CLOUDFLARE

Cloudflare DDoS Threat Report

Q2 2023

Content

Executive Summary

Welcome to Cloudflare's quarterly distributed denial-of-service (DDoS) report for the months April to June 2023. This report uncovers insights and trends about the DDoS threat landscape observed across Cloudflare's global network this second quarter of 2023.

The second quarter of 2023 was characterized by thought-out, tailored and persistent waves of DDoS attack campaigns on various fronts.

At the HTTP layer, we detected pro-Russian hacktivist groups REvil, Killnet and Anonymous Sudan being very active against Western internet websites and an uptick in low volume, highly randomized DDoS attacks. Over the past quarter, DNS-based DDoS attacks have become the most common DDoS attack vector — with 32% of all DDoS attacks targeting the DNS protocol. At the UDP layer, we observed attacks leveraging a zero-day vulnerability (CVE-2022-26143, TP240PhoneHome) we disclosed in March 2022.

Beyond specific attack campaigns, we break down application and network-layer attack trends alongside the industry and regional variations. Finally, we provide guidance on how to proactively harden your security in order to ensure service continuity through an ever-evolving DDoS threat landscape.

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

Report Highlights

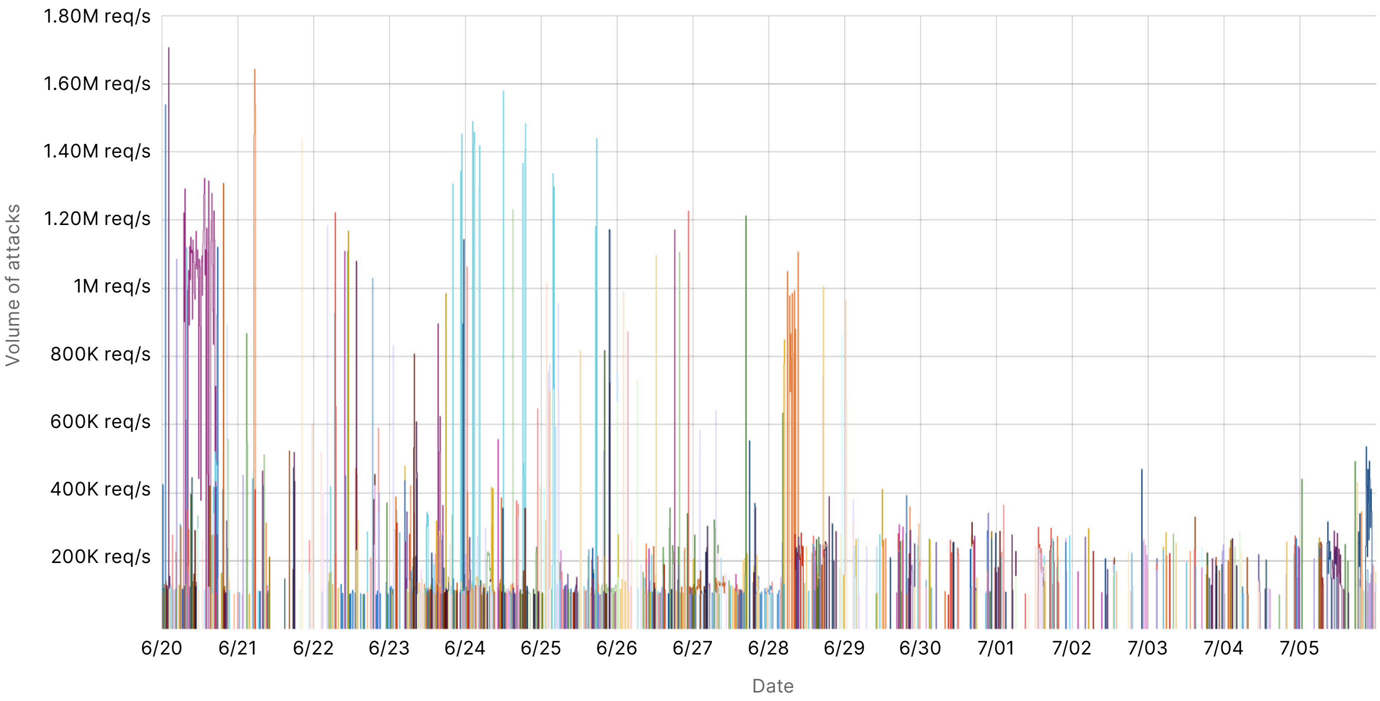
Hacktivist alliance dubbed “Darknet Parliament” in action

On June 14, Pro-Russian hacktivist groups including Killnet, a resurgence of REvil and Anonymous Sudan announced that they have joined forces, known as the “Darknet Parliament”.

Their stated aims are to execute “massive” cyber attacks on the Western financial system including Western banks, the US Federal Reserve System, and the SWIFT network (Society for Worldwide Interbank Financial Telecommunication).

In this quarter, Darknet Parliament launched as many as 10,000 DDoS attacks against Cloudflare-protected websites. However, banking and financial services websites were only the ninth most attacked industry — based on attacks we’ve seen against our customers as part of this campaign. Our systems have been automatically detecting and mitigating attacks associated with this campaign.

10,000 attacks from Killnet, REvil and Anonymous Sudan in Q2 2023 across industries



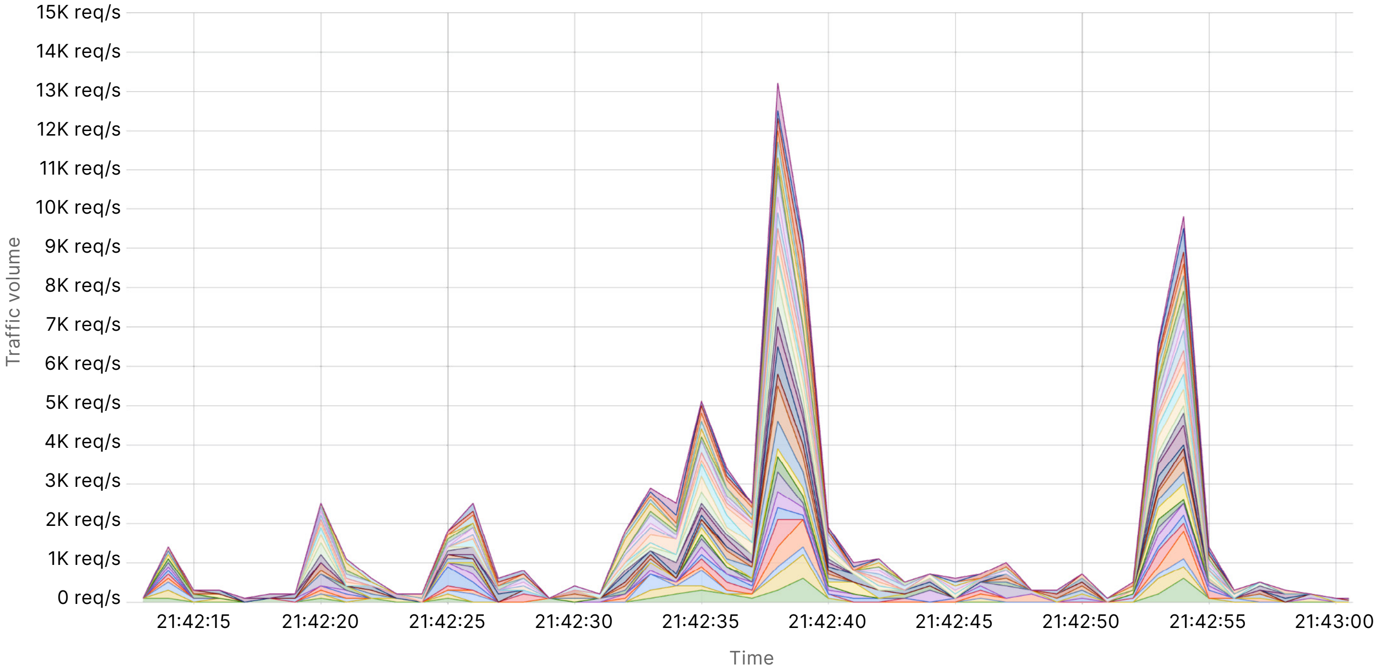
Low volume, highly randomized HTTP DDoS attacks

An HTTP DDoS attack is a DDoS attack over the Hypertext Transfer Protocol (HTTP). It targets HTTP Internet properties such as websites and API gateways. We've observed an uptick in low-volume, highly-randomized HTTP DDoS attacks over the past few months. This was previously a tactic mostly employed by well funded state sponsored actors.

It appears the threat actors behind these attacks have deliberately engineered the attacks to overcome mitigation systems by adeptly imitating users' browser behavior very accurately. In some cases, they introduce a high degree of randomization on various properties such as user agents and JA3 fingerprints.

An example of such an attack is provided below. Each different color represents a different randomization feature.

HTTP traffic volume over time for a low-volume, highly-randomised HTTP DDoS attack



DNS Laundering DDoS Attacks

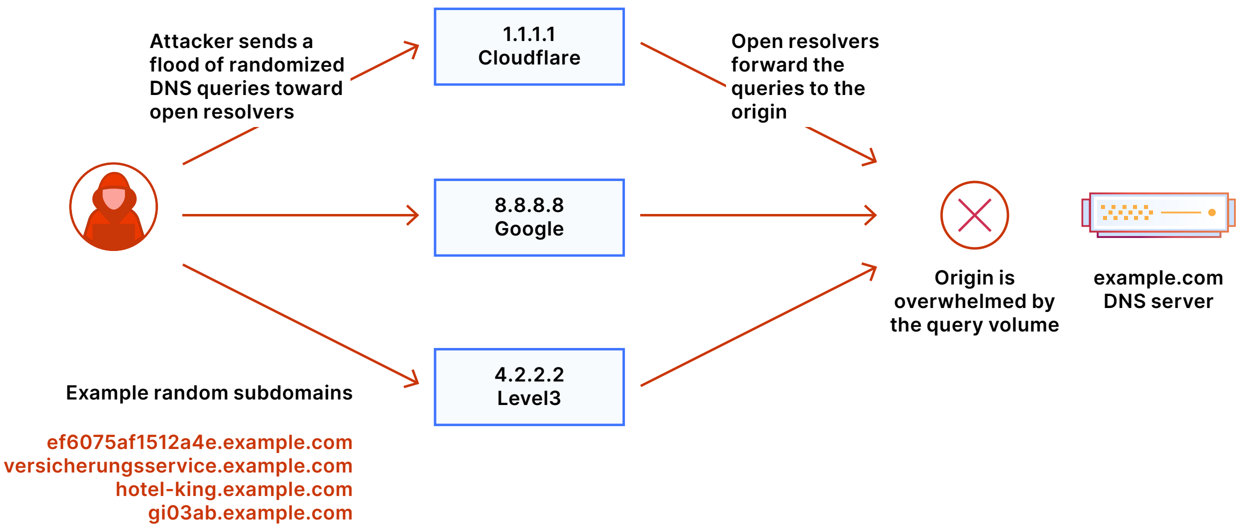
Over the past quarter, DNS-based DDoS attacks have become the most common DDoS attack vector — with 32% of all DDoS attacks targeting the DNS protocol. The Domain Name System, or DNS, serves as the phone book of the Internet. DNS helps translate the human-friendly website address (e.g. www.cloudflare.com) to a machine-friendly IP address (e.g. 104.16.124.96). By disrupting DNS servers, attackers impact the machines' ability to connect to a website, and by doing so making websites unavailable to users.

A concerning and fast-growing type is the DNS laundering attack. This can pose severe challenges to organizations that operate their own authoritative DNS servers. A DNS laundering attack is the process of making bad, malicious traffic appear as good, legitimate traffic by laundering it via reputable recursive DNS resolvers. This is similar to the process of making "dirty money" appear legal, otherwise known as money laundering.

In a DNS laundering attack, the threat actor will query subdomains of a domain that is managed by the victim's DNS server. The prefix that defines the subdomain is randomized and is never used more than once or twice in such an attack. Due to the randomization element, recursive DNS servers will never have a cached response and will need to forward the query to the victim's authoritative DNS server. The authoritative DNS server is then bombarded by so many queries until it cannot serve legitimate queries or even crashes all together.

A large Asian financial institution and a North American DNS provider are amongst the recent victims of such attacks. The source includes reputable recursive DNS servers like Google's 8.8.8.8 and Clouflare's 1.1.1.1. The attacked domain is valid and has to service legitimate queries. Hence, DNS administrators cannot block the attack source nor block all queries to the attacked domain. It's challenging to distinguish legitimate queries from malicious ones.

Attack chain of a DNS Laundering DDoS Attack

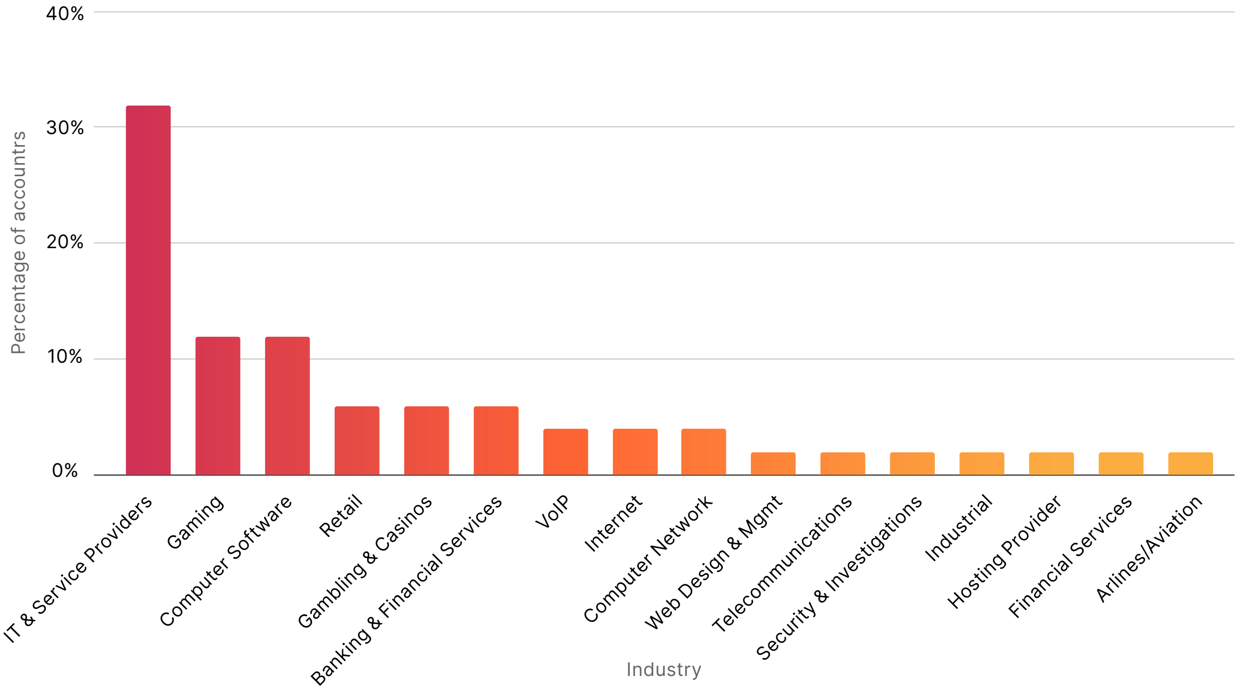

Attacker sends a flood of randomized DNS queries toward open resolvers
1.1.1.1 Cloudflare
8.8.8.8 Google
4.2.2.2 Level3
Open resolvers forward the queries to the origin
Origin is overwhelmed by the query volume
example.com DNS server
Example random subdomains
ef6075af1512a4e.example.com
versicherungsservice.example.com
hotel-king.example.com
gi03ab.example.com

“Startblast”: Exploiting Mitel vulnerabilities for DDoS attacks

At the UDP layer, we observed attacks leveraging a zero-day vulnerability (CVE-2022-26143, TP240PhoneHome) that we disclosed in March 2022. Together with other members of the InfoSec community, we identified this vulnerability in the Mitel MiCollab business phone system, exposing the system to UDP amplification DDoS attacks.

The campaign name “Startblast” comes from the eponymous debugging command that is crucial to exploiting this vulnerability. We’ve detected the majority of attacks targeting IT and service providers, more than the Gaming industry. This attack type has grown the fastest among network layer DDoS attacks in the past quarter.

Starblast attack campaigns by industry in Q2 2023



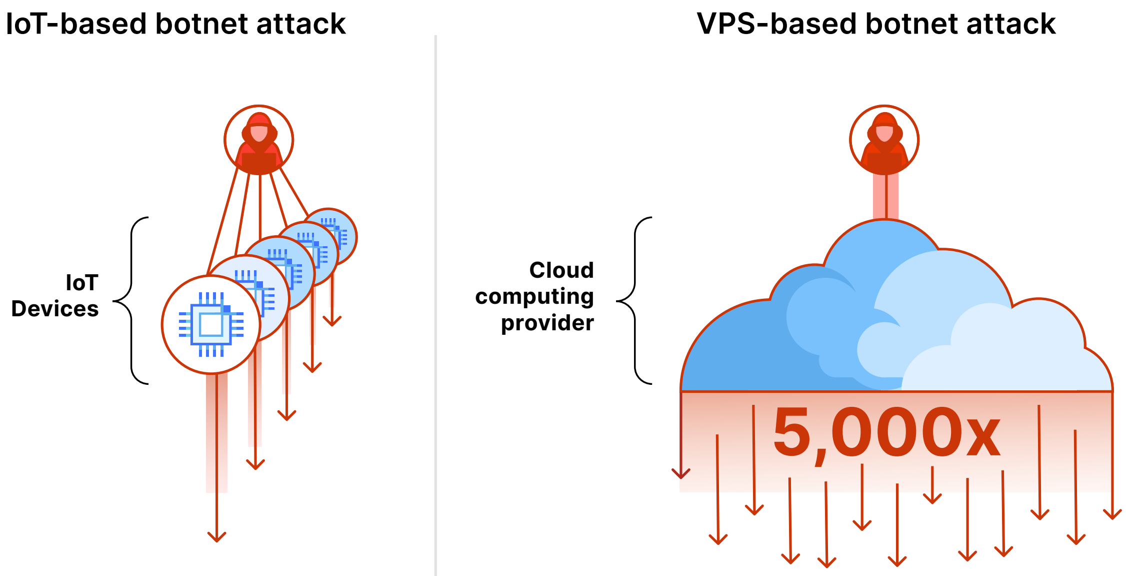
The continued rise of high performance botnets

As discussed in the Cloudflare DDoS Trends Report Q1 2023, we continue to witness an evolution in botnet DNA. The era of VM-based DDoS botnets has arrived and with it hyper-volumetric DDoS attacks. These botnets are comprised of Virtual Machines (VMs, or Virtual Private Servers, VPS) rather than Internet of Things (IoT) devices which makes them so much more powerful, up to 5,000 times stronger.

Cloudflare is collaborating with prominent cloud computing providers to combat these new botnets. We have seen early results: significant components of these botnets have been neutralized. Since then in Q2 2023, we have not seen further hyper-volumetric attacks (of the scale seen in Q1 2023 and before).

Our goal is to automate and expand this collaboration further. We request cloud computing providers, hosting providers, and other general service providers to join Cloudflare's Botnet Threat Feed.

This is free to providers and we don't sell our data to third-parties. This provides visibility into attacks originating within service providers' own networks, contributing to our collective efforts to dismantle botnets.



Key DDoS Trends — Q2 2023

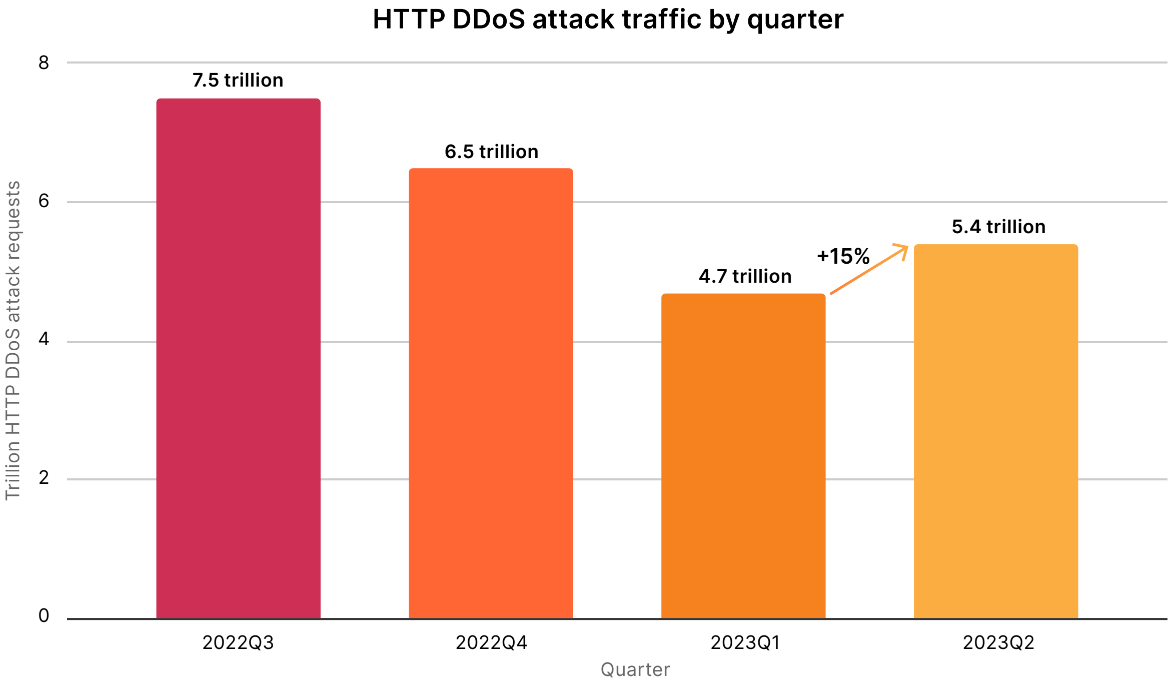
The following sections of the report will review key trends around who and what is being attacked.

Overall traffic volume changes

Application and network-layer DDoS attacks decreased by 35% and 14% respectively in the first six months of 2023 versus the same period last year. At Cloudflare, we also hope this trend of year on year decline continues as Cloudflare and the information security community make it harder and more painful for cybercriminals out there.

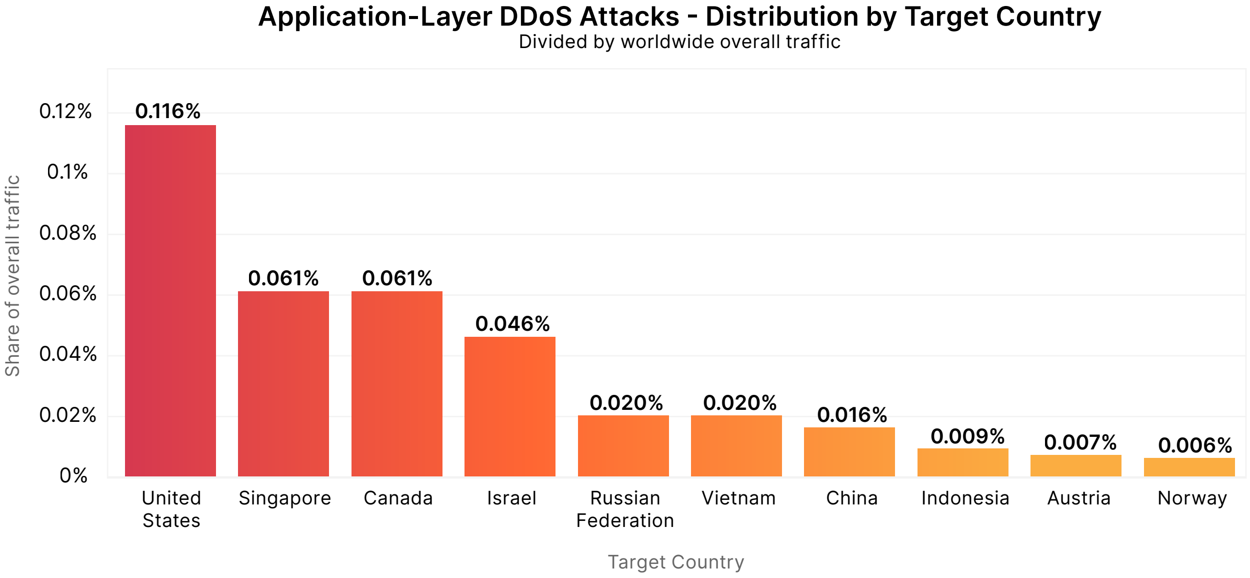
A note of caution that we did see a 15% rise in application layer DDoS attacks between Q2 2023 and the same period last year. Don’t let your defenses slip just yet!

Overall, HTTP DDoS attacks increased by 15% QoQ despite a 35% decrease YoY. Additionally, network-layer DDoS attacks decreased this quarter by approximately 14% compared to last quarter.



Top targeted countries

Last quarter, we reported that Israel was the most attacked country by application-layer DDoS attacks. This quarter, the websites located in the United States are back in the lead, with websites in Singapore and in Canada in second and third places, respectively. Attacks targeting Israeli websites decreased by 33%, moving the country's ranking to fourth.



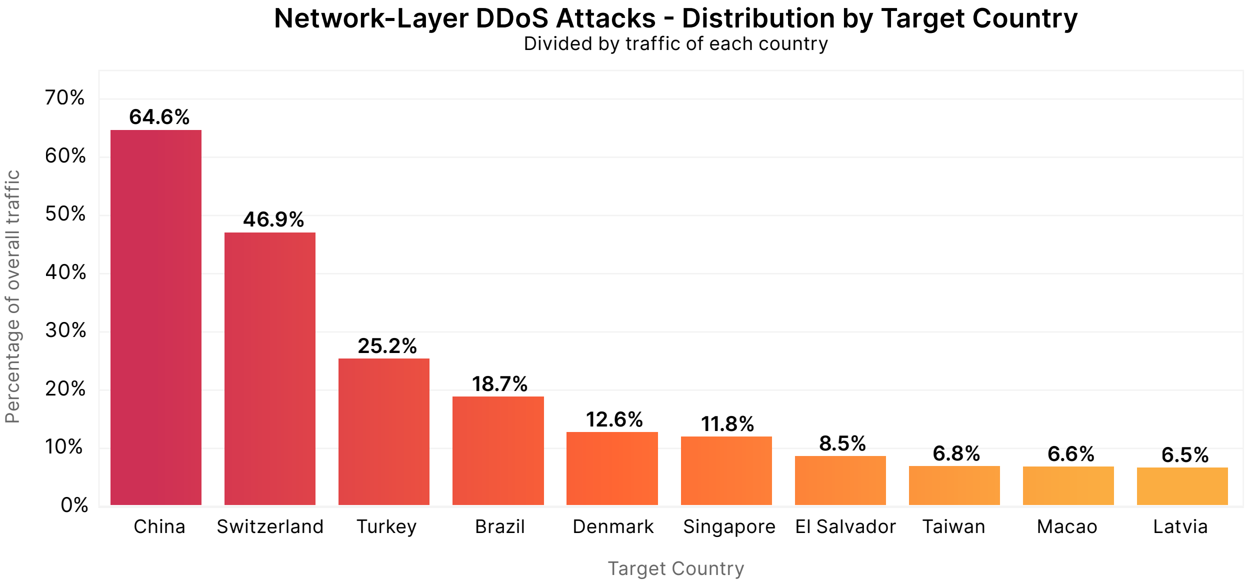
⚠ 2x more application-layer DDoS attacks

The United States receives 2x more application-layer DDoS attacks than the next most attacked country

⚠ More than 10%

More than 10% of Palestine and St. Kitts and Nevis overall application-layer traffic is filled with DDoS attacks

At the network layer, China is back to the top spot in terms of seeing the most network layer DDoS attacks. Every 2 out 3 bytes to Chinese networks carried DDoS attacks in Q2 2023. And we've seen this high of a malicious traffic share to China in multiple quarters. The unique situation in Q1 2023 where 83% of bytes to Finnish networks carried DDoS attacks has subsided. Finland has dropped out of the top ten of countries and regions facing DDoS attacks.

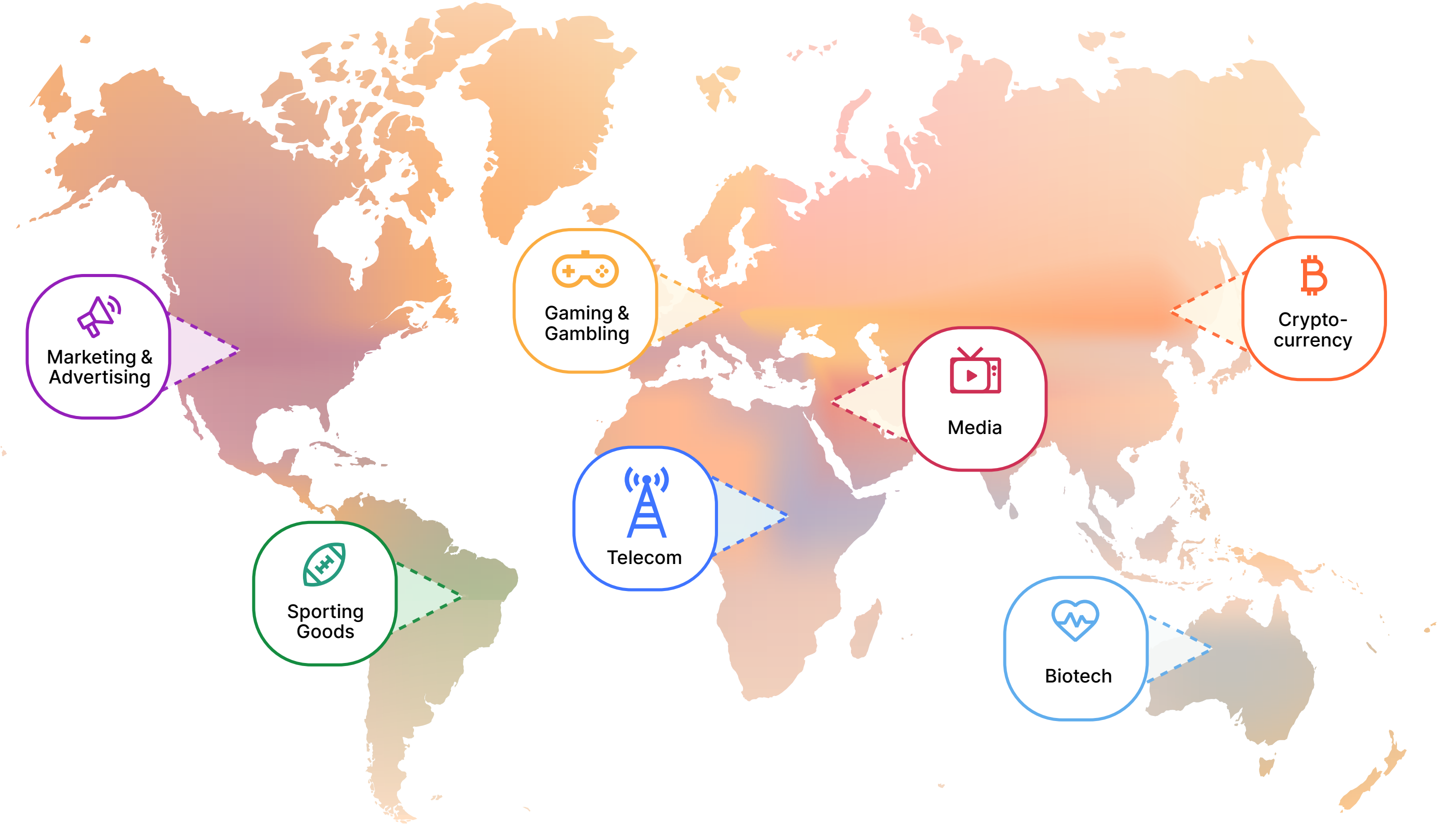


Industry and regional variations in DDoS attacks

Cryptocurrency websites were targeted with the largest amount of HTTP DDoS attack traffic in Q2 2023. Six out of every ten thousand HTTP requests towards cryptocurrency websites were part of these attacks. This represents a 600% increase compared to the previous quarter.

Gaming and gambling websites came in second place as their attack share increased by 19% in Q2 2023 compared to Q1 2023. Marketing and advertising websites not far behind in third place with little change in their share of attacks.

Unfortunately, non-profit organizations are facing a lot of attacks. In fact, 12% of HTTP traffic to non-profits was DDoS attacks - the second highest industry in share of traffic. Cloudflare protects more than 2,271 Non-profit organizations in 111 countries as part of Project Galileo which celebrated its ninth anniversary this year. Over the past months, an average of 67.7 million cyber attacks targeted non-profits on a daily basis.



Top Attacked Industry by Region

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