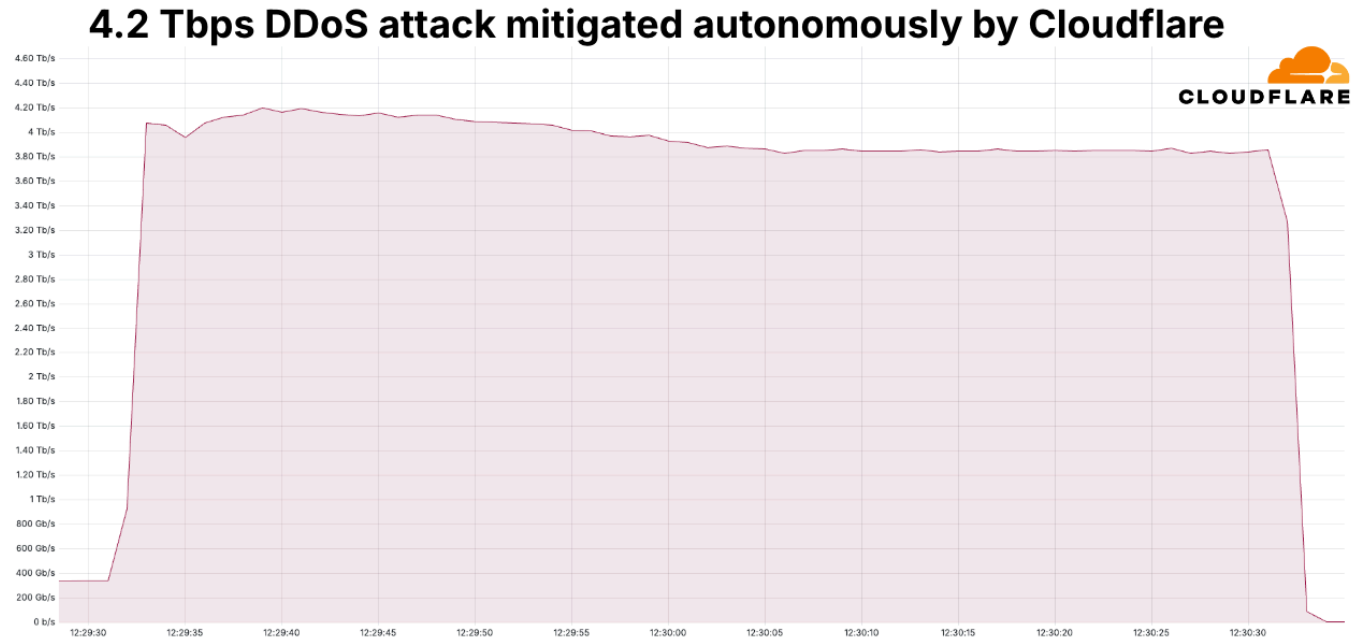
In the first half of 2024, Cloudflare's autonomous DDoS defense systems automatically detected and mitigated 8.5 million DDoS attacks: 4.5 million in Q1 and 4 million in Q2. In Q3, our systems mitigated nearly 6 million DDoS attacks bringing it to a total of 14.5 million DDoS attacks year-to-date. That's an average of around 2,200 DDoS attacks every hour.

Of those attacks, Cloudflare mitigated over 200 hyper-volumetric network-layer DDoS attacks that exceeded 1 Tbps or 1 Bpps. The largest attacks peaked at 3.8 Tbps and 2.2 Bpps. Read more about these attacks and how our DDoS defense systems mitigated them autonomously.



Distribution of hyper-volumetric DDoS attacks over time

As we were writing this blog post, our systems continued to detect and mitigate these massive attacks and a new record has just been broken again, only three weeks after our last disclosure. On October 21, 2024, Cloudflare's systems autonomously detected and mitigated a 4.2 Tbps DDoS attack that lasted around a minute.



4.2 Tbps DDoS attack mitigated autonomously by Cloudflare

DDoS attack types and characteristics

Of the 6 million DDoS attacks, half were HTTP (application layer) DDoS attacks and half were network layer DDoS attacks. Network layer DDoS attacks increased by 51% QoQ and 45% YoY, and HTTP DDoS attacks increased by 61% QoQ and 68% YoY.

Attack duration

90% of DDoS attacks, including the largest of attacks, were very short-lived. We did see, however, a slight increase (7%) in attacks lasting more than an hour. These longer attacks accounted for 3% of all attacks.

Attack vectors

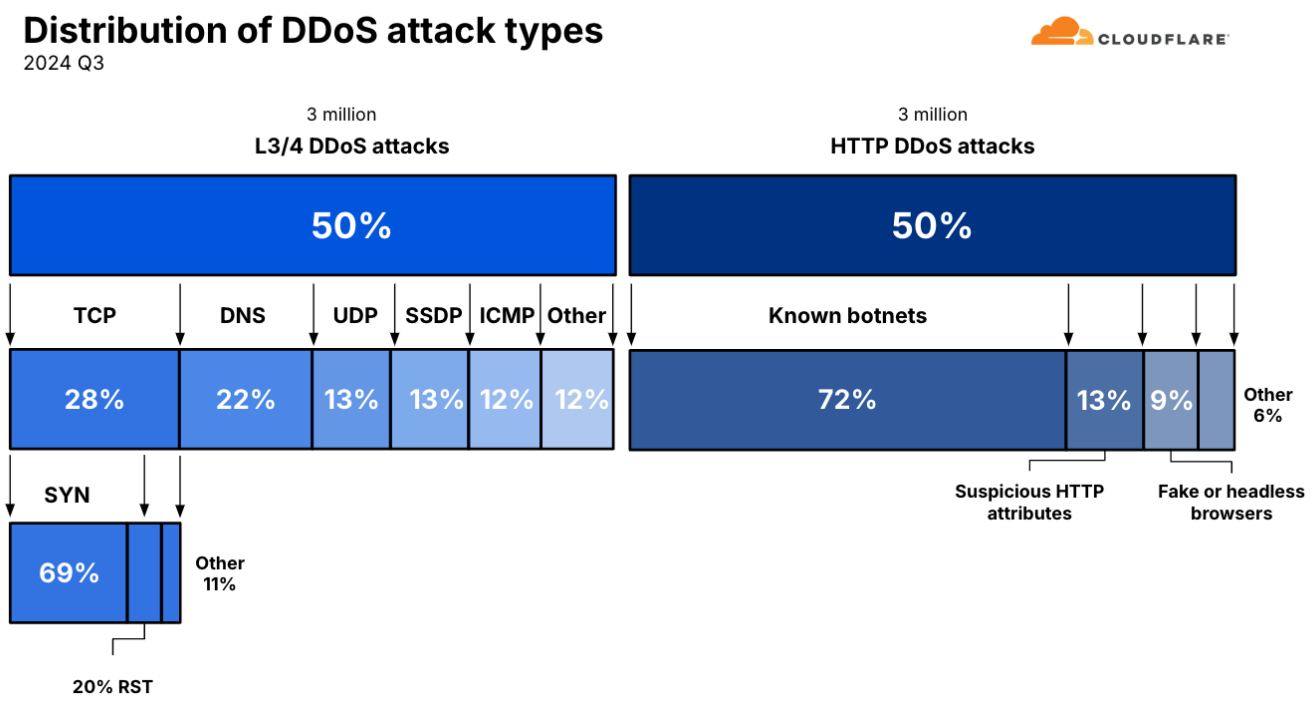
In Q3, we saw an even distribution in the number of network-layer DDoS attacks compared to HTTP DDoS attacks. Of the network-layer DDoS attacks, SYN flood was the top attack vector followed by DNS flood attacks, UDP floods, SSDP reflection attacks, and ICMP reflection attacks.

On the application layer, 72% of HTTP DDoS attacks were launched by known botnets and automatically mitigated by our proprietary heuristics. The fact

that 72% of DDoS attacks were mitigated by our home-grown heuristics showcases the advantages of operating a large network. The volume of traffic and attacks that we see let us craft, test, and deploy robust defenses against botnets.

Another 13% of HTTP DDoS attacks were mitigated due to their suspicious or unusual HTTP attributes, and another 9% were HTTP DDoS attacks launched by fake browsers or browser impersonators. The remaining 6% of "Other" includes attacks that targeted login endpoints and cache busting attacks.

One thing to note is that these attack vectors, or attack groups, are not necessarily exclusive. For example, known botnets also impersonate browsers and have suspicious HTTP attributes, but this breakdown is our attempt to categorize the HTTP DDoS attacks in a meaningful way.



Distribution of DDoS attacks in 2024 Q3

In Q3, we observed a 4,000% increase in SSDP amplification attacks compared to the previous quarter. An SSDP (Simple Service Discovery Protocol) attack is a type of reflection and amplification DDoS attack that exploits the UPnP (Universal Plug and Play) protocol. Attackers send SSDP requests to

vulnerable UPnP-enabled devices such as routers, printers, and IP-enabled cameras, and spoof the source IP address to be the victim's IP address. These devices respond to the victim's IP address with large amounts of traffic, overwhelming the victim's infrastructure. The amplification effect allows attackers to generate massive traffic from small requests, causing the victim's service to go offline. Disabling UPnP on unnecessary devices and using DDoS mitigation strategies can help defend against this attack.

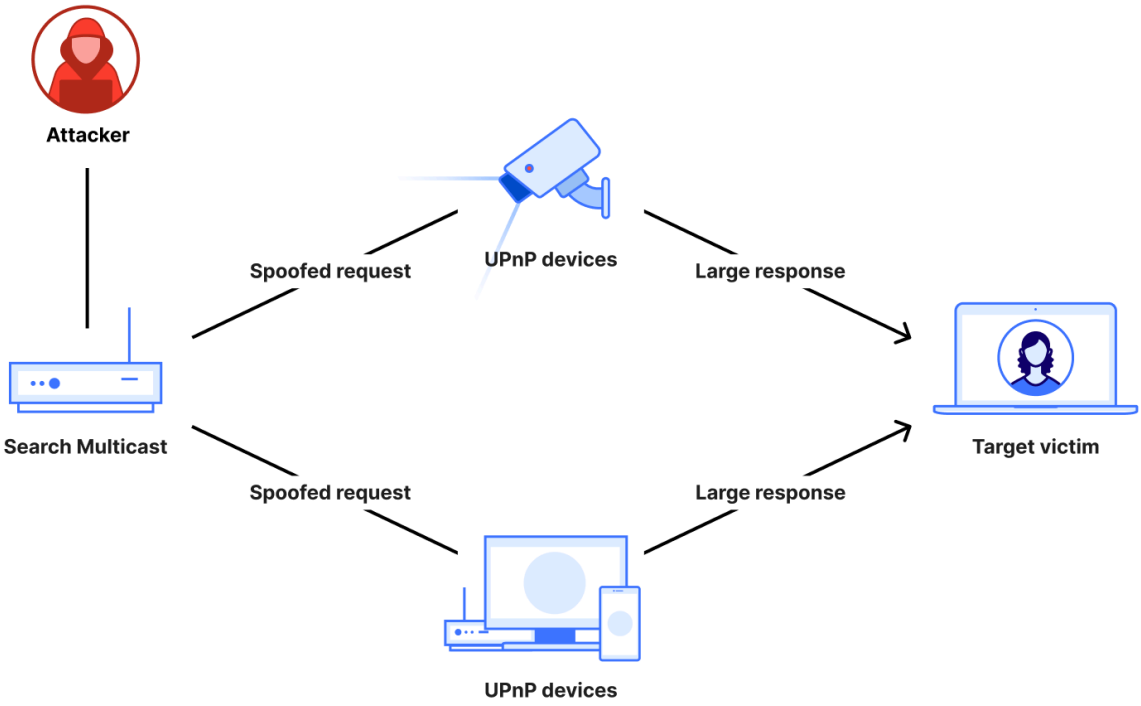


Illustration of an SSDP amplification attack

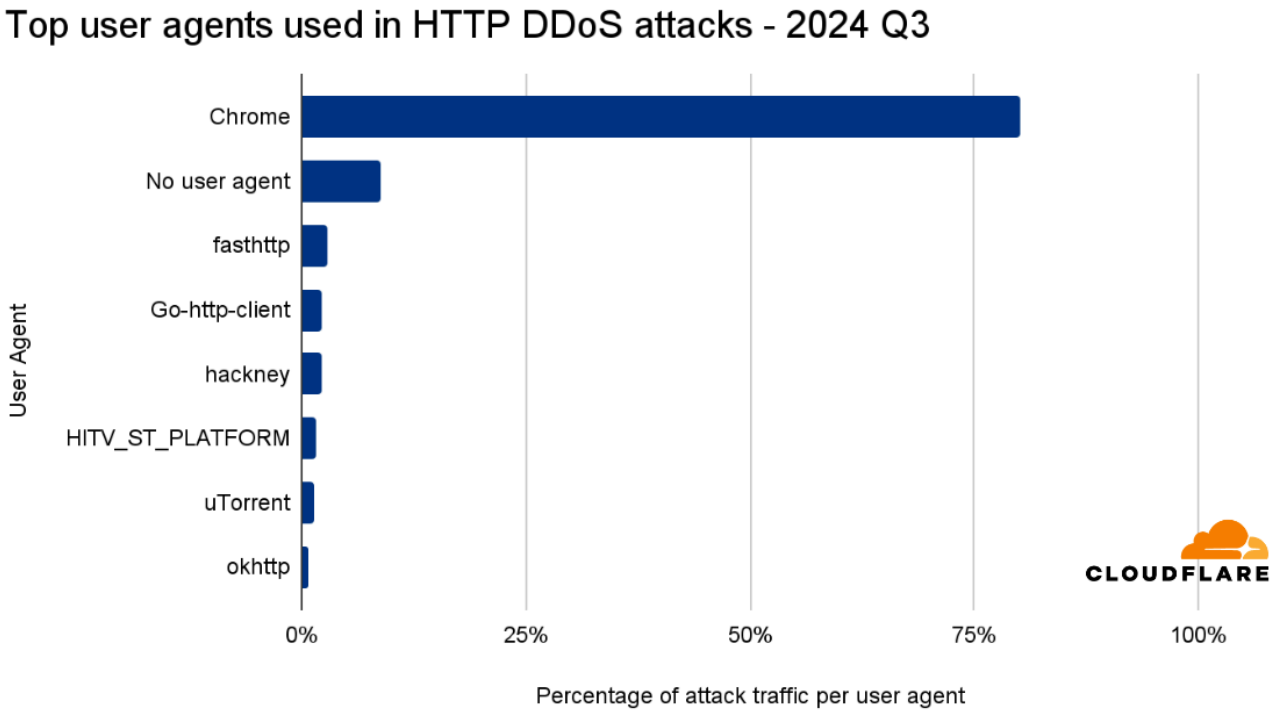
User agents used in HTTP DDoS attacks

When launching HTTP DDoS attacks, threat actors want to blend in to avoid detection. One tactic to achieve this is to spoof the user agent. This lets them appear as a legitimate browser or client if done successfully.

In Q3, 80% of HTTP DDoS attack traffic impersonated the *Google Chrome* browser, which was the most common user agent observed in attacks. More specifically, Chrome 118, 119, 120, and 121 were the most common versions.

In second place, no user agent was seen for 9% of HTTP DDoS attack traffic.

In third and fourth place, we observed attacks using the *Go-http-client* and *fasthttp* user agents. The former is the default HTTP client in Go's standard library and the latter is a high-performance alternative. *fasthttp* is used to build fast web applications, but is often used for DDoS attacks and web scraping too.



Top user agents used in DDoS attacks

The user agent *hackney* came in fifth place. It's an HTTP client library for Erlang. It's used for making HTTP requests and is popular in Erlang/Elixir ecosystems.

An interesting user agent shows up in the sixth place: *HITV_ST_PLATFORM*. This user agent appears to be associated with smart TVs or set-top boxes. Threat actors typically avoid using uncommon user agents, as evidenced by the frequent use of Chrome user agents in cyberattacks. Therefore, the presence of *HITV_ST_PLATFORM* likely suggests that the devices in question are indeed compromised smart TVs or set-top boxes.

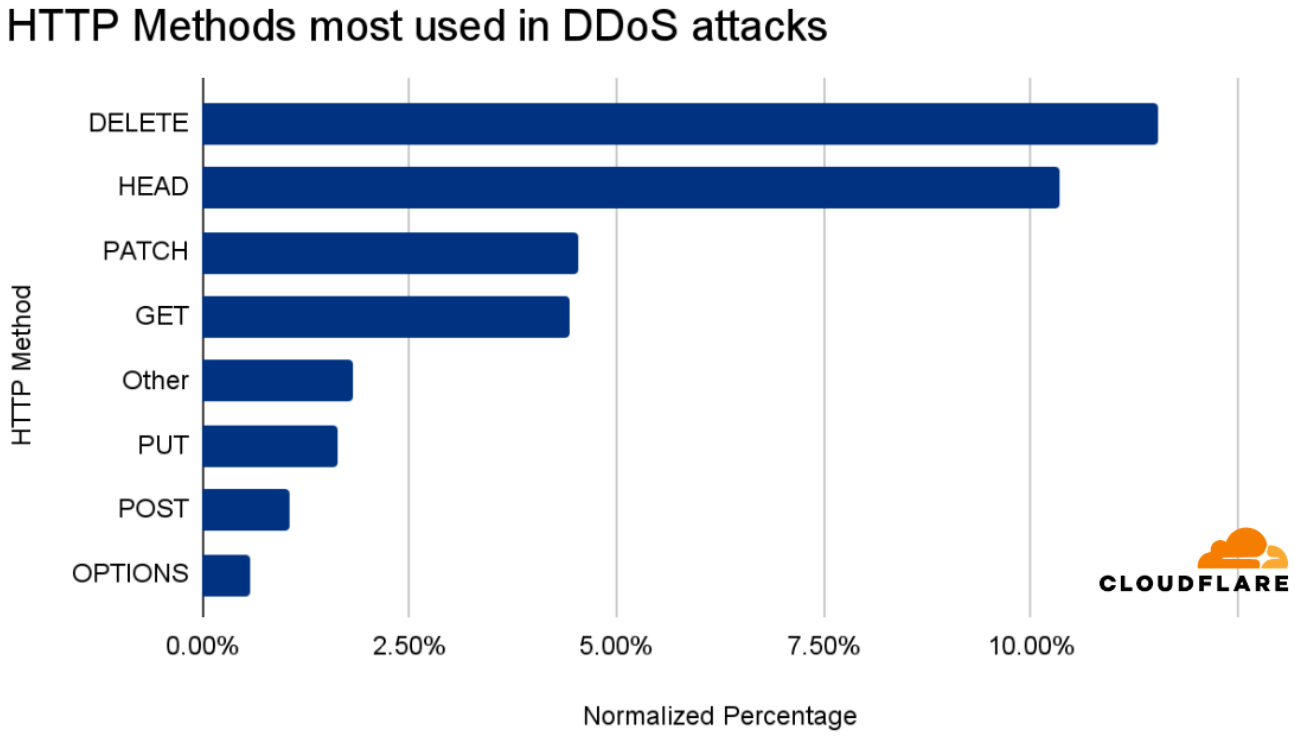
In seventh place, we saw the *uTorrent* user agent being used in attacks. This user agent is associated with a popular BitTorrent client that's used for downloading files.

Lastly, *okhttp* was the least common user agent in DDoS attacks despite its popularity as an HTTP client for Java and Android applications.

HTTP attack attributes

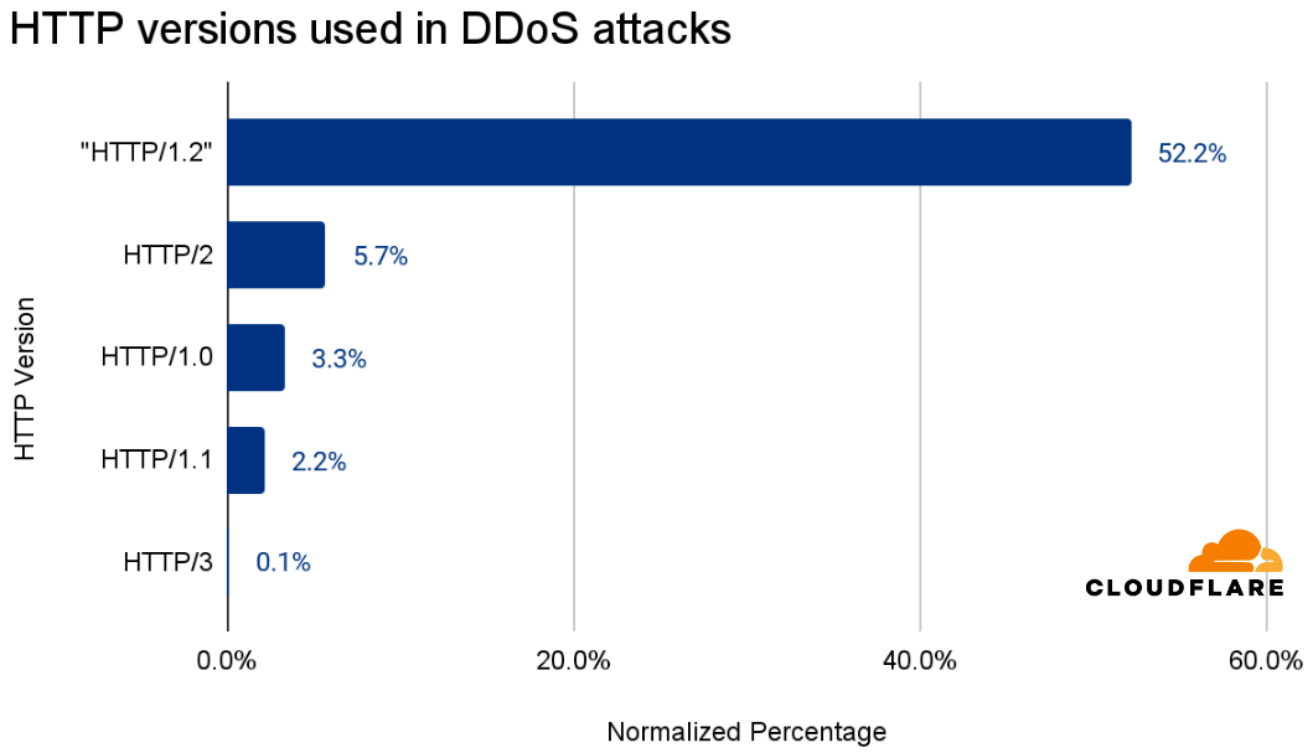
While 89% of HTTP DDoS attack traffic used the GET method, it is also the most commonly used HTTP method. So when we normalize the attack traffic by dividing the number of attack requests by total request per HTTP method, we get a different picture.

Almost 12% of all requests that used the DELETE method were part of an HTTP DDoS attack. After DELETE, we see that HEAD, PATCH and GET are the methods most commonly used in DDoS attack requests.

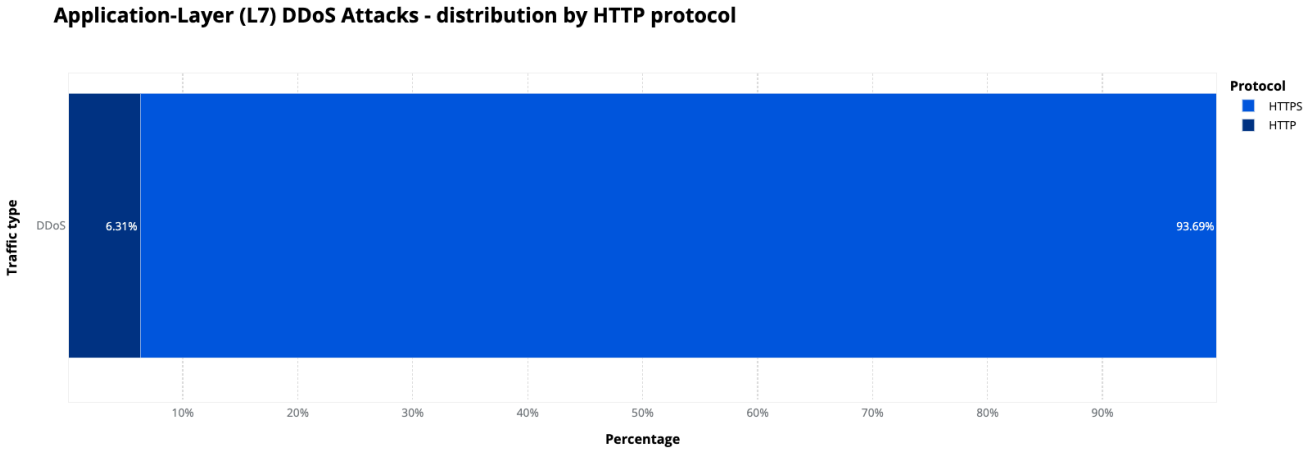


While 80% of DDoS attack requests were over HTTP/2 and 19% were over HTTP/1.1, they represented a much smaller portion when normalized by the total traffic by version. When we normalize the attack requests by all requests

by version, we see a different picture. Over half of traffic to the non-standard or mislabeled “HTTP/1.2” version was malicious and part of DDoS attacks. It's important to note that “HTTP/1.2” is not an official version of the protocol.



The vast majority of HTTP DDoS attacks are actually encrypted — almost 94% — using HTTPS.



Targets of DDoS attacks

Top attacked locations

China was the most attacked location in the third quarter of 2024. The United Arab Emirates was ranked second, with Hong Kong in third place, followed

closely by Singapore, Germany, and Brazil.

Canada was ranked seventh, followed by South Korea, the United States, and Taiwan as number ten.

Top attacked industries

In the third quarter of 2024, Banking & Financial Services was the most targeted by DDoS attacks. Information Technology & Services was ranked in second place, followed by the Telecommunications, Service Providers, and Carriers sector.

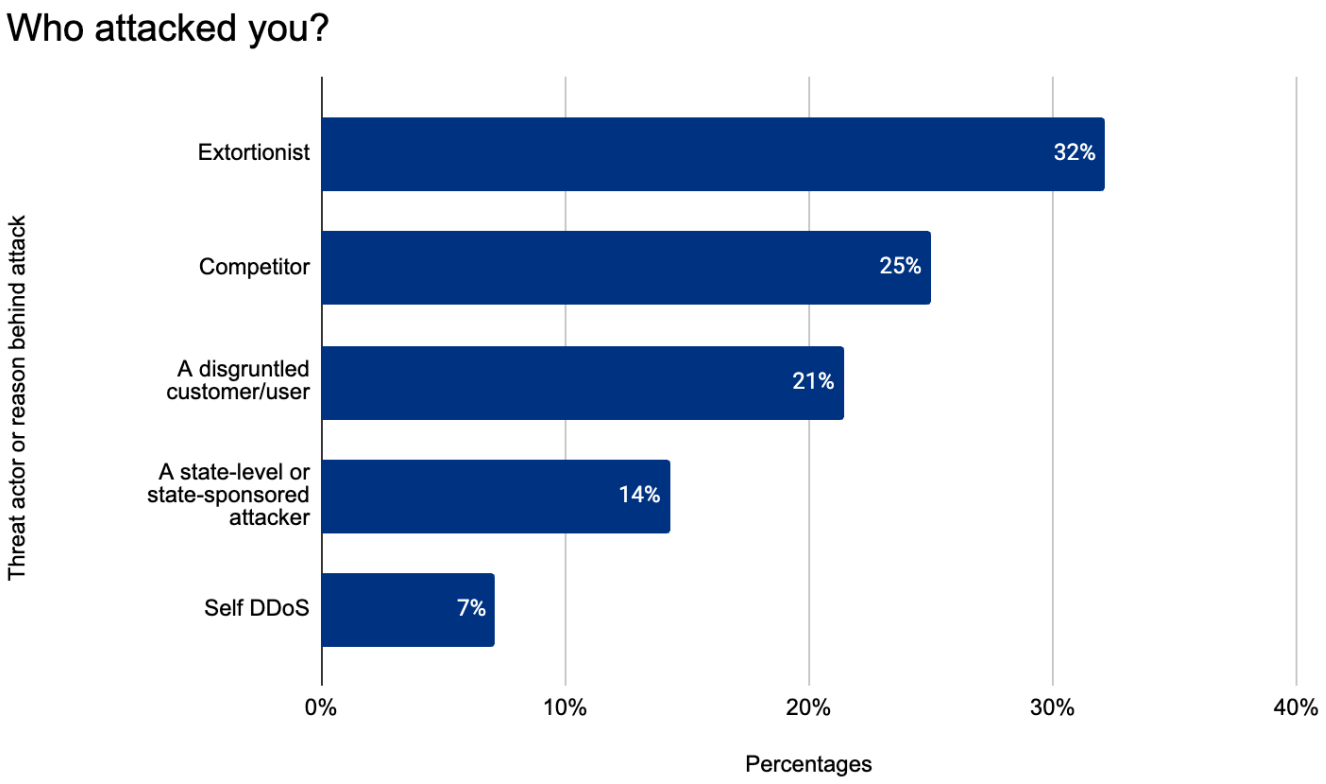
Cryptocurrency, Internet, Gambling & Casinos, and Gaming followed closely behind as the next most targeted industries. Consumer Electronics, Construction & Civil Engineering, and the Retail industries rounded out the top ten most attacked industries.

Sources of DDoS attacks

Threat actors

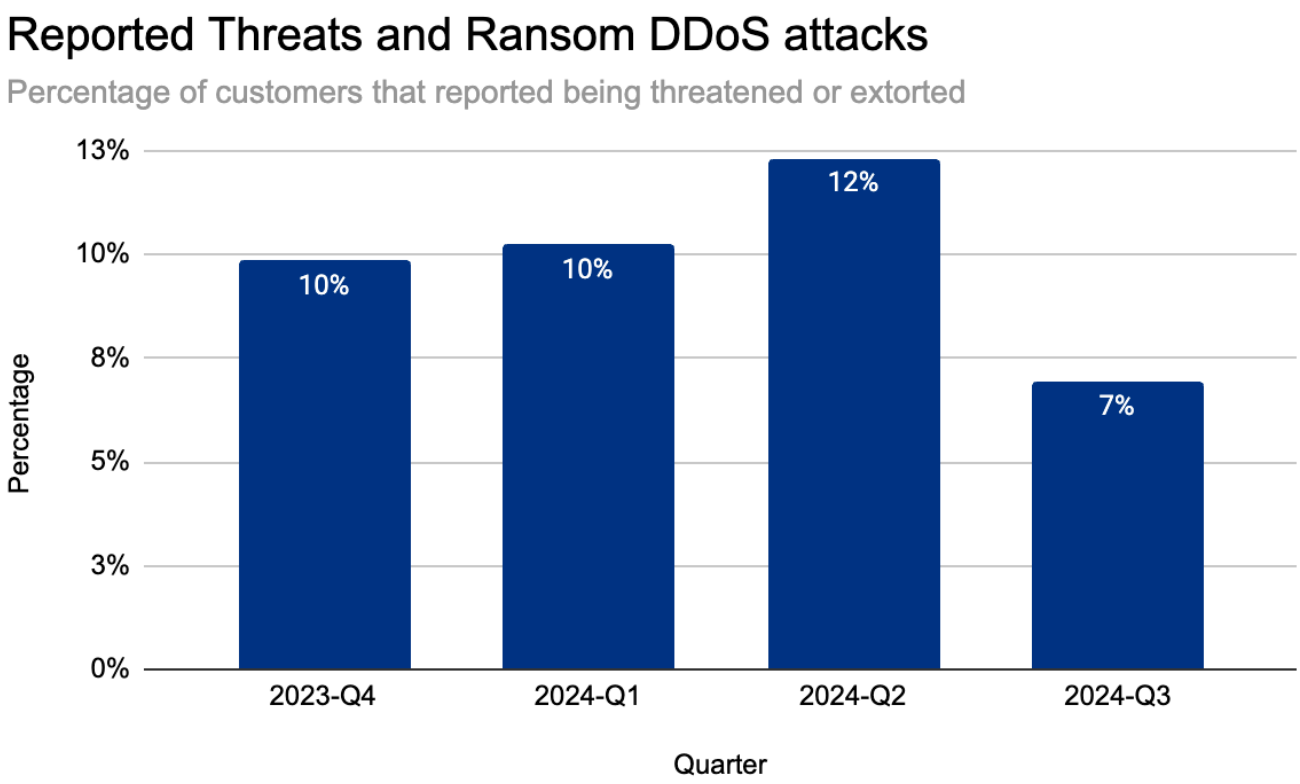
For a few years now, we've been surveying our customers that have been subjected to DDoS attacks. The survey covers various factors, such as the nature of the attack and the threat actors. In the case of threat actors, while 80% of survey respondents said that they don't know who attacked them, 20% said they did. Of those, 32% said that the threat actors were extortionists. Another 25% said a competitor attacked them, and another 21% said that a disgruntled customer or user was behind the attack. 14% of respondents said that the attacks were carried out by a state or a state-sponsored group. Lastly, 7% said that they mistakenly attacked themselves. One example of when a self-DDoS attack occurs is a post-firmware update for

IoT devices that causes all devices to *phone home* at the same time, resulting in a flood of traffic.



Distribution of the top threat actors

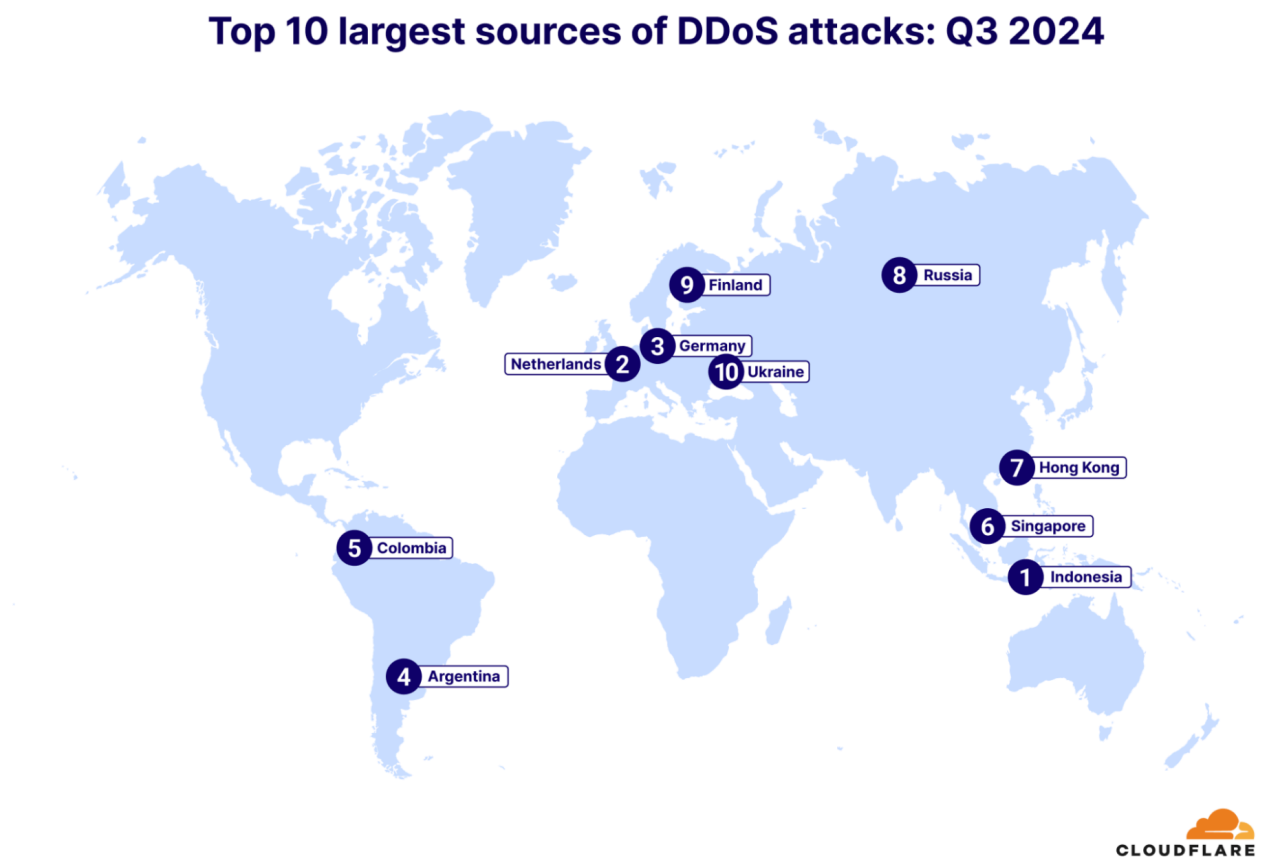
While extortionists were the most common threat actor, overall, reports of Ransom DDoS attacks decreased by 42% QoQ, but increased 17% YoY. A total of 7% of respondents reported being subjected to a Ransom DDoS attack or threatened by the attacker. In August, however, that figure increased to 10% — that's one out of ten.



Reports of Ransom DDoS attacks by quarter

Top source locations of DDoS attacks

Indonesia was the largest source of DDoS attacks in the third quarter of 2024. The Netherlands was the second-largest source, followed by Germany, Argentina, and Colombia.



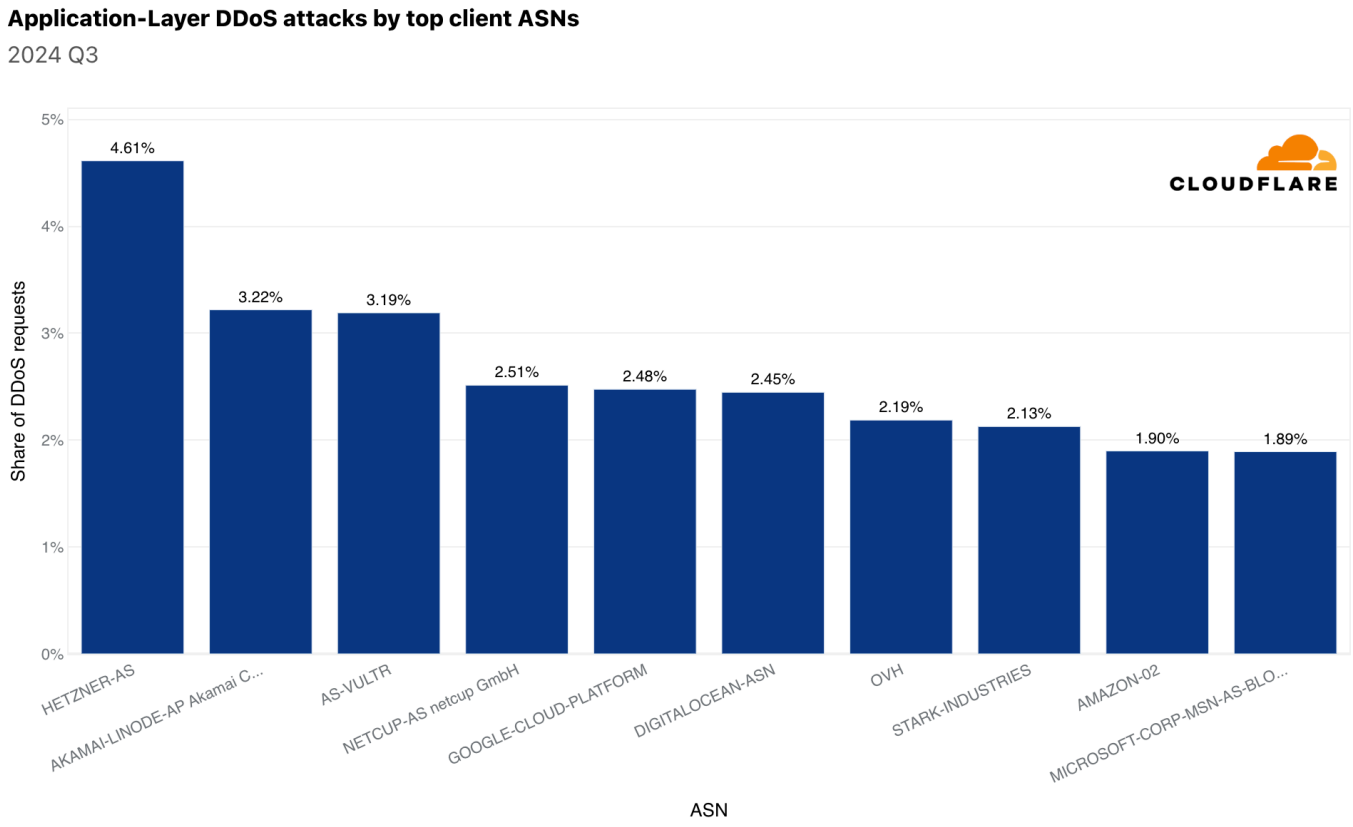
The next five largest sources included Singapore, Hong Kong, Russia, Finland, and Ukraine.

Top source networks of DDoS attacks

For service providers that operate their own networks and infrastructure, it can be difficult to identify who is using their infrastructure for malicious intent, such as generating DDoS attacks. For this reason, we provide a free threat intelligence feed to network operators. This feed provides service providers information on IP addresses from within their networks that we've seen participate in subsequent DDoS attacks.

On that note, Hetzner (AS24940), a German-based IT provider, was the largest source of HTTP DDoS attacks in the third quarter of 2024. Linode (AS63949), a cloud computing platform acquired by Akamai in 2022, was the second-largest source of HTTP DDoS attacks. Vultr (AS64515), a Florida-based service provider, came in third place.

Netcup (AS197540), another German-based IT provider, came in fourth place. Google Cloud Platform (AS15169) followed in fifth place. DigitalOcean (AS14061) came in sixth place, followed by French provider OVH (AS16276), Stark Industries (AS44477), Amazon Web Services (AS16509), and Microsoft (AS8075).



Networks that were that largest sources of HTTP DDoS attacks in 2024 Q3

Key takeaways

This quarter, we observed an unprecedented surge in hyper-volumetric DDoS attacks, with peaks reaching 3.8 Tbps and 2.2 Bpps. This mirrors a similar trend from the same period last year, when application layer attacks in the HTTP/2 Rapid Reset campaign exceeded 200 million requests per second (Mrps). These massive attacks are capable of overwhelming Internet properties, particularly those relying on capacity-limited cloud services or on-premise solutions.

The increasing use of powerful botnets, fueled by geopolitical tensions and global events, is expanding the range of organizations at risk — many of

which were not traditionally considered prime targets for DDoS attacks. Unfortunately, too many organizations reactively deploy DDoS protections after an attack has already caused significant damage.

Our observations confirm that businesses with well-prepared, comprehensive security strategies are far more resilient against these cyberthreats. At Cloudflare, we're committed to safeguarding your Internet presence. Through significant investment in our automated defenses and a robust portfolio of security products, we ensure proactive protection against both current and emerging threats — so you don't have to.

Cloudflare's connectivity cloud protects entire corporate networks, helps customers build Internet-scale applications efficiently, accelerates any website or Internet application, wards off DDoS attacks, keeps hackers at bay, and can help you on your journey to Zero Trust.

Visit 1.1.1.1 from any device to get started with our free app that makes your Internet faster and safer.

To learn more about our mission to help build a better Internet, start here. If you're looking for a new career direction, check out our open positions.

Discuss on Hacker News

ON AIR | CLOUDFLARE TV

Derechos Digitales en Latinoamérica [S2E1] - Cultivando Género AC en Cloudflare TV

Tune In

DDoS Reports DDoS Advanced DDoS Cloudflare Radar Attacks