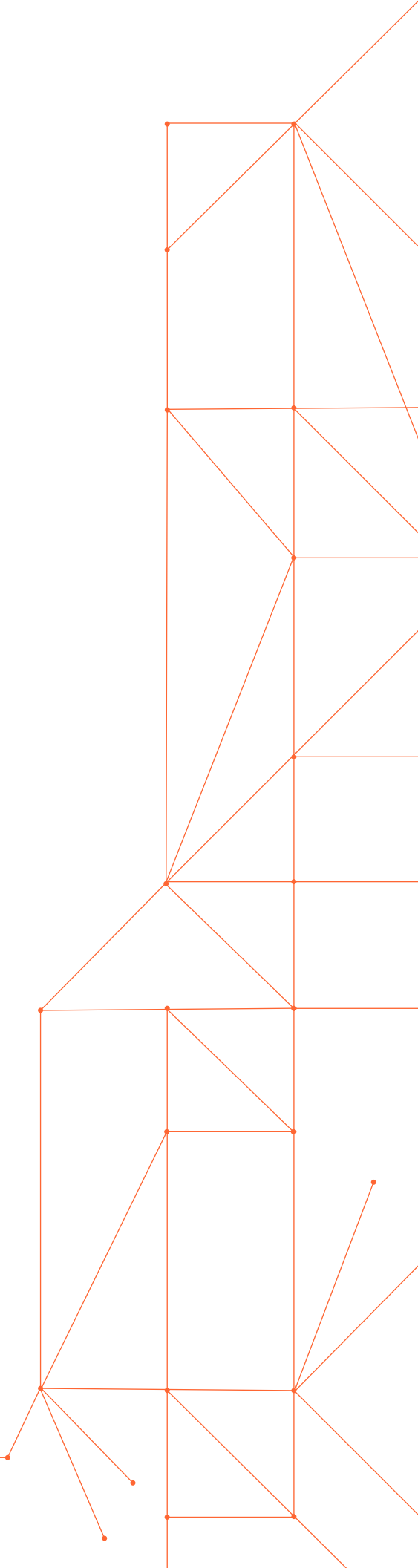
CLOUDFLARE

THREAT REPORT

Cloudflare DDoS Trends Report

Q1 2023

Content



Executive Summary

Welcome to Cloudflare's quarterly distributed denial-of-service (DDoS) report for the first quarter of 2023. This report uncovers insights and trends about the DDoS threat landscape observed across Cloudflare's global network from January through March of 2023.

This year so far has been characterized by a series of hacktivist DDoS campaigns, as well as emergence of hyper-volumetric attacks exceeding 71M requests per second, launched from high-performance VPS-based botnets. We also see Ransom DDoS attacks hold steady from Q4 2022, constituting over 16% of all DDoS attacks detected and stopped by Cloudflare.

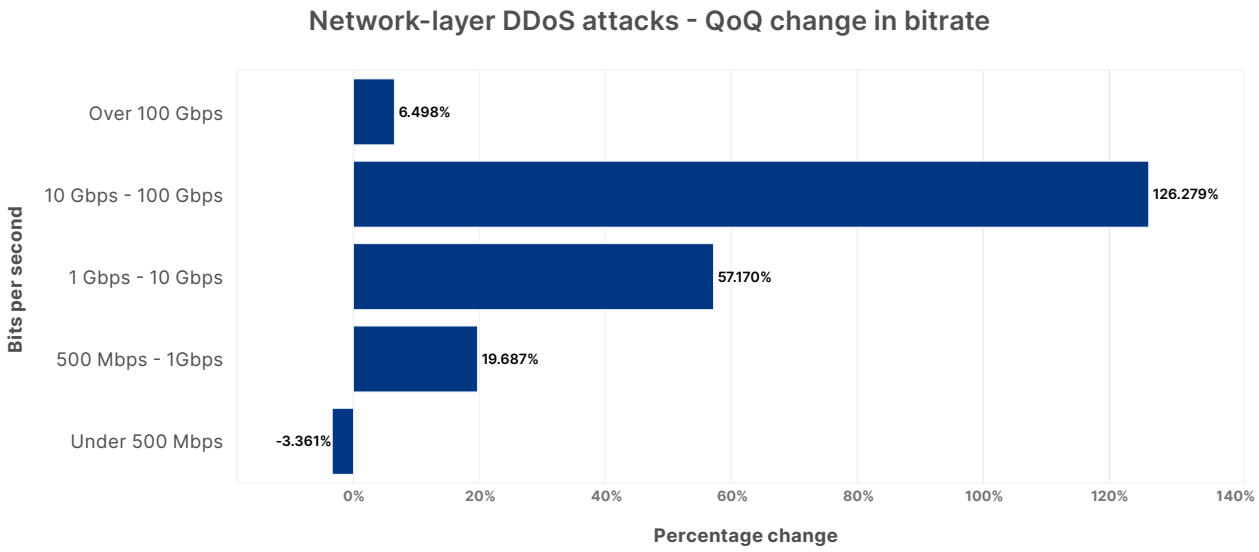
This report aggregates and analyzes all the attacks seen across the Cloudflare global network and offers key insights into the current threat landscape. In the sections below, we will outline general DDoS attack trends before breaking down application-layer, network-layer, and ransom DDoS attack insights. We also explore where DDoS attacks have been observed, share patterns in attack rates and durations, and dive deeper into attack vectors and emerging threats. 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

Global DDoS attack trends

Large-scale volumetric attacks continue to glow in size and frequency. In Q4 2022, attacks exceeding 100 Gbps increased by 67% quarter over quarter. In Q1 2023, the growth has slowed slightly to just 6%, but it's still trending higher. The largest growth was in the 10-100 Gbps range, which saw a 126% increase quarter over quarter.



This is a continuation of the trend we have observed over the years with botnets increasing in size and attack tools becoming more widely available.

While attack techniques continue to evolve, in Q1 2023 we saw DNS-based attacks were the most common. We also observed surges in attacks using SPSS, DNS amplification and GRE.

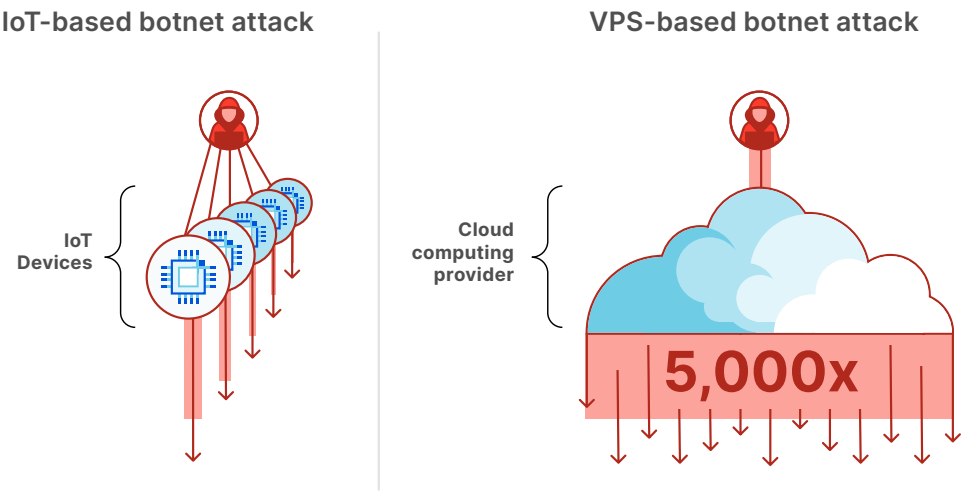
In terms of overall bandwidth, globally, Internet companies saw the largest amount of HTTP DDoS attack traffic. Afterwards, it was the Marketing and Advertising, Computer Software, Gaming / Gambling, and Telecommunications industries.

The rise of high performance botnets

In Q1, 2023, we saw hyper-volumetric DDoS attacks — one such attack exceeding 71M requests per second. Hyper-volumetric attacks leverage a new generation of botnets that are composed of Virtual Private Servers (VPS) instead of Internet of Things (IoT) devices.

Historically, large botnets have relied on small, compromised IoT devices such as smart security cameras to orchestrate their attacks. Despite the limited throughput of each IoT device, together — usually numbering in the hundreds of thousands or millions — they generated enough traffic to disrupt their targets.

The new generation of botnets uses a smaller number of devices, but each device is substantially stronger. These devices are often virtual private servers (VPS) offered by cloud computing providers. These high-performance botnets that can be as much as 5,000x stronger. Attackers gain access to VPS's by compromising unpatched servers or hacking into management consoles using leaked API credentials.

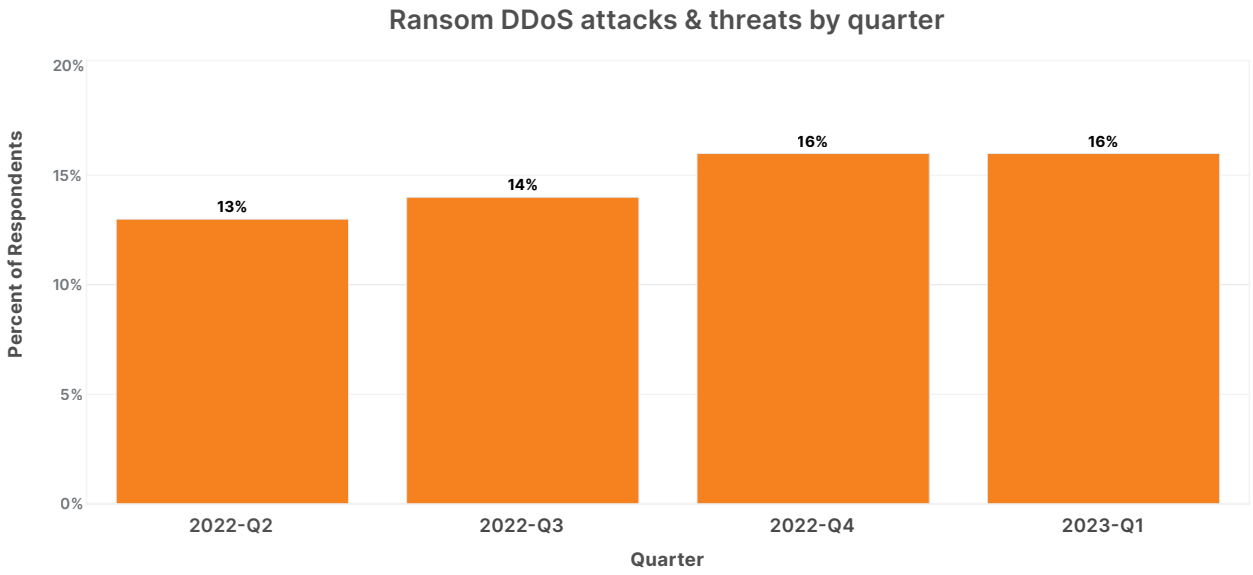


Cloudflare has been working with key cloud computing providers to crack down on these VPS-based botnets. Substantial portions of such botnets have been disabled thanks to the cloud computing providers' rapid response and diligence.

Ransom DDoS attacks

DDoS attacks are often carried out to extort ransom payments. As opposed to Ransomware attacks, which require some malware intrusion through a phishing link or zero-day exploit, Ransom DDoS attacks don't require any breach of the target systems. They instead target resources that are designed to be open to the Internet, such as customer-facing websites and apps, or public IP addresses for corporate networks.

We continue to survey Cloudflare customers and track the percentage of DDoS events where the customer received a ransom note. This number has been steadily rising through 2022 and currently stands at 16% - the same as in Q4 2022.

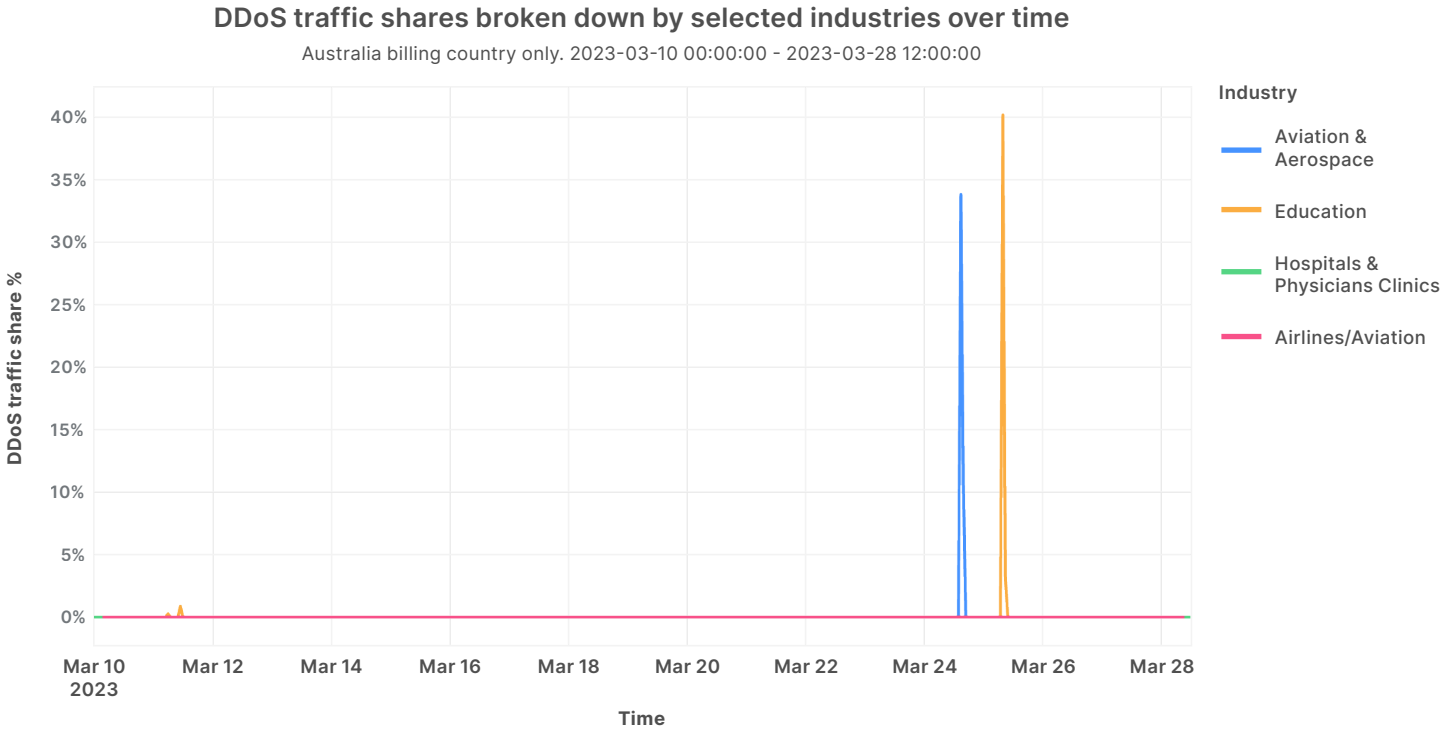


The months of January 2023 and March 2023 were the second highest in terms of Ransom DDoS activity as reported by our users. The highest month thus far remains November 2022 — the month of Black Friday, Thanksgiving, and Singles Day in China — a lucrative month for threat actors.

Rise in hacktivist campaigns

Since late 2022, we have noticed a series of hacktivist campaigns against Western targets led by pro-Russian groups with names like ‘Killnet’. Based on our observations, these groups are loosely organized gangs of hackers using Telegram channels and they do not employ any sophisticated techniques or tools. More recently, we have seen groups like AnonymousSudan join these efforts.

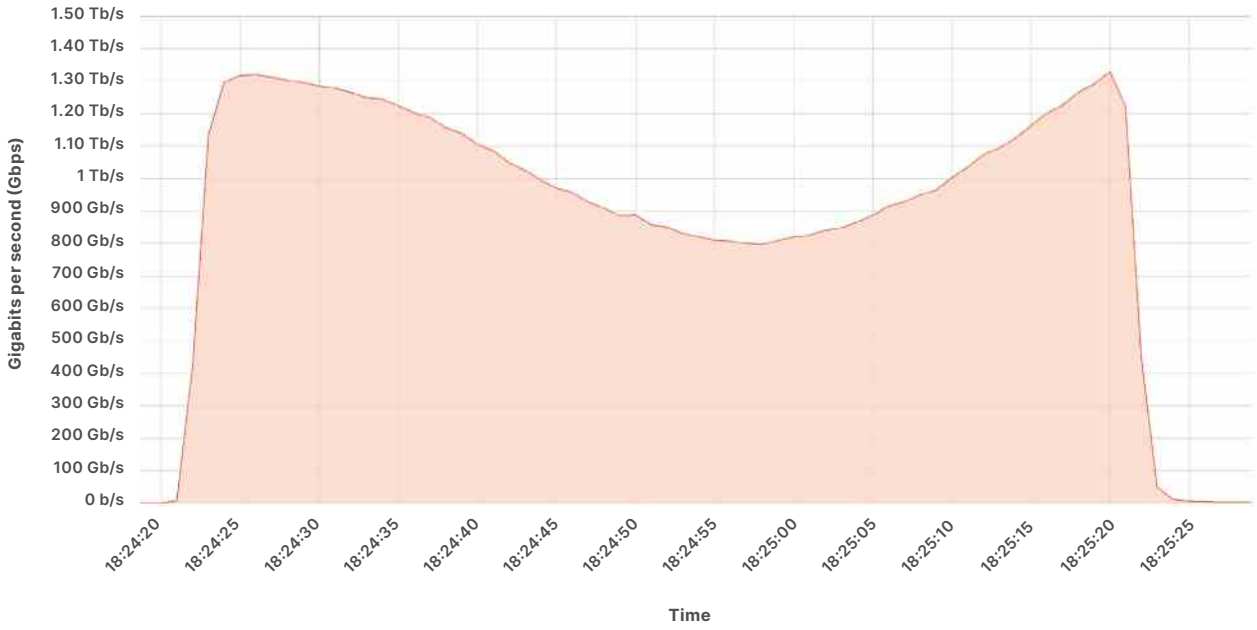
In October 2022 we noticed a wave of attacks targeting US airport websites but the damage was limited. In January 2023, we noticed similar attacks targeting healthcare organizations across the US and Western Europe. More recently in March 2023 we noticed a similar wave of attacks targeting Australian university websites.



While we don’t see any novel or sophisticated attack techniques used by these groups, we advise all organizations to remain vigilant about these campaigns and ensure adequate DDoS protection to ensure service continuity.

Terabit attacks targeting Telcos

Another large attack we saw in Q1 was a 1.3 Tbps (terabits per second) DDoS attack targeting a South American Telecommunications provider. It was a multi-vector attack involving DNS and UDP attack traffic.



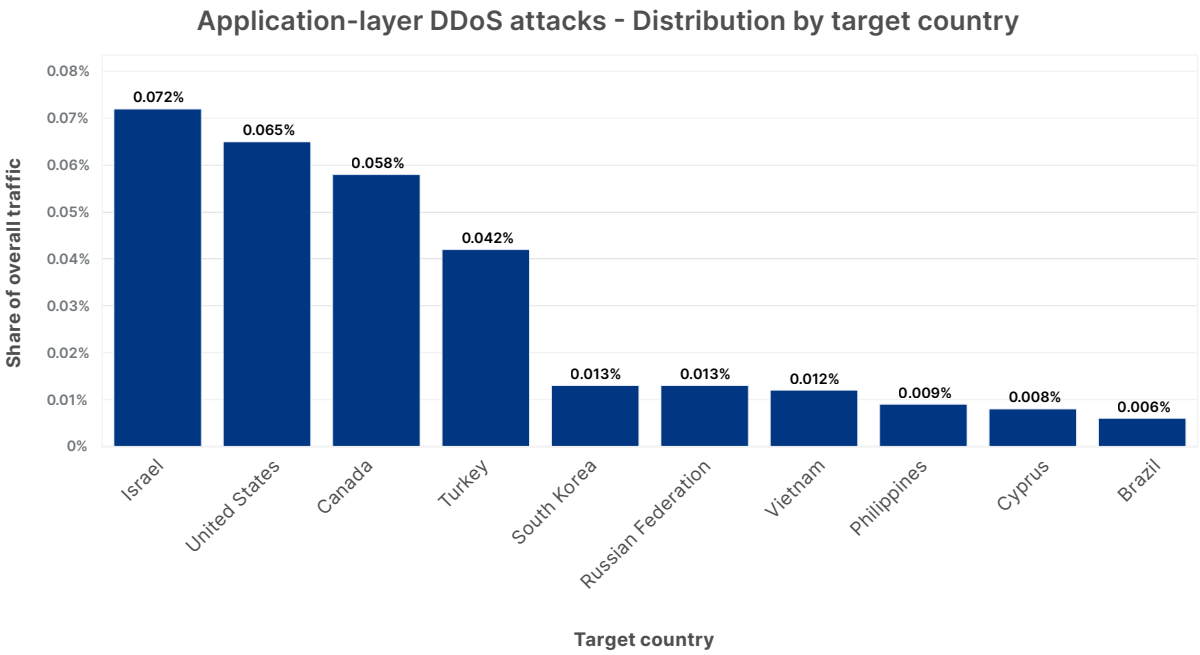
While the attack lasted only a minute, it was part of a broader campaign which included multiple Terabit-strong attacks originating from a 20,000-strong Mirai-variant botnet. Most of the attack traffic originated from the US, Brazil, Japan, Hong Kong, and India. Cloudflare systems automatically detected and mitigated it without any impact to the customer's networks.

Key DDoS Trends — Q1 2023

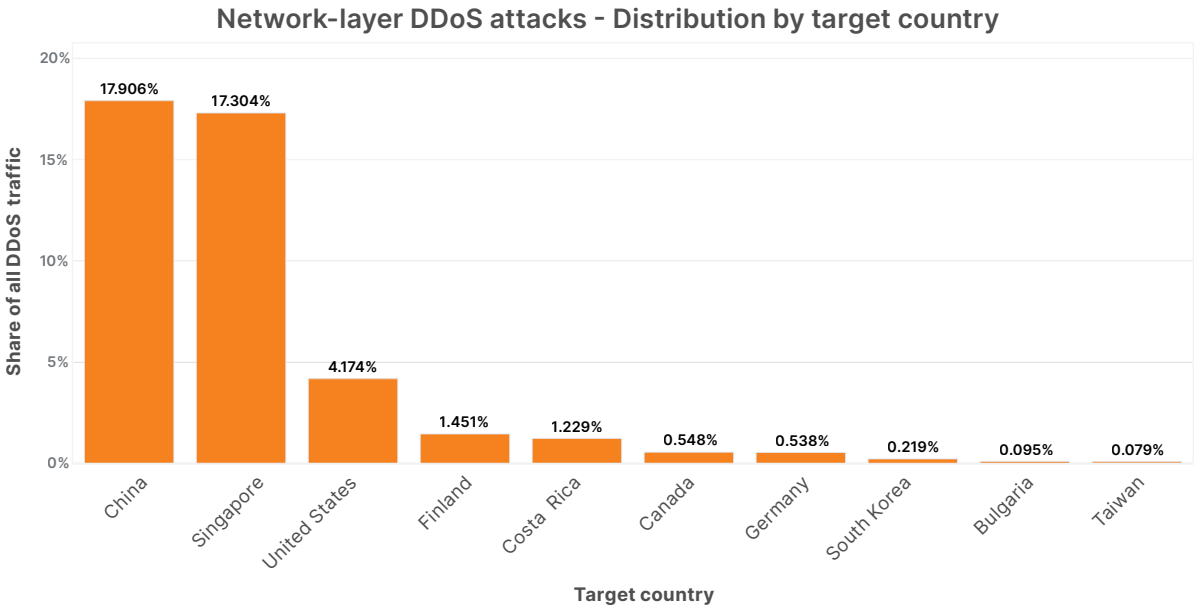
The following sections of the report will review key trends around who and what is being attacked.

Top targeted countries

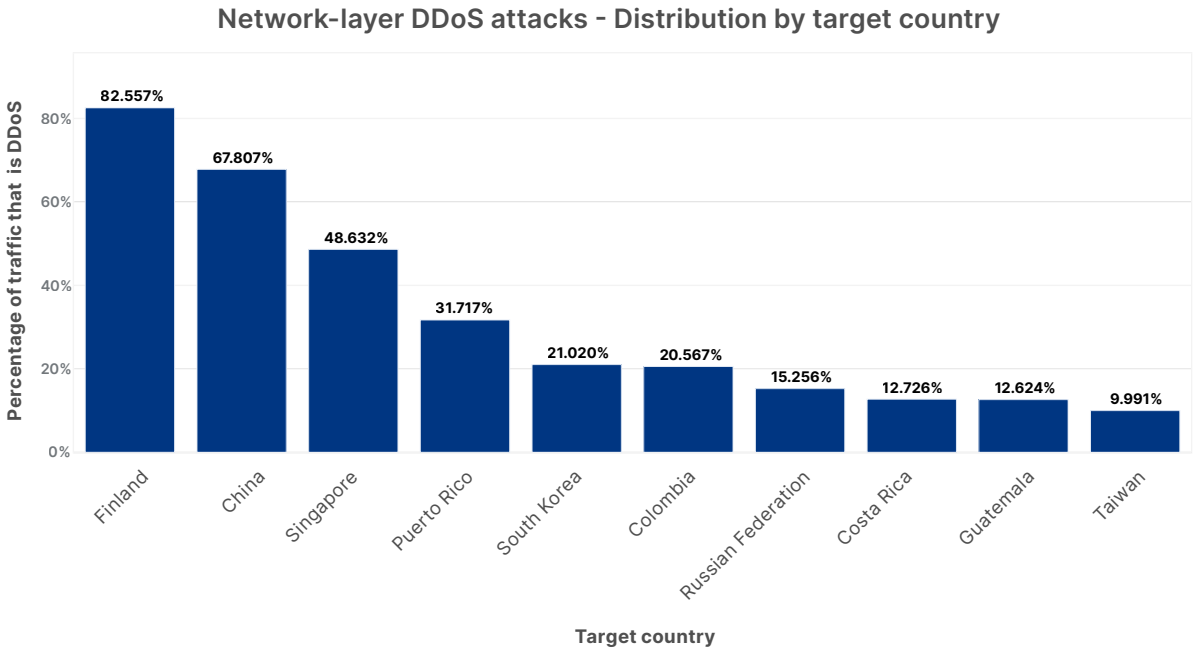
Perhaps related to the judicial reform protests, or the ongoing tensions in the West Bank, in Q1 2023, Israel jumped to the first place as the country targeted by the most HTTP DDoS attack traffic — even higher than the United States. This is a significant spike. Just short of a single percent of all HTTP traffic that Cloudflare processed in the first quarter of the year, was part of HTTP DDoS attacks that targeted Israeli websites. Following closely behind Israel are the US, Canada, and Turkey.



Looking at the total amount of network-layer DDoS attack traffic, China came in first place. Almost 18% of all network-layer DDoS attack traffic came from China. Closely in second, Singapore came in second place with a 17% share. The US came in third, followed by Finland.

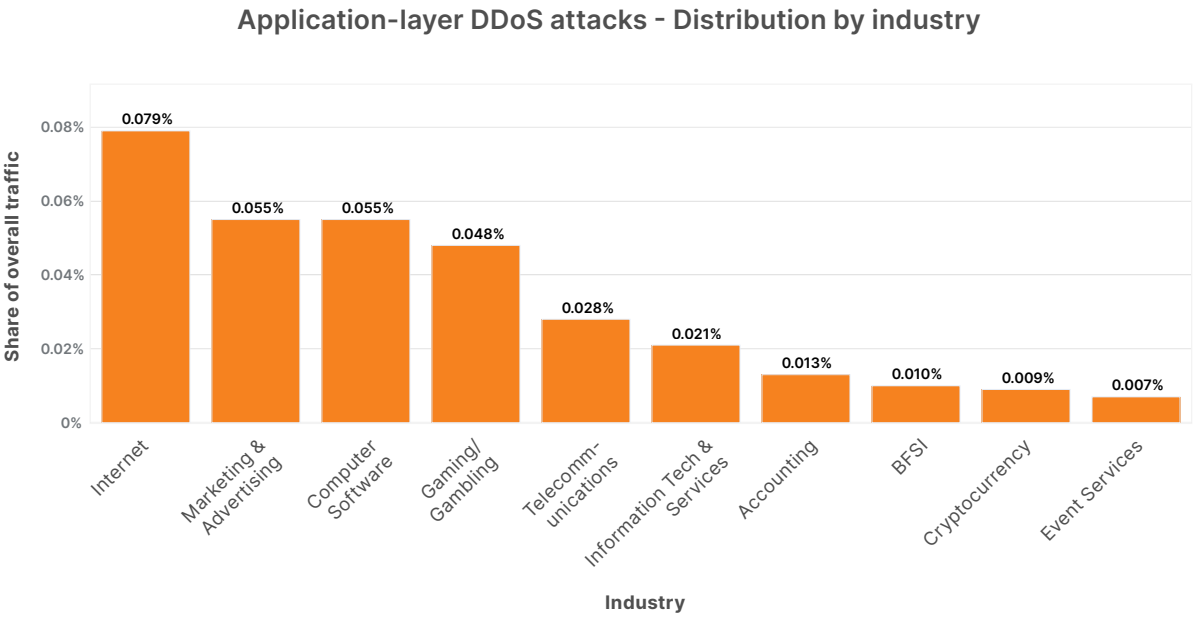


When we normalize attacks to a country by all traffic to that country, Finland jumps to the first place, perhaps due to its newly approved NATO membership. Nearly 83% of all traffic to Finland was network-layer attack traffic. China followed closely with 68% and Singapore again with 49%.



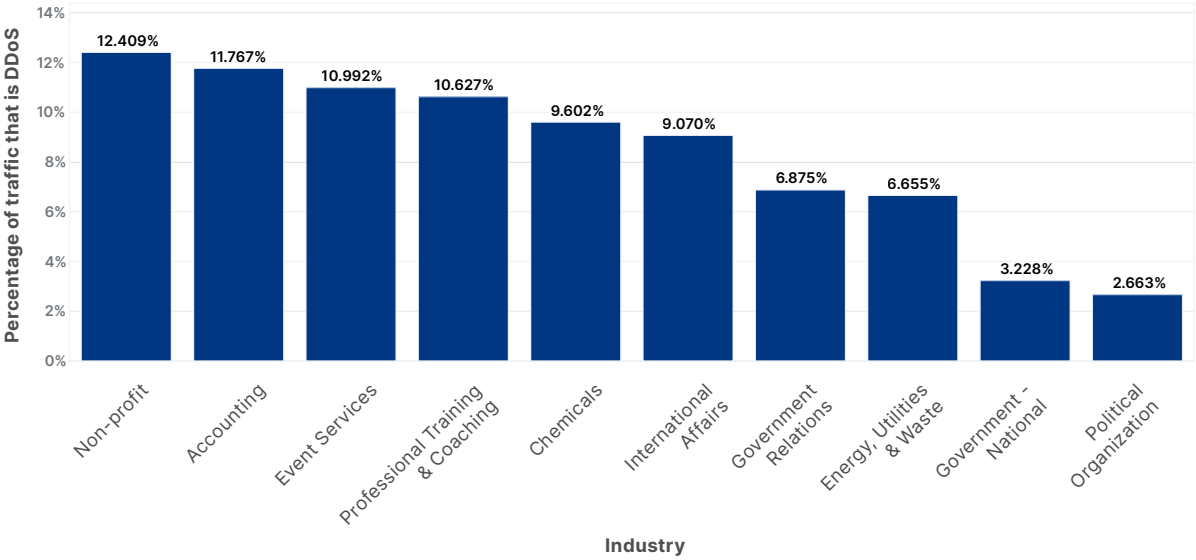
Top targeted industries

In terms of overall bandwidth, globally, Internet companies saw the largest amount of HTTP DDoS attack traffic. Afterwards, it was the Marketing and Advertising, Computer Software, Gaming/Gambling, and Telecommunications industries.



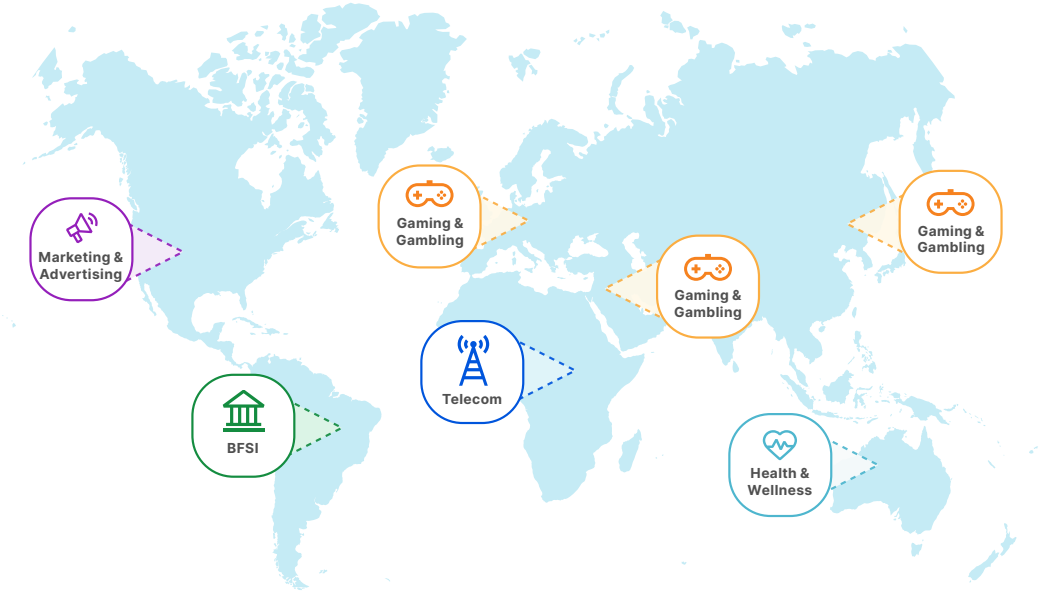
By percentage of attack traffic out of total traffic to an industry, Non-profits were the most targeted in the first quarter of the year, followed by Accounting firms. Despite the uptick of attacks on healthcare, the industry didn't make it into the top ten. Also up there were Chemicals, Government, and Energy Utilities & Waste industries. Looking at the US, almost 2% of all traffic to US Federal websites were part of DDoS attacks.

Application-layer DDoS attacks - Distribution by industry

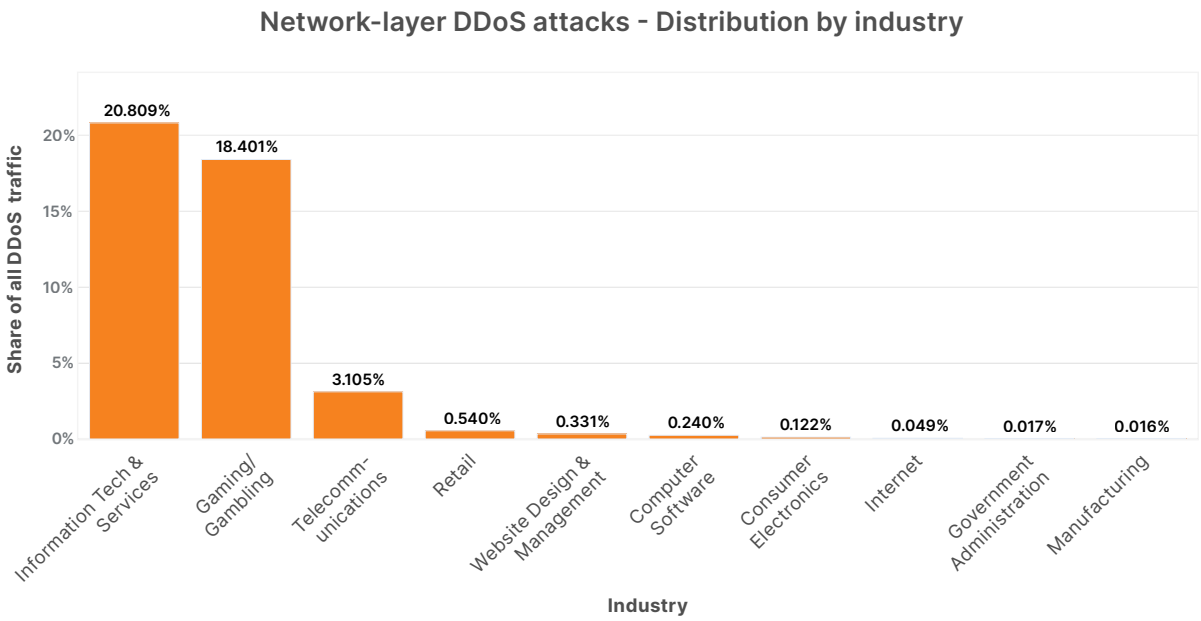


On a regional scale, the Gaming & Gambling industry was the most targeted in Asia, Europe, and the Middle East. In South and Central America, the Banking, Financial Services and Insurance (BFSI) industry was the most targeted. In North America it was the Marketing & Advertising industry followed by Telecommunications — which was also the most attacked industry in Africa. Last but not least, in Oceania, the Health, Wellness and Fitness industry was the most targeted by HTTP DDoS attacks.

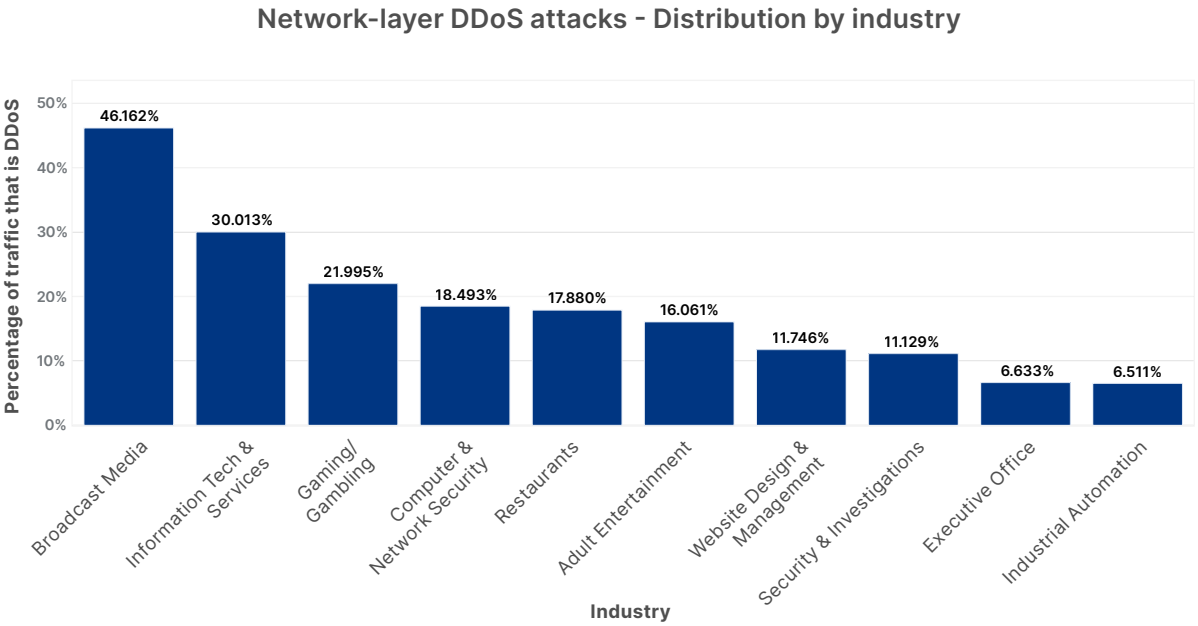
Top attacked industry by region



Diving lower in the OSI stack, based on the total volume of L3/4 attack traffic, the most targeted industries were Information Technology and Services, Gaming/Gambling, and Telecommunications.

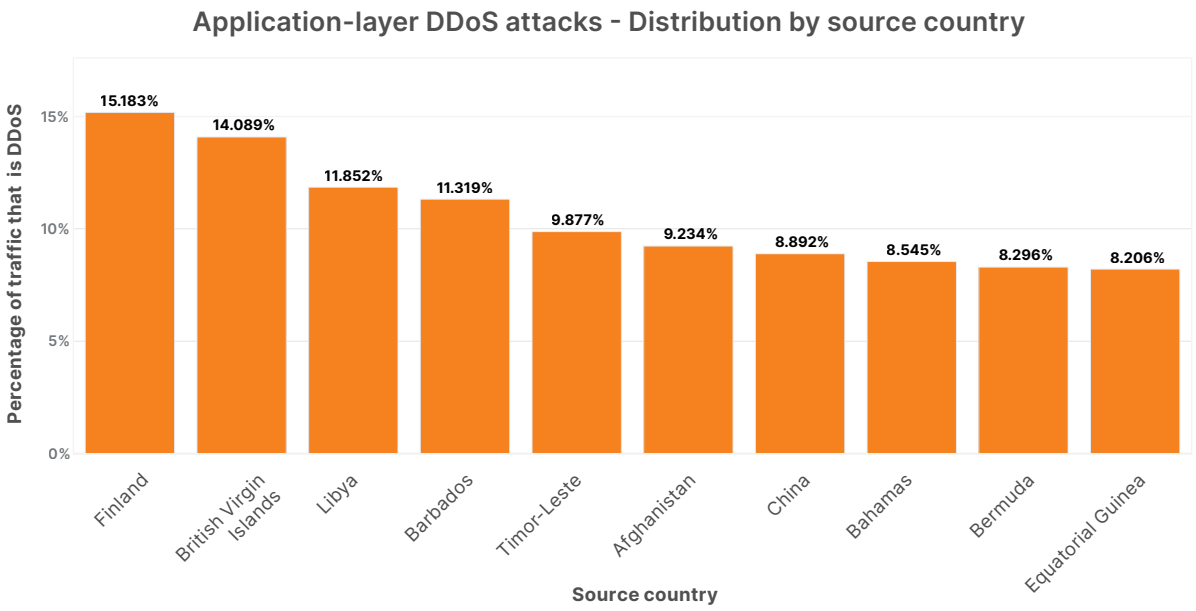


When comparing the attack traffic to the total traffic per industry, we see a different picture. Almost every second byte transmitted to Broadcast Media companies was L3/4 DDoS attack traffic.

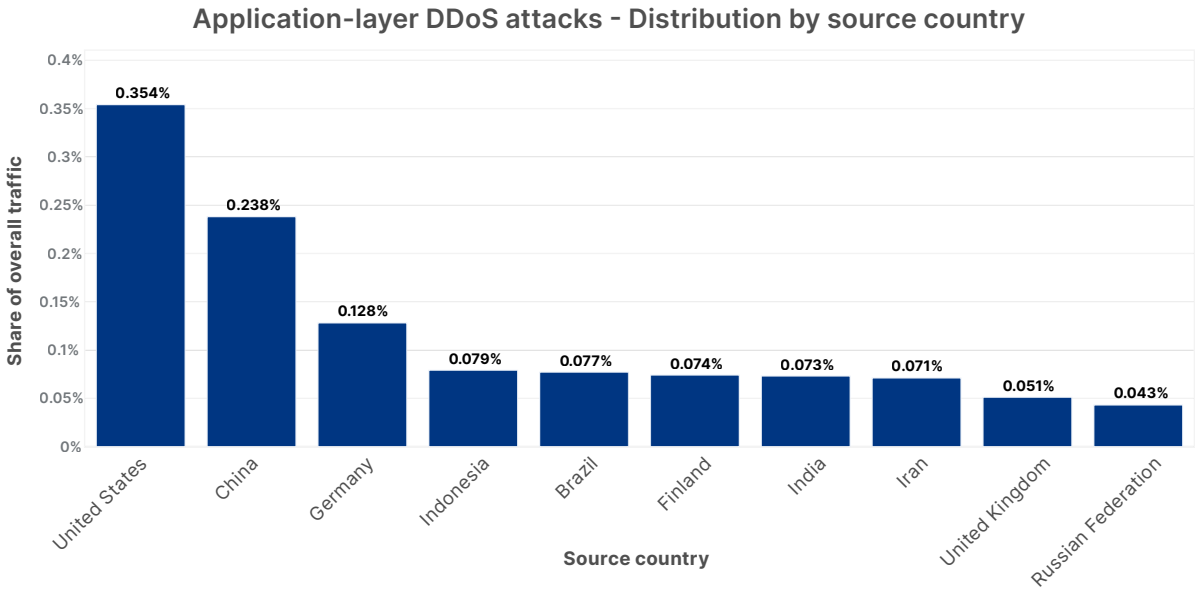


Top attack sources

In the first quarter of 2023, Finland was the largest source of HTTP DDoS attacks in terms of the percentage of attack traffic out of all traffic per country. Closely after Finland, the British Virgin Islands came in second place, followed by Libya and Barbados.

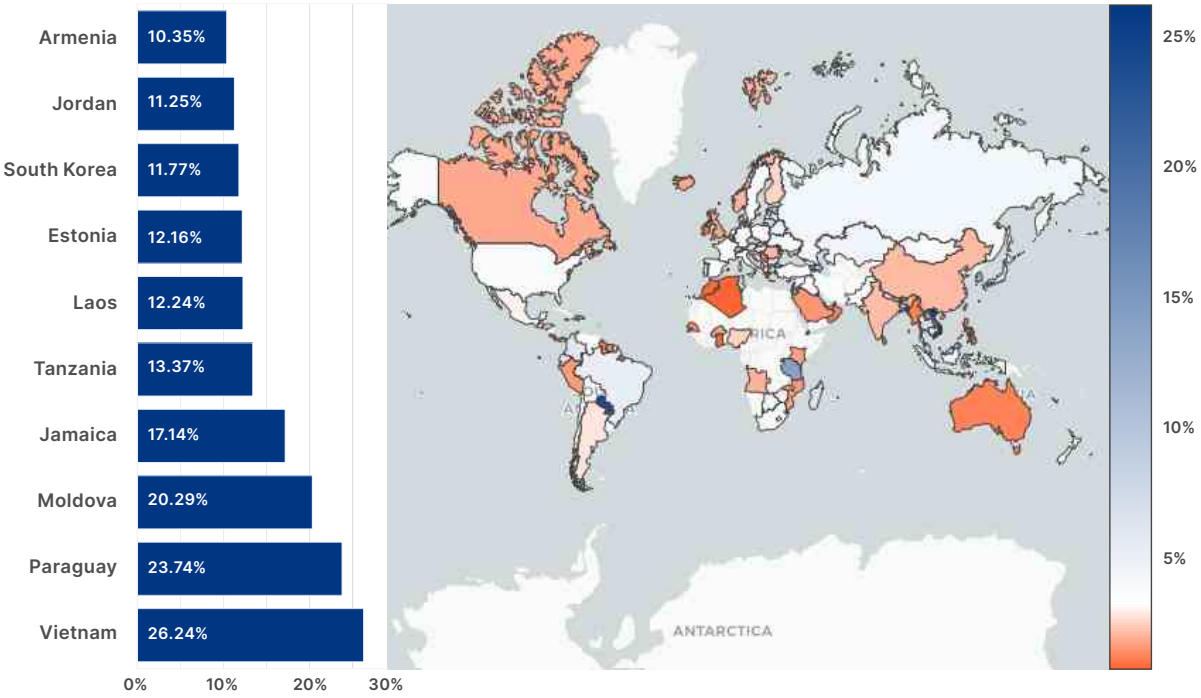


In terms of absolute volumes, the most HTTP DDoS attack traffic came from US IP addresses. China came in second, followed by Germany, Indonesia, Brazil, and Finland.



At the network layer, Vietnam was the largest source of L3/4 DDoS attack traffic. Almost a third of all L3/4 traffic we ingested in our Vietnam data centers was attack traffic. Following Vietnam were Paraguay, Moldova, and Jamaica.

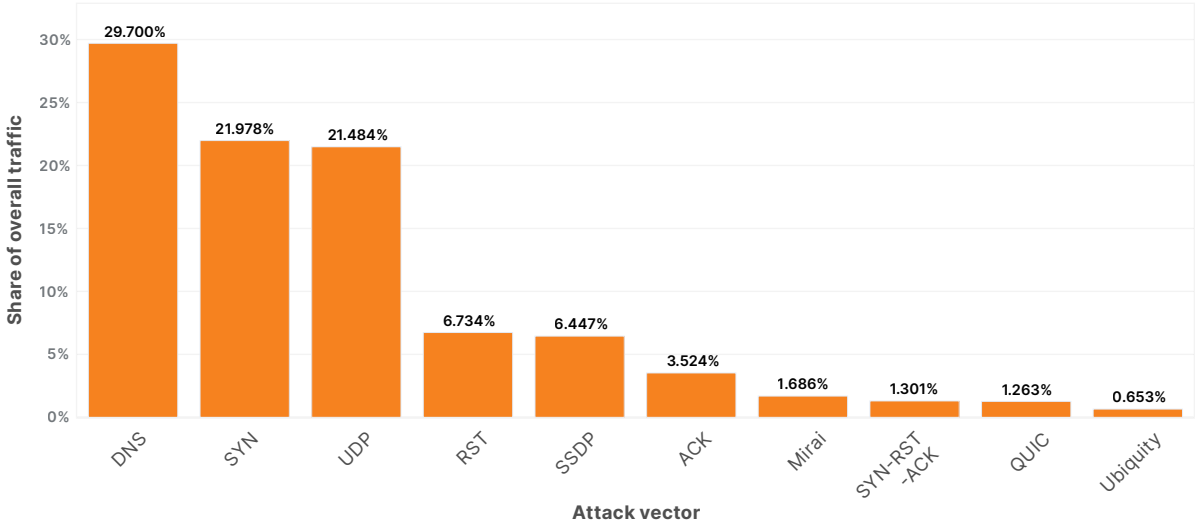
Network-layer DDoS attacks - Top ingress countries worldwide



Attack vectors

This quarter we saw a tectonic shift. With a 22% share, SYN floods scooched to the second place, making DNS-based DDoS attacks the most popular attack vector (30%). Almost a third of all L3/4 DDoS attacks were DNS-based; either DNS floods or DNS amplification/reflection attacks. Not far behind, UDP-based attacks came in third with a 21% share.

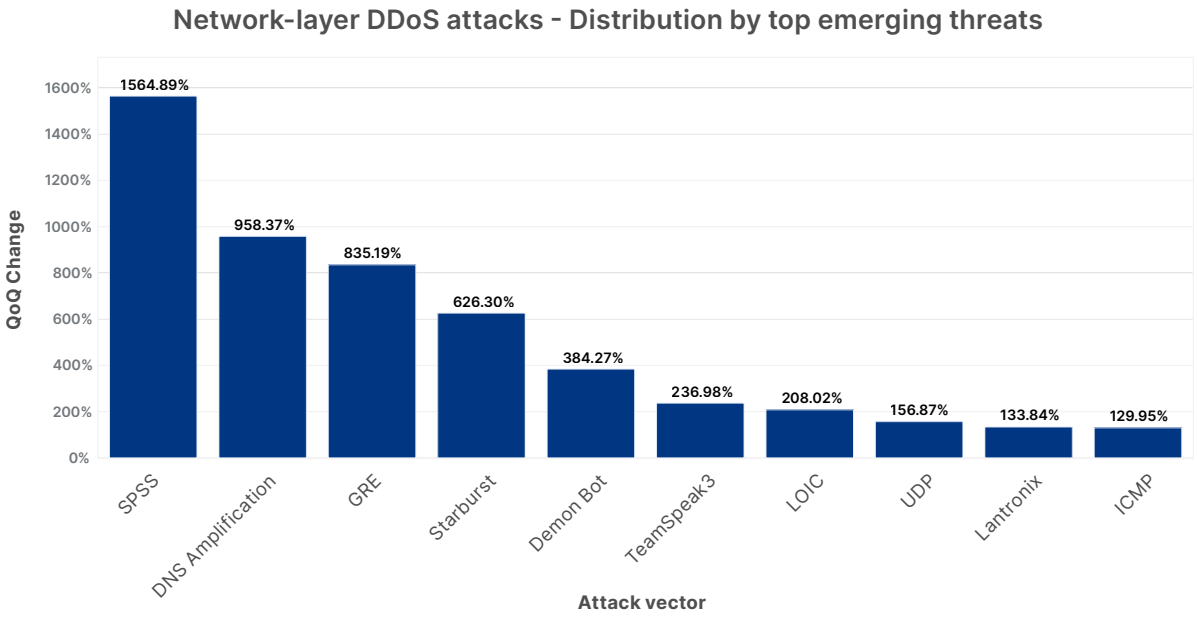
Network-layer DDoS attacks - Distribution by top attack vectors



Emerging threats

Every quarter we see the reemergence of old, and sometimes even ancient, attack vectors. What this tells us is that even decade-old vulnerabilities are still being exploited to launch attacks. Threat actors are recycling and reusing old methods — perhaps hoping that organizations have dropped those protections against older methods.

In the first quarter of 2023, there was a massive surge in SPSS-based DDoS attacks, DNS amplification attacks and GRE-based DDoS attacks.



Key Takeaways

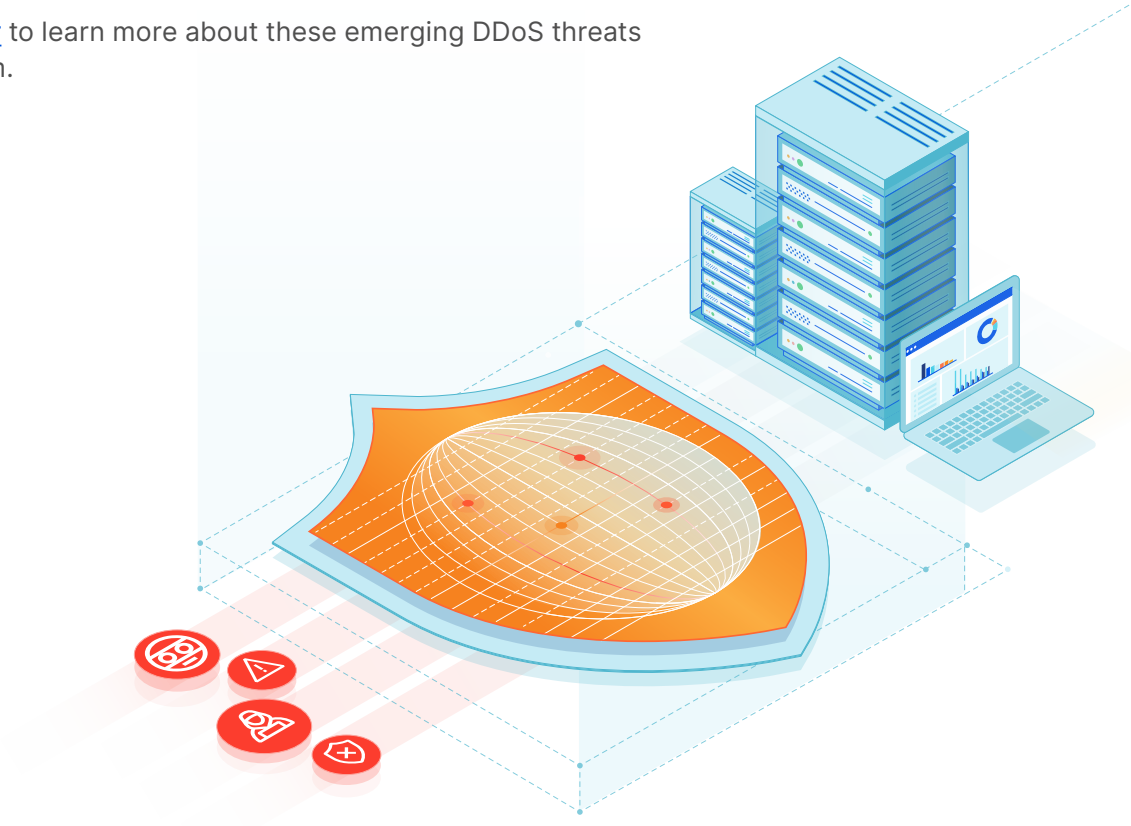
DDoS attacks are a problem almost as old as the Internet and it's a matter of when, not if your Internet-facing infrastructure will be targeted. While the goal has traditionally been to disrupt service availability for different nefarious reasons, ransom DDoS attacks introduce an additional layer of financial motivation. While we continue to monitor ransomware and ransom DDoS trends as they evolve, our advice remains the same — do not pay. Instead, work with local law enforcement to curtail the threat and invest in strong DDoS defenses so that your organization becomes an uneconomical target for these attacks.

With the rise in VPS-based botnets, expect more hyper-volumetric attacks at the application layer as extreme levels of computing power can now be commandeered and directed at your organization. Combating this threat will require on-going collaboration between cloud computing providers and DDoS mitigation providers like Cloudflare so that these VPS-based botnets can be disabled quickly once detected.

We also advise organizations to be hyper-vigilant for hacktivist campaigns targeting critical infrastructure. We will continue to monitor this situation and report on developments via the Cloudflare blog. Subscribe to the blog for regular updates.

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 | www.cloudflare.com

REV:BDES-4486.2023APR21