CLOUDFLARE

The State of DDoS Threats:

Q3 2023

Content

Executive Summary

Welcome to the third DDoS threat report of 2023. DDoS attacks, or distributed denial-of-service attacks, are a type of cyber attack that aims to disrupt websites (and other types of Internet properties) to make them unavailable for legitimate users by overwhelming them with excessive traffic. Think of it as causing a traffic jam on a critical road, preventing people from reaching their destination.

Our network is one of the largest in the world, spanning more than 300 cities in over 100 countries. We handle a massive amount of internet traffic, serving over 64 million web requests per second at its peak and processing 2.3 billion DNS queries daily. On average, we thwart 140 billion cyber threats each day. This vast data volume provides us with a unique perspective on the DDoS threat landscape, enabling us to share valuable insights and trends with the cybersecurity community.

In recent weeks, we've observed a surge in DDoS and other cyber attacks, coinciding with the conflict in Israel and Palestine. To support humanitarian efforts during these challenging times, we are offering our services free of charge. Our thoughts are with those striving for peace in the Middle East.

Cloudflare has successfully mitigated thousands of high-volume HTTP DDoS attacks. Notably, 89 of these attacks surpassed 100 million requests per second (rps), with the largest peaking at 201 million rps—a threefold increase compared to the previous record of 71 million rps. This campaign contributed to a 65% overall increase in HTTP DDoS attack traffic during Q3, compared to the previous quarter.

Similarly, Layer 3 and Layer 4 DDoS attacks increased by 14%, with numerous attacks in the terabit-per-second levels. The largest attack targeted Cloudflare's free DNS resolver, 1.1.1.1, and reached a peak of 2.6 terabits per second (Tbps).

Notably, gaming and gambling companies experienced the highest volume of HTTP DDoS attack traffic, surpassing the cryptocurrency industry from the previous quarter.

An interactive version of this report is also available on Cloudflare Radar.

Report Highlights

Campaign of hyper-volumetric DDoS attacks exploiting HTTP/2 Rapid Resets

Beginning in late August 2023, Cloudflare, along with several other vendors, became the target of a sophisticated and persistent DDoS attack campaign. This campaign exploited the HTTP/2 Rapid Reset vulnerability (CVE-2023-44487).

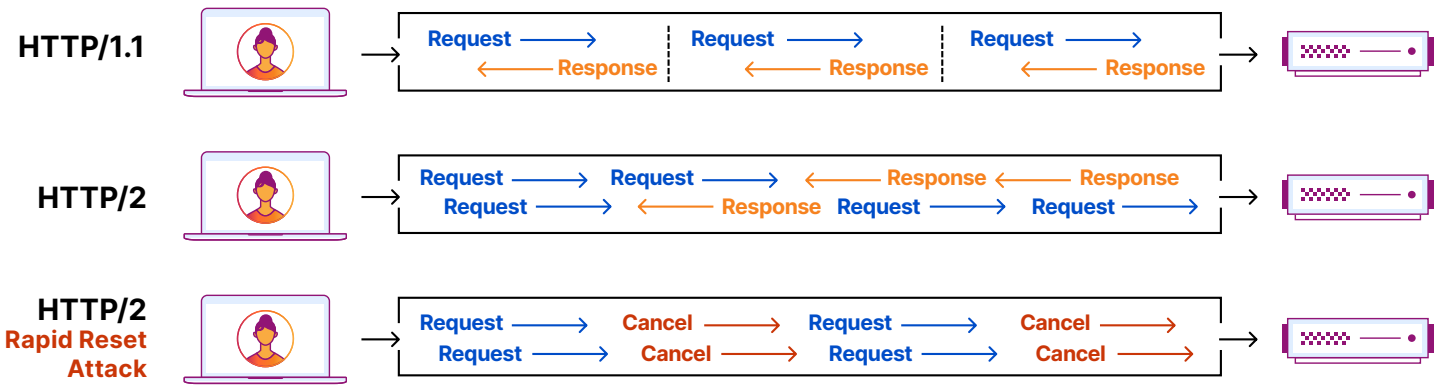
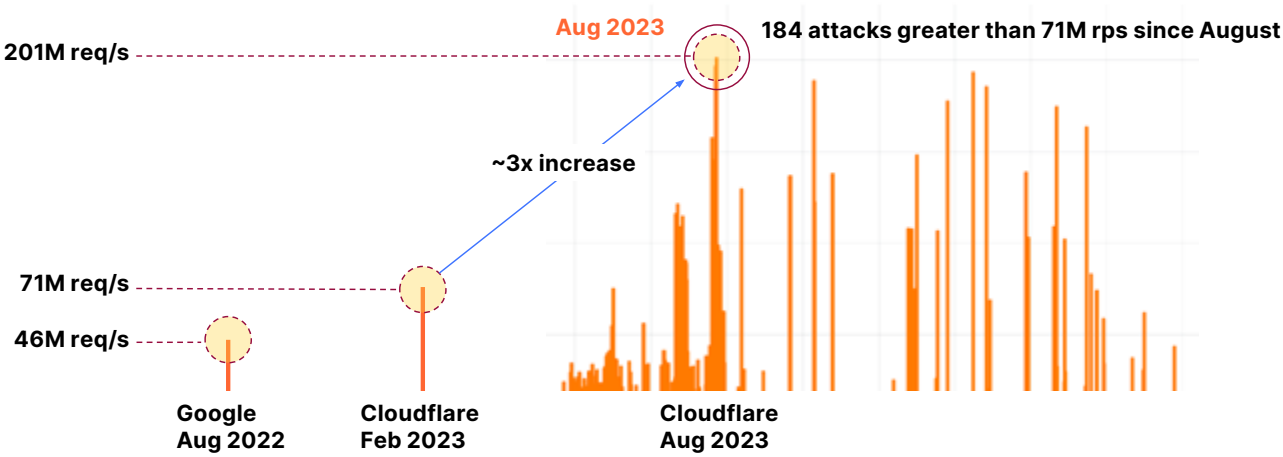


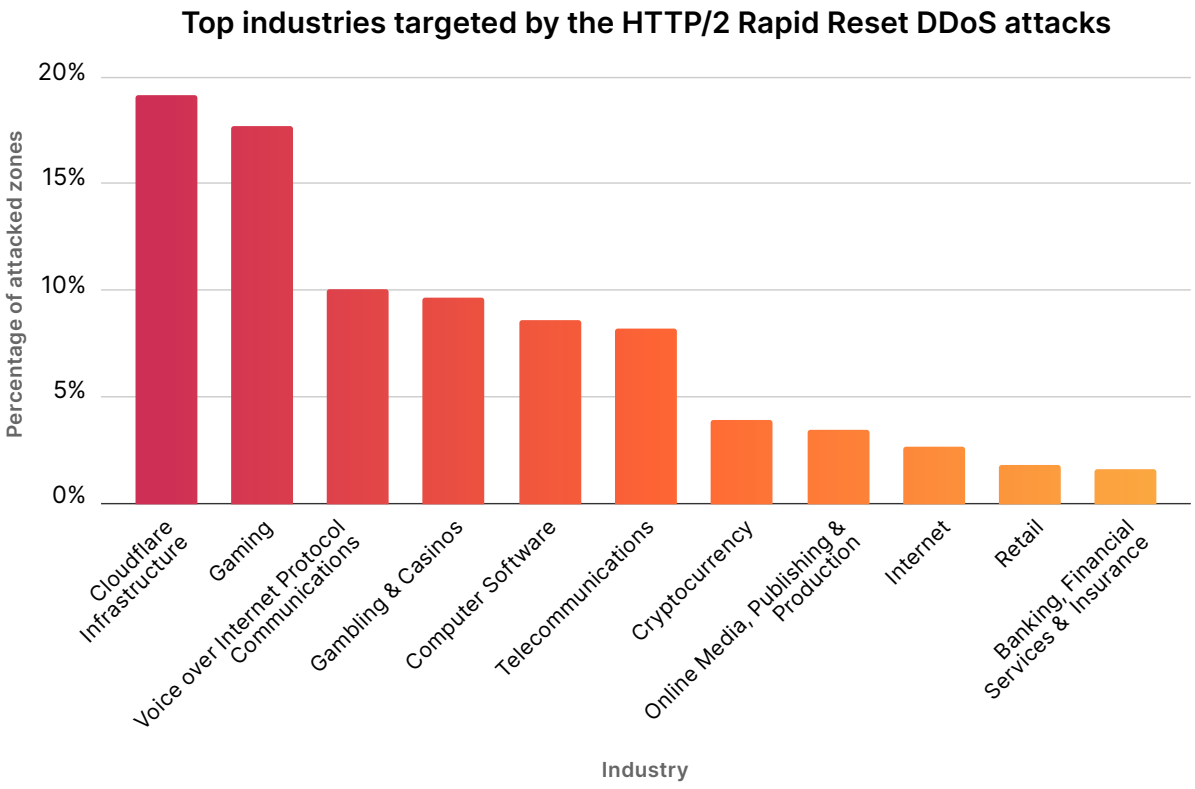
Illustration of a HTTP/2 Rapid Reset DDoS attack

The DDoS campaign included thousands of hyper-volumetric DDoS attacks over HTTP/2 that peaked in the range of millions of requests per second. The average attack rate was 30 million rps. Approximately 89 of the attacks peaked above 100 million rps and the largest one we saw hit 201 million rps.

HTTP/2 Rapid Reset campaign of hyper-volumetric DDoS attacks



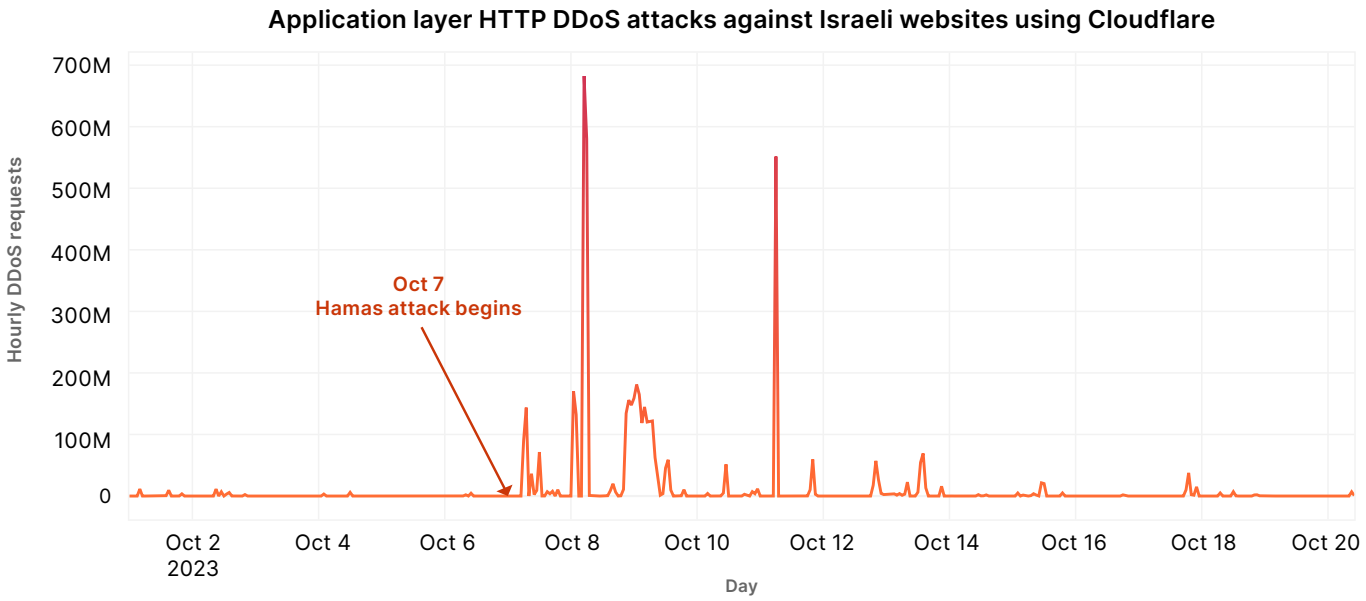
The primary focus of the two-month-long DDoS campaign was on cloud infrastructure vendors such as Cloudflare. Specifically, 19% of all attacks targeted Cloudflare websites and infrastructure. Another 18% targeted Gaming companies, and 10% targeted well known VoIP providers.



Cyber attacks in the Israel-Hamas war

Various pro-Palestinian hacktivist groups have targeted Israeli websites and mobile apps. On October 14, we revealed the findings of an investigation conducted by the Cloudforce One Threat Operations team. We identified malicious Android mobile applications impersonating the legitimate RedAlert - Rocket Alerts application. These malicious apps were successful in gaining unauthorized access to sensitive user information, including the mobile phone's contact list, SMS messages, phone call logs, installed applications, and even details about the phone and SIM card itself. For more technical details regarding our investigation, you can find them here.

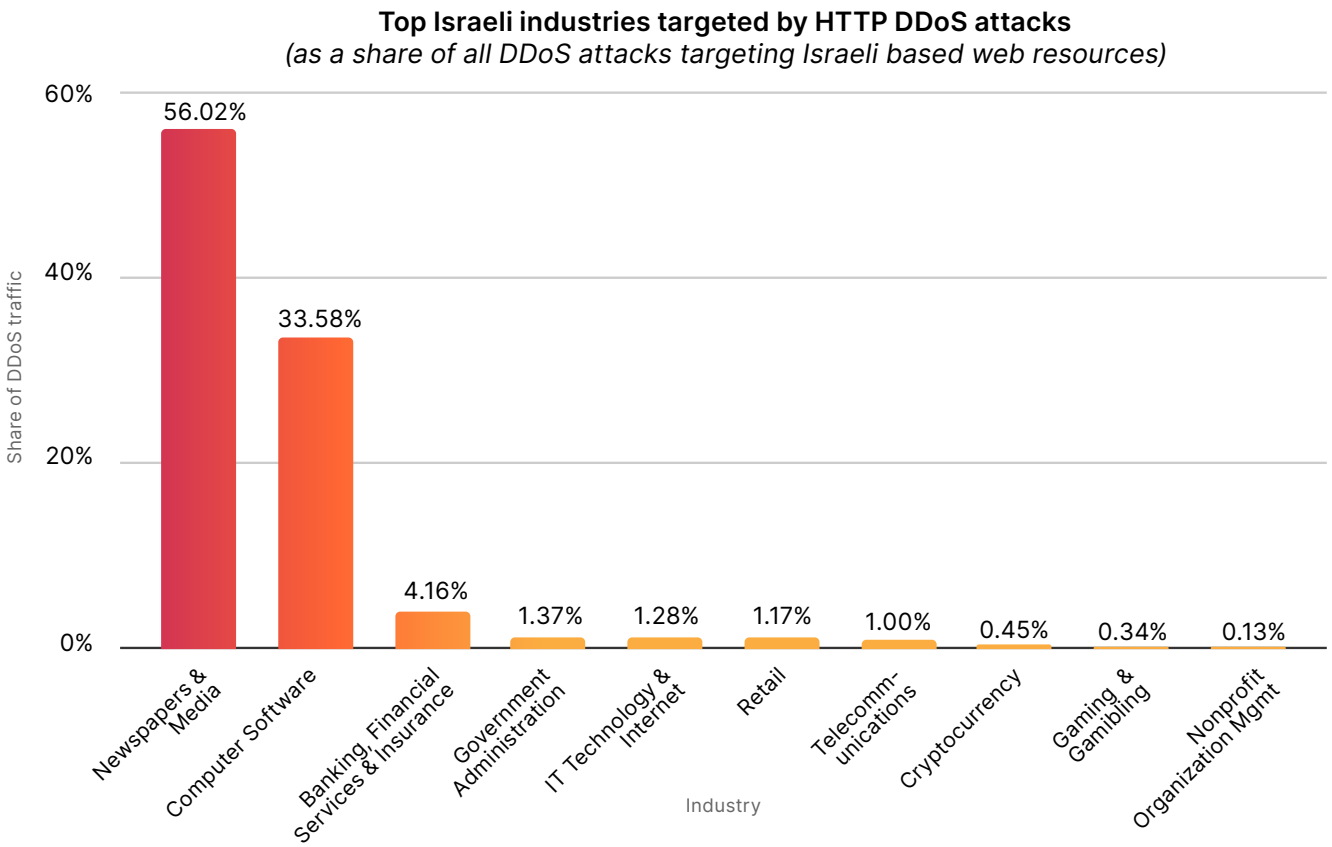
Following the October 7 attack by Hamas, Israeli websites came under a sustained barrage of DDoS attacks in the ensuing days. Cloudflare has helped to onboard and protect many of these targeted websites.



Before October 7, we saw minimal HTTP DDoS attack requests towards Israeli websites using Cloudflare. However, the situation took a sharp turn on October 7 when the percentage of DDoS attack traffic surged. On that day, nearly 1 out of every 100 requests directed at Israeli websites using Cloudflare were identified as part of an HTTP DDoS attack. This alarming figure quadrupled on October 8.

Since the October 7 attack, Newspaper and Media websites have been the main target of DDoS attacks — accounting for 56% of all attacks against Israeli websites. Similar trends were observed during the Russia-Ukraine conflict, where Ukrainian media and broadcasting websites were extensively targeted. In recent years, conflicts on the ground are often accompanied by cyber attacks on websites that provide crucial information for civilians.

The second most targeted industry in Israel was the Computer Software industry. Almost 34% of all DDoS attacks targeted computer software companies. In third place, and more significantly, Banking, Financial Services and Insurance (BFSI) companies were attacked. Government Administration websites came in fourth place.

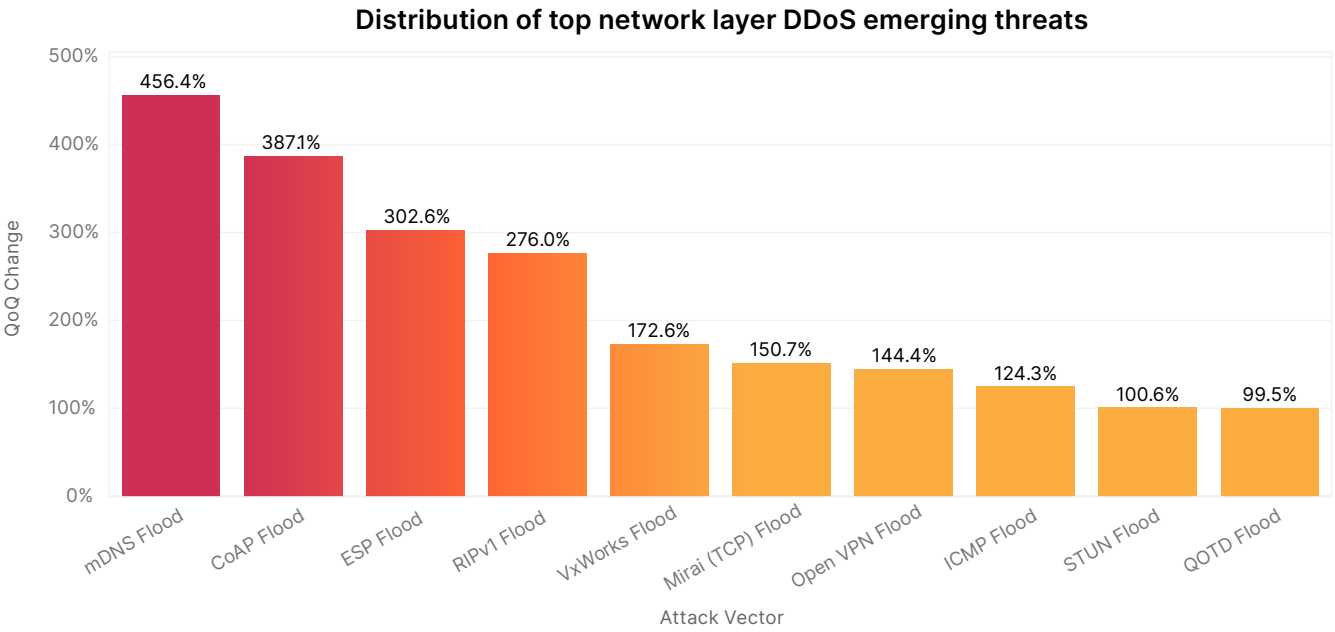


Cyber attacks against Palestinian websites

During the same time frame, from October 1, Cloudflare automatically detected and mitigated over 454 million HTTP DDoS attack requests that targeted Palestinian websites using Cloudflare. While that figure is barely a tenth of the amount of attack requests we saw against Israeli websites using Cloudflare, it represented a larger portion of the overall traffic towards Palestinian websites using Cloudflare.

Before the Hamas attack, we didn't see any DDoS attacks against Palestinian websites using Cloudflare. That changed on October 7; over 46% of all traffic to Palestinian websites using Cloudflare were part of HTTP DDoS attacks. On October 9, that figure increased to almost 60%. Nearly 6 out of every 10 HTTP requests towards Palestinian websites using Cloudflare were part of DDoS attacks.

Emerging attack vectors at the network layer



mDNS DDoS attacks increased by 456%

Multicast DNS (mDNS) is a UDP-based protocol that is used in local networks for service/device discovery. Vulnerable mDNS servers respond to unicast queries originating outside the local network, which are 'spoofed' (altered) with the victim's source address. This results in amplification attacks. In Q3, we noticed a large increase of mDNS attacks; a 456% increase compared to the previous quarter.

CoAP DDoS attacks increased by 387%

The Constrained Application Protocol (CoAP) is designed for use in simple electronics and enables communication between devices in a low-power and lightweight manner. However, it can be abused for DDoS attacks via IP spoofing or amplification, as malicious actors exploit its multicast support or leverage poorly configured CoAP devices to generate large amounts of unwanted network traffic. This can lead to service disruption or overloading of the targeted systems, making them unavailable to legitimate users.

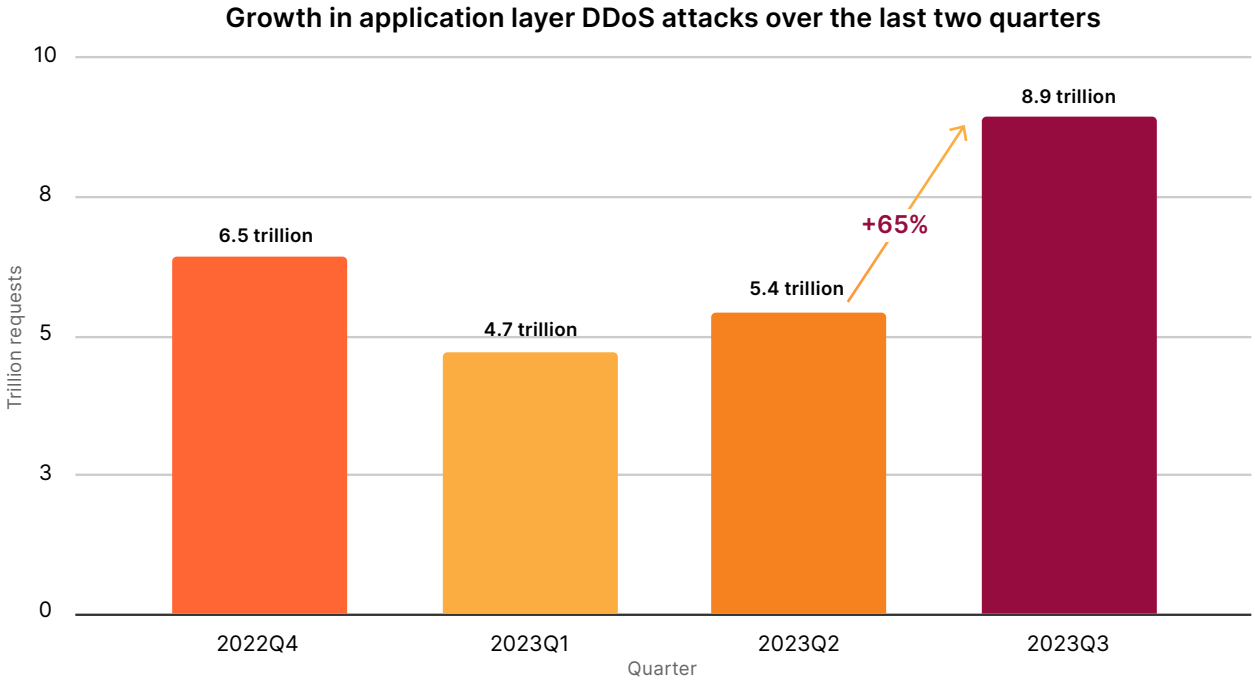
ESP DDoS attacks increased by 303%

The Encapsulating Security Payload (ESP) protocol is part of IPsec and provides confidentiality, authentication, and integrity to network communications. However, it could potentially be abused in DDoS attacks if malicious actors exploit misconfigured or vulnerable systems to reflect or amplify traffic towards a target, leading to service disruption. Like with other protocols, securing and properly configuring the systems using ESP is crucial to mitigate the risks of DDoS attacks.

Quarterly DDoS Trends — Q3 2023

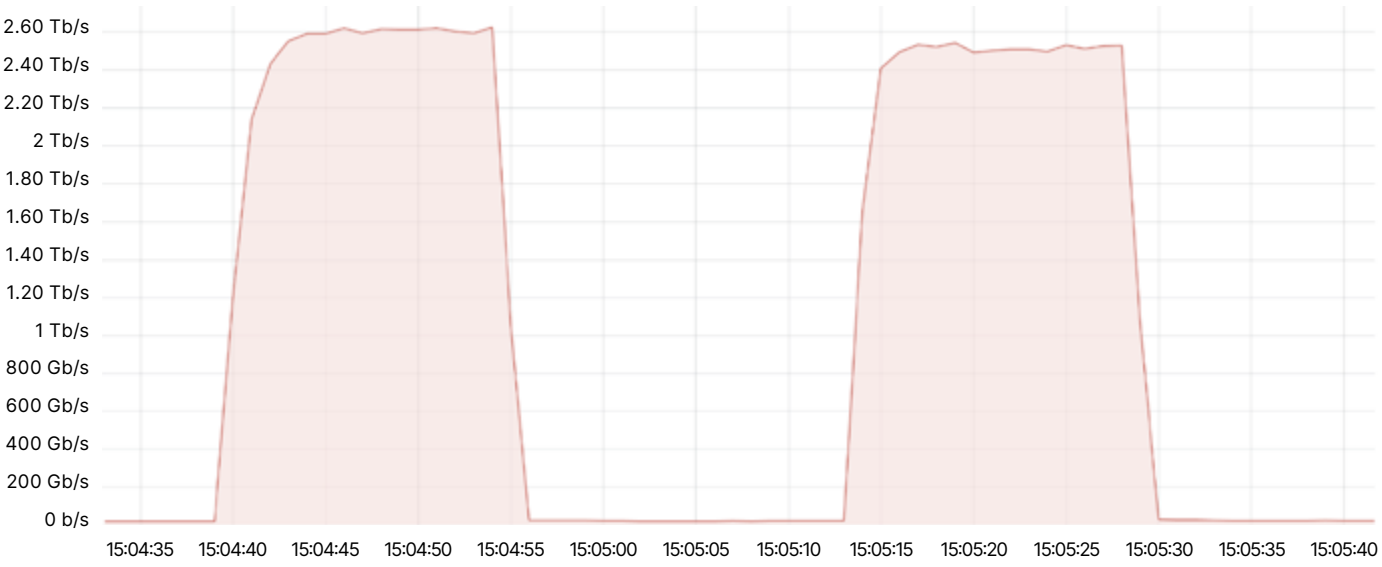
Overall traffic volume changes

Last quarter, the volume of HTTP DDoS attacks increased by 15% QoQ. This quarter, it grew even more. Attack volume increased by 65% QoQ to a total staggering figure of 8.9 trillion HTTP DDoS requests that Cloudflare systems automatically detected and mitigated.



We saw a minor increase of 14% in Layer 3 and Layer 4 DDoS attacks — similar to the figures we saw in the first quarter of this year. In Q3, our DDoS defenses automatically detected and mitigated numerous DDoS attacks in the terabit-per-second range. The largest attacks we saw peaked at 2.6 Tbps. This attack was part of a broader campaign that targeted Cloudflare's free DNS resolver 1.1.1.1. It was a UDP flood that was launched by a Mirai-variant botnet.

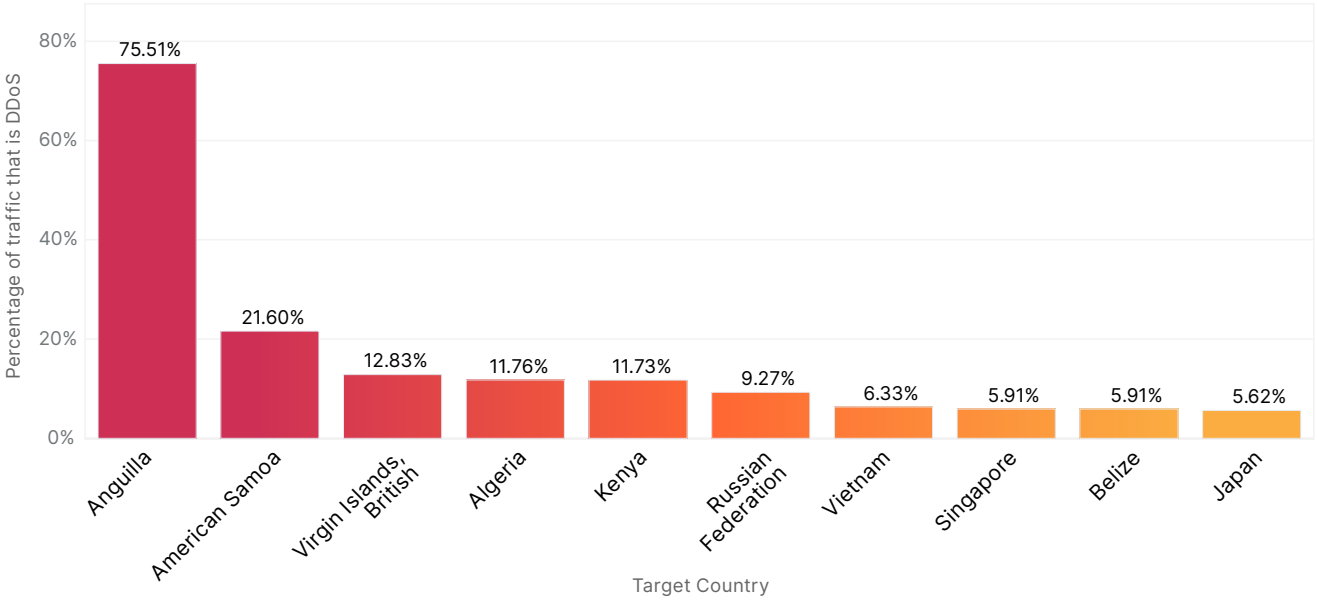
Mirai botnet based UDP flood attacks peaking at 2.6 Tbps



Top targeted countries

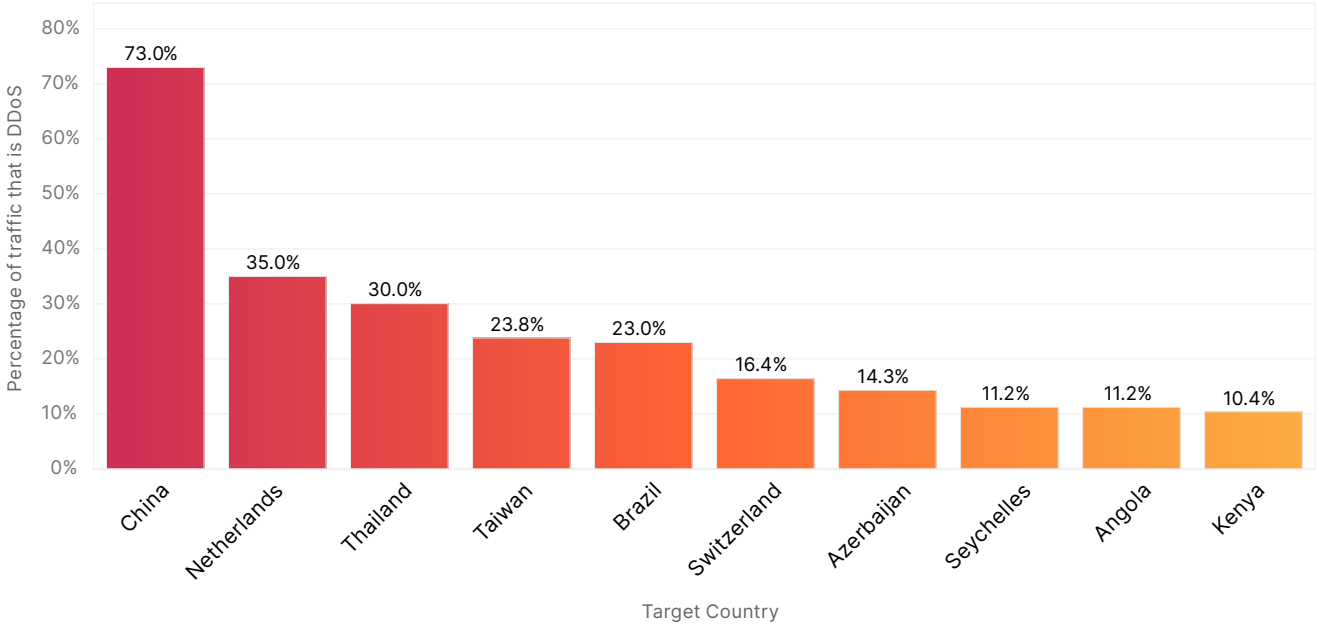
The top three most attacked countries as a share of their overall HTTP traffic are small population, island nations. Anguilla, a small set of islands east of Puerto Rico, jumps to the first place as the most attacked country. Over 75% of all traffic to Anguilla websites were HTTP DDoS attacks. In second place, American Samoa, a group of islands east of Fiji. In third, the British Virgin Islands. In fourth place, Algeria, and then Kenya, Russia, Vietnam, Singapore, Belize, and Japan.

Application layer DDoS traffic as a share of HTTP traffic for the top attacked countries



At the network layer, the country and region based comparison is very stark. Similar to Q2 2023 (April to June), China remains in first place this quarter (July to September) as the most attacked as a percentage of their overall network traffic. Cloudflare saw that 73% of traffic to China Internet networks was attack traffic. Netherlands received the second-highest proportion of attack traffic (representing 35% of the country's overall traffic), closely followed by Thailand, Taiwan and Brazil.

Network layer DDoS traffic as a share of network traffic for the top attacked countries



Industry and regional variations in DDoS attacks

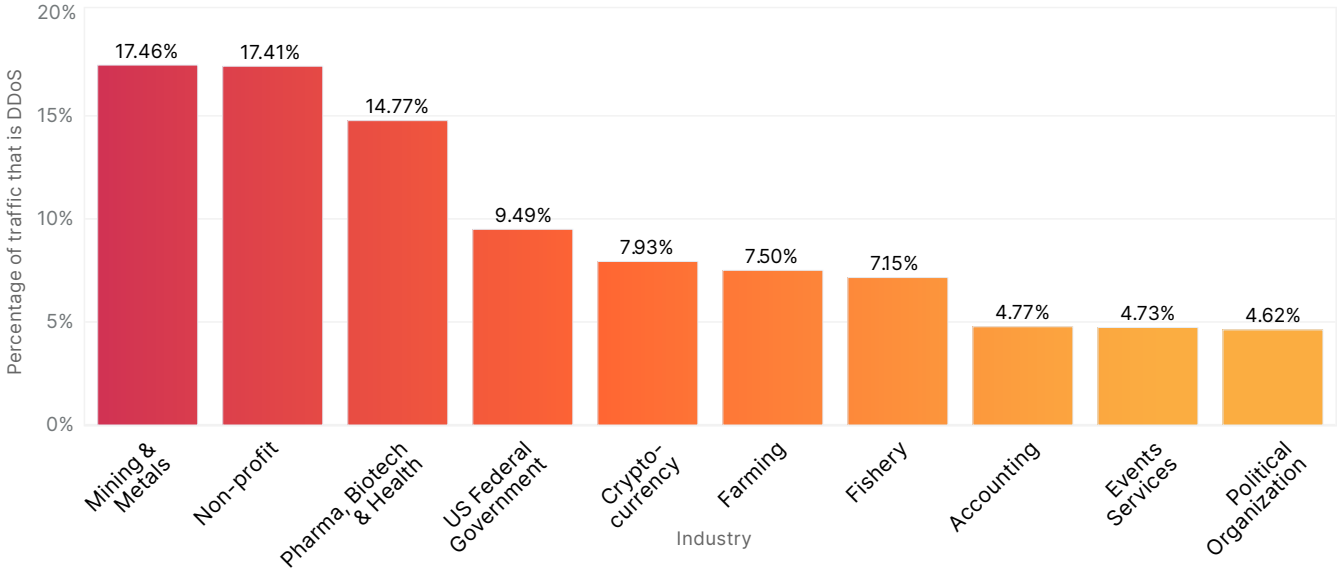
The Gaming and Gambling industry has long been one of the most attacked industries compared to others. But when we look at the HTTP DDoS attack traffic relative to each specific industry, we see a different picture. The Gaming and Gambling industry has so much user traffic that, despite being the most attacked industry by volume, it doesn't even make it into the top ten when we put it into the per-industry context.

Instead, what we see is that the Mining and Metals industry was targeted by the most attacks compared to its total traffic — 17.46% of all traffic to Mining and Metals companies were DDoS attack traffic.

Following closely in second place, 17.41% of all traffic to Non-profits were HTTP DDoS attacks. Many of these attacks are directed at more than 2,400 Non-profit and independent media organizations in 111 countries that Cloudflare protects for free as part of Project Galileo, which celebrated its ninth anniversary this year. Over the past quarter alone, Cloudflare mitigated an average of 180.5 million cyber threats against Galileo-protected websites every day.

Pharmaceuticals, Biotechnology and Health companies came in third, and US Federal Government websites in fourth place. Almost one out of every 10 HTTP requests to US Federal Government Internet properties were part of an attack. In fifth place, Cryptocurrency and then Farming and Fishery not far behind.

HTTP DDoS attacks: Top attacked industries compared to their own traffic



Recommendations and takeaways

Best practices	Optimize your Cloudflare usage
Update or make a Denial of Service Response Plan.	Have you integrated Cloudflare alerts and threat intelligence into your security operations? Do you know how to reach all the necessary collaborators in case of an attack? Are they trained on the response plan?
Deploy threat intelligence and in-line, automated DDoS mitigation solutions.	Use multiple detection techniques to deal with the attack trends listed in this report: 1. Dynamic stateless fingerprinting 2. Machine learning-based classification 3. Anomalous traffic detection 4. Traffic profiling and stateful mitigation 5. Threat intelligence on current DDoS activity and trends
Update your infrastructure to be more resilient for your traffic profile. **Improve network and application performance to avoid bottlenecks.**	Ensure capacity in your DDoS mitigation tooling is large enough to handle twice the largest attacks on record and twice the max rates of your legitimate traffic. Auto-reduce HTTP/2 multiplexing ceiling when under attack, enabling WAF Leverage a digital waiting room Optimize caching, manage loads better with a Content Delivery Network (CDN) and cloud based loading balancing solutions.
Use a positive security model: Ensure traffic that you want, gets in reliably.	Keep ports important to your business and in use open Using schema validation and an API Gateway for API traffic
Leverage threat intelligence and artificial intelligence to stay ahead of emerging threats.	Bot scores that can be used within firewall and rate-limiting rules

At Cloudflare, we want to make it even easier — and free — for organizations of all sizes to protect themselves against even the largest and most complex DDoS attacks. We have been providing free unmetered and unlimited DDoS protection to all of our customers since 2017 — when we pioneered the concept.

Watch the DDoS trends webinar to learn more about these emerging DDoS threats and how to defend against them.

1 888 99 FLARE | enterprise@cloudflare.com | Cloudflare.com

REV:BDES-5348.2023NOV20