Cloudflare DDoS threat report for 2022 Q4

01/10/2023

Omer Yoachimik

15 min read

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

Welcome to our DDoS Threat Report for the fourth and final quarter of 2022. This report includes insights and trends about the DDoS threat landscape - as observed across Cloudflare's global network.

In the last quarter of the year, as billions around the world celebrated holidays and events such as Thanksgiving, Christmas, Hanukkah, Black Friday, Singles' Day, and New Year, DDoS attacks persisted and even increased in size, frequency, and sophistication whilst attempting to disrupt our way of life.

Cloudflare's automated DDoS defenses stood firm and mitigated millions of attacks in the last quarter alone. We've taken all of those attacks, aggregated, analyzed, and prepared the bottom lines to help you better understand the threat landscape.

Global DDoS insights

In the last quarter of the year, despite a year-long decline, the amount of HTTP DDoS attack traffic still increased by 79% YoY. While most of these attacks were small, Cloudflare constantly saw terabit-strong attacks, DDoS attacks in the hundreds of millions of packets per second, and HTTP DDoS attacks peaking in the tens of millions of requests per second launched by sophisticated botnets.

- Volumetric attacks surged; the number of attacks exceeding rates of 100 gigabits per second (Gbps) grew by 67% quarter-over-quarter (QoQ), and the number of attacks lasting more than three hours increased by 87% QoQ.
- Ransom DDoS attacks steadily increased this year. In Q4, over 16% of respondents reported receiving a threat or ransom demand as part of the DDoS attack that targeted their Internet properties.

Industries most targeted by DDoS attacks

- HTTP DDoS attacks constituted 35% of all traffic to Aviation and Aerospace Internet properties.
- Similarly, over a third of all traffic to the Gaming/Gambling and Finance industries was network-layer DDoS attack traffic.
- A whopping 92% of traffic to Education Management companies was part of network-layer DDoS attacks. Likewise, 73% of traffic to the Information

Technology and Services and the Public Relations & Communications industries were also network-layer DDoS attacks.

Source and targets of DDoS attacks

- In Q4, 93% of network-layer traffic to Chinese Internet properties behind Cloudflare were part of network-layer DDoS attacks. Similarly, over 86% of traffic to Cloudflare customers in Lithuania and 80% of traffic to Cloudflare customers in Finland was attack traffic.
- On the application-layer, over 42% of all traffic to Georgian Internet properties behind Cloudflare was part of HTTP DDoS attacks, followed by Belize with 28%, and San Marino in third place with just below 20%. Almost 20% of all traffic from Libya that Cloudflare saw was application-layer DDoS attack traffic.
- Over 52% of all traffic recorded in Cloudflare's data centers in Botswana was network-layer DDoS attack traffic. Similarly, in Cloudflare's data centers in Azerbaijan, Paraguay, and Palestine, network-layer DDoS attack traffic constituted approximately 40% of all traffic.

Quick note: this quarter, we've made a change to our algorithms to improve the accuracy of our data which means that some of these data points are incomparable to previous quarters. Read more about these changes in the next section *Changes to the report methodologies*.

To skip to the report, click here.

Sign up to the DDoS Trends Webinar to learn more about the emerging threats and how to defend against them.

Changes to the report methodologies

Since our first report in 2020, we've always used percentages to represent attack traffic, i.e., the percentage of attack traffic out of all traffic including

legitimate/user traffic. We did this to normalize the data, avoid data biases, and be more flexible when it comes to incorporating new mitigation system data into the report.

In this report, we've introduced changes to the methods used to calculate some of those percentages when we bucket attacks by certain *dimensions* such as *target country*, *source country*, or *target industry*. In the *application-layer* sections, we previously divided the amount of attack HTTP/S requests to a given dimension by all the HTTP/S requests to all dimensions. In the *network-layer* section, specifically in *Target industries* and *Target countries,* we used to divide the amount of attack IP packets to a given dimension by the total attack packets to all dimensions.

From this report onwards, we now divide the attack requests (or packets) to a given dimension only by the total requests (or packets) to that given dimension. We made these changes in order to align our calculation methods throughout the report and improve the data accuracy so it better represents the attack landscape.

For example, the top industry attacked by application-layer DDoS attacks using the previous method was the Gaming and Gambling industry. The attack requests towards that industry accounted for 0.084% of all traffic (attack and non-attack) to all industries. Using that same old method, the Aviation and Aerospace industry came in 12th place. Attack traffic towards the Aviation and Aerospace industry accounted for 0.0065% of all traffic (attack and non-attack) to all industries. However, using the new method, the Aviation and Aerospace industry came in as the number one most attacked industry — attack traffic formed 35% of all traffic (attack and non-attack) towards that industry alone. Again using the new method, the Gaming and Gambling industry came in 14th place — 2.4% of its traffic was attack traffic.

The old calculation method used in previous reports to calculate the percentage of attack traffic for each dimension was the following:

- Percentage of application-layer DDoS attack traffic: $\frac{attack\_requests\_to\_dimensionX}{all\_requests}$
- Percentage of network-layer DDoS attack traffic: $\frac{attack\_packets\_to\_dimensionX}{all\_attack\_packets}$

The new calculation method used from this report onwards is the following:

- Percentage of application-layer DDoS attack traffic: $\frac{attack\_requests\_to\_dimensionX}{all\_requests\_to\_dimensionX}$
- Percentage of network-layer DDoS attack traffic: $\frac{attack\_packets\_to\_dimensionX}{all\_packets\_to\_dimensionX}$

The changes apply to the following metrics:

1. Target industries of application-layer DDoS attacks
2. Target countries of application-layer DDoS attacks
3. Source of application-layer DDoS attacks
4. Target industries of network-layer DDoS attacks
5. Target countries of network-layer DDoS attacks

No other changes were made in the report. The *Source of network-layer DDoS attacks* metrics already use this method since the first report. Also, no changes were made to the *Ransom DDoS attacks*, *DDoS attack rate*, *DDoS attack duration, DDoS attack vectors,* and *Top emerging threats* sections. These metrics do not take legitimate traffic into consideration and no methodology alignment was needed.

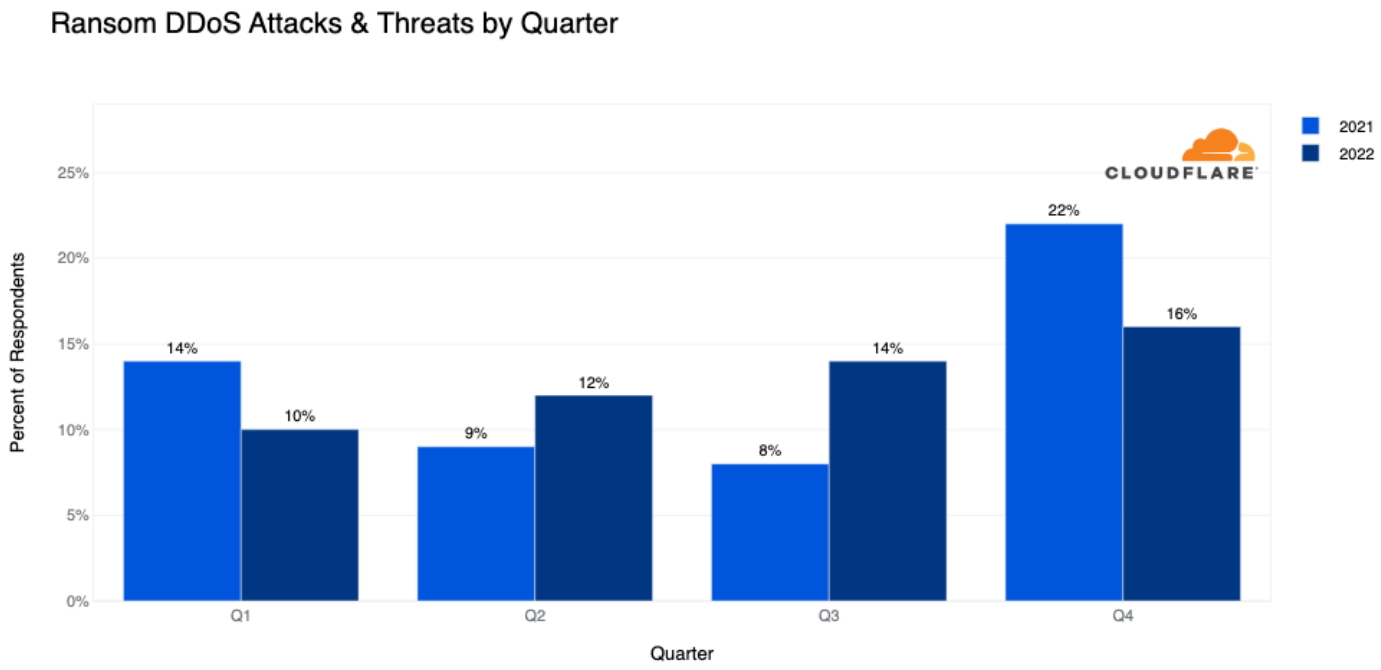
With that in mind, let's dive in deeper and explore these insights and trends. You can also view an interactive version of this report on Cloudflare Radar.

Ransom DDoS attacks

As opposed to Ransomware attacks, where the victim is tricked into downloading a file or clicking on an email link that encrypts and locks their computer files until they pay a ransom fee, Ransom DDoS attacks can be much easier for attackers to launch. Ransom DDoS attacks don't require tricking the victim into opening an email or clicking a link, nor do they require a network intrusion or a foothold to be carried out.

In a Ransom DDoS attack, the attacker doesn't need access to the victim's computer but rather just floods them with enough traffic to negatively impact their Internet services. The attacker will demand a ransom payment, usually in the form of Bitcoin, to stop and/or avoid further attacks.

In the last quarter of 2022, 16% of Cloudflare customers that responded to our survey reported being targeted by HTTP DDoS attacks accompanied by a threat or a ransom note. This represents a 14% increase QoQ but a 16% decrease YoY in reported Ransom DDoS attacks.



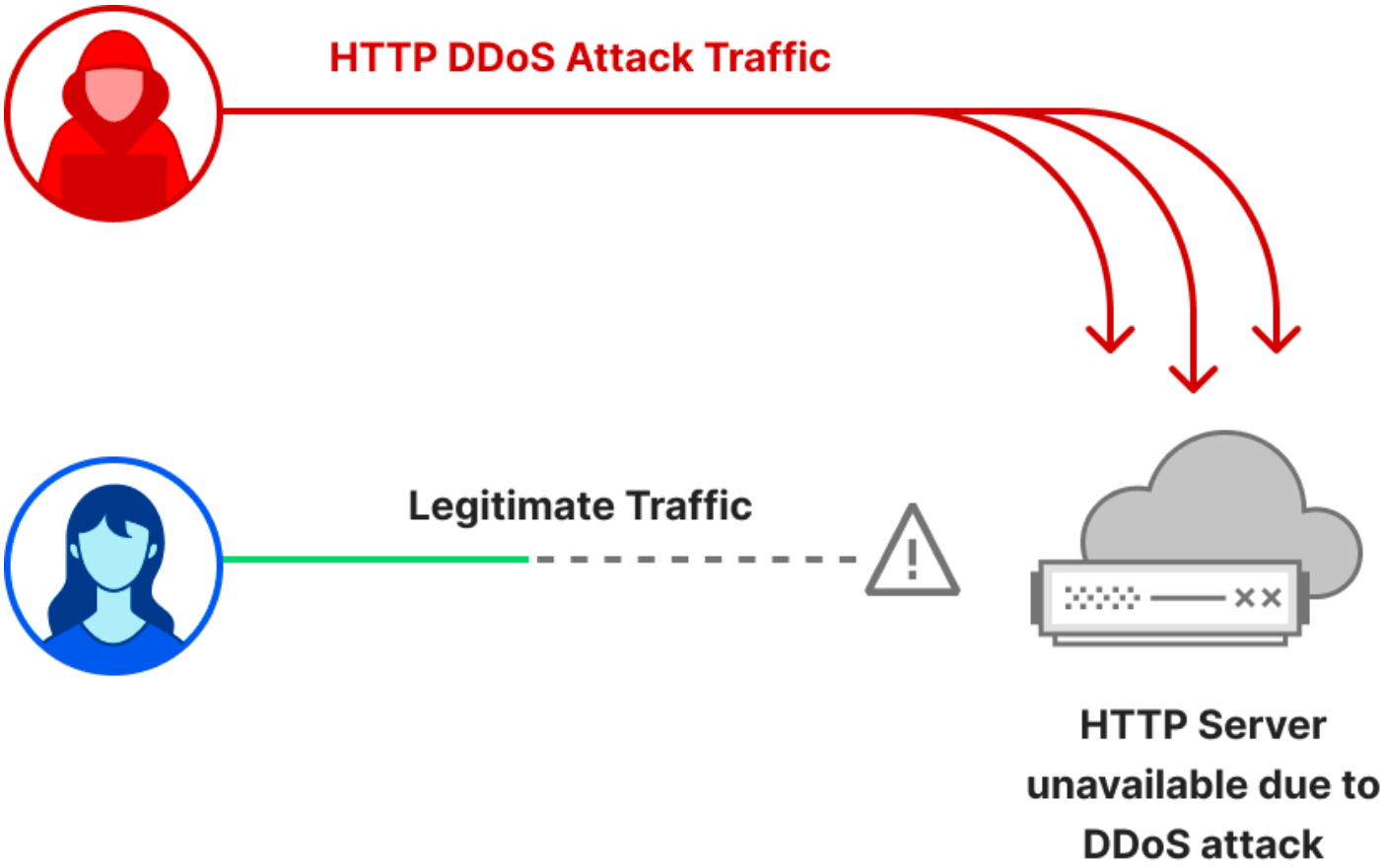
Distribution of Ransom DDoS attacks over 2021 and 2022 by quarter (each column represents the percentage of users reporting a ransom attack)

How we calculate Ransom DDoS attack trends

Cloudflare's systems constantly analyze traffic and automatically apply mitigation when DDoS attacks are detected. Each DDoS'd customer is prompted with an automated survey to help us better understand the nature of the attack and the success of the mitigation. For over two years, Cloudflare has been surveying attacked customers. One of the questions in the survey asks the respondents if they received a threat or a ransom note. Over the past two years, on average, we collected 187 responses per quarter. The responses of this survey are used to calculate the percentage of Ransom DDoS attacks.

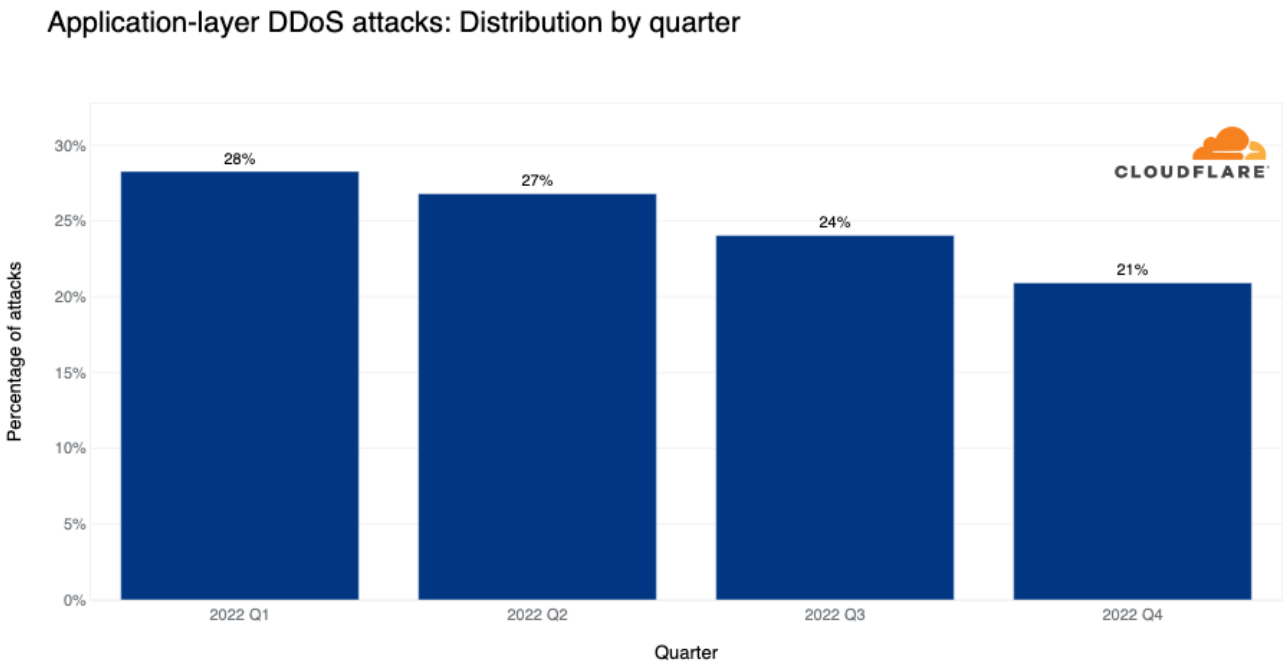
Application-layer DDoS attack landscape

Application-layer DDoS attacks, specifically HTTP/S DDoS attacks, are cyber attacks that usually aim to disrupt web servers by making them unable to process legitimate user requests. If a server is bombarded with more requests than it can process, the server will drop legitimate requests and - in some cases - crash, resulting in degraded performance or an outage for legitimate users.



Application-layer DDoS attack trends

When we look at the graph below, we can see a clear downward trend in attacks each quarter this year. However, despite the downward trend, HTTP DDoS attacks still increased by 79% when compared to the same quarter of previous year.

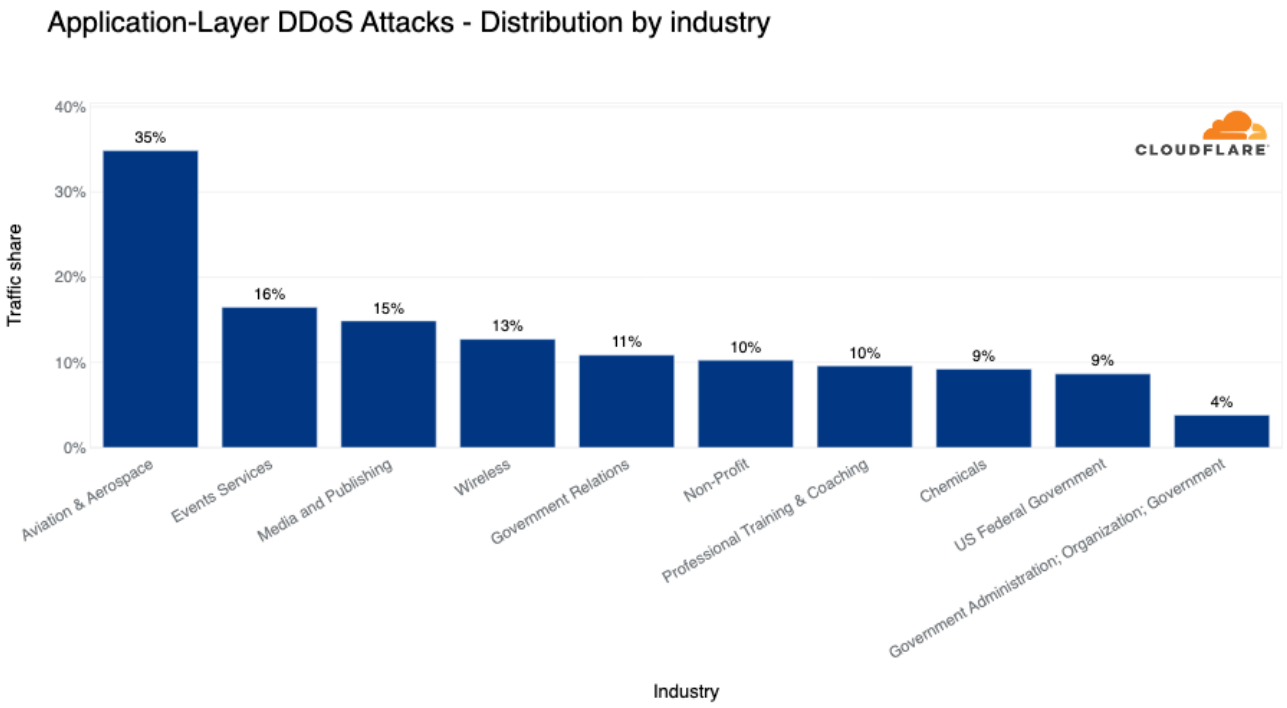


Distribution of HTTP DDoS attacks over the last year by quarter

Target industries of application-layer DDoS attacks

In the quarter where many people travel for the holidays, the Aviation and Aerospace was the most attacked industry. Approximately 35% of traffic to the industry was part of HTTP DDoS attacks. In second place, the Events Services industry saw over 16% of its traffic as HTTP DDoS attacks.

In the following places were the Media and Publishing, Wireless, Government Relations, and Non-profit industries. To learn more about how Cloudflare protects non-profit and human rights organizations, read our recent Impact Report.



Top industries targeted by HTTP DDoS attacks in 2022 Q4

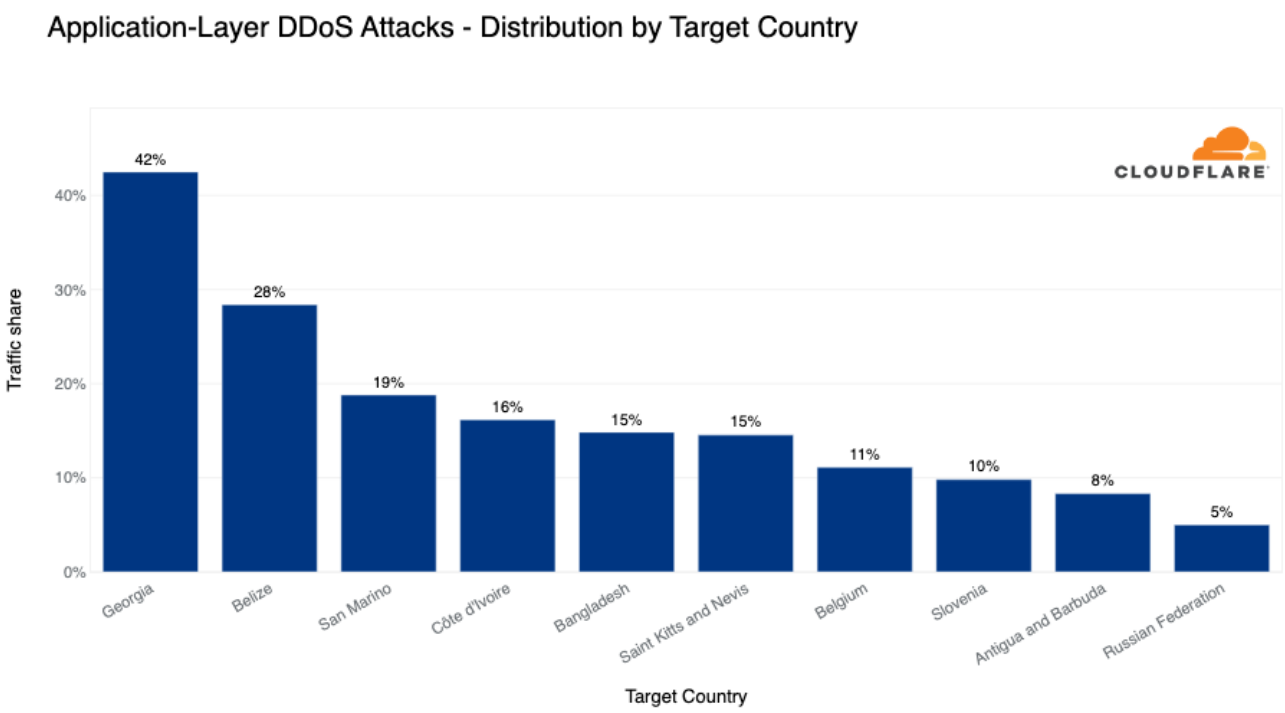
When we break it down regionally, and after excluding generic industry buckets like *Internet* and *Software,* we can see that in North America and Oceania the Telecommunications industry was the most targeted. In South America and Africa, the Hospitality industry was the most targeted. In Europe and Asia, Gaming & Gambling industries were the most targeted. And in the Middle East, the Education industry saw the most attacks.

Top industries targeted by HTTP DDoS attacks in 2022 Q4, by region

Target countries of application-layer DDoS attacks

Bucketing attacks by our customers' billing address helps us understand which countries are more frequently attacked. In Q4, over 42% of all traffic to Georgian HTTP applications behind Cloudflare was DDoS attack traffic.

In second place, Belize-based companies saw almost a third of their traffic as DDoS attacks, followed by San Marino in third with just below 20% of its traffic being DDoS attack traffic.

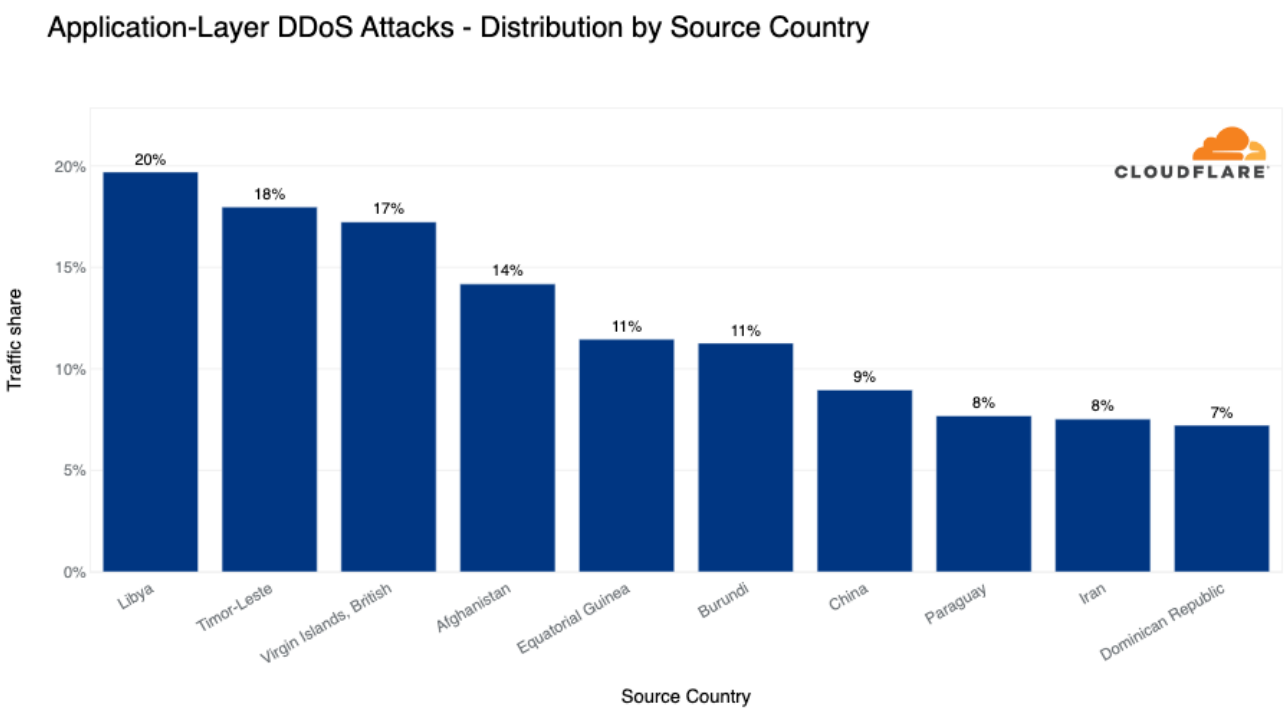


Top countries targeted by HTTP DDoS attacks in 2022 Q4

Source of application-layer DDoS attacks

Quick note before we dive in. If a country is found to be a major source of DDoS attacks, it doesn't necessarily mean that it is that country that launches the attacks. Most often with DDoS attacks, attackers are launching attacks remotely in an attempt to hide their true location. Top source countries are more often indicators that there are botnet nodes operating from within that country, perhaps hijacked servers or IoT devices.

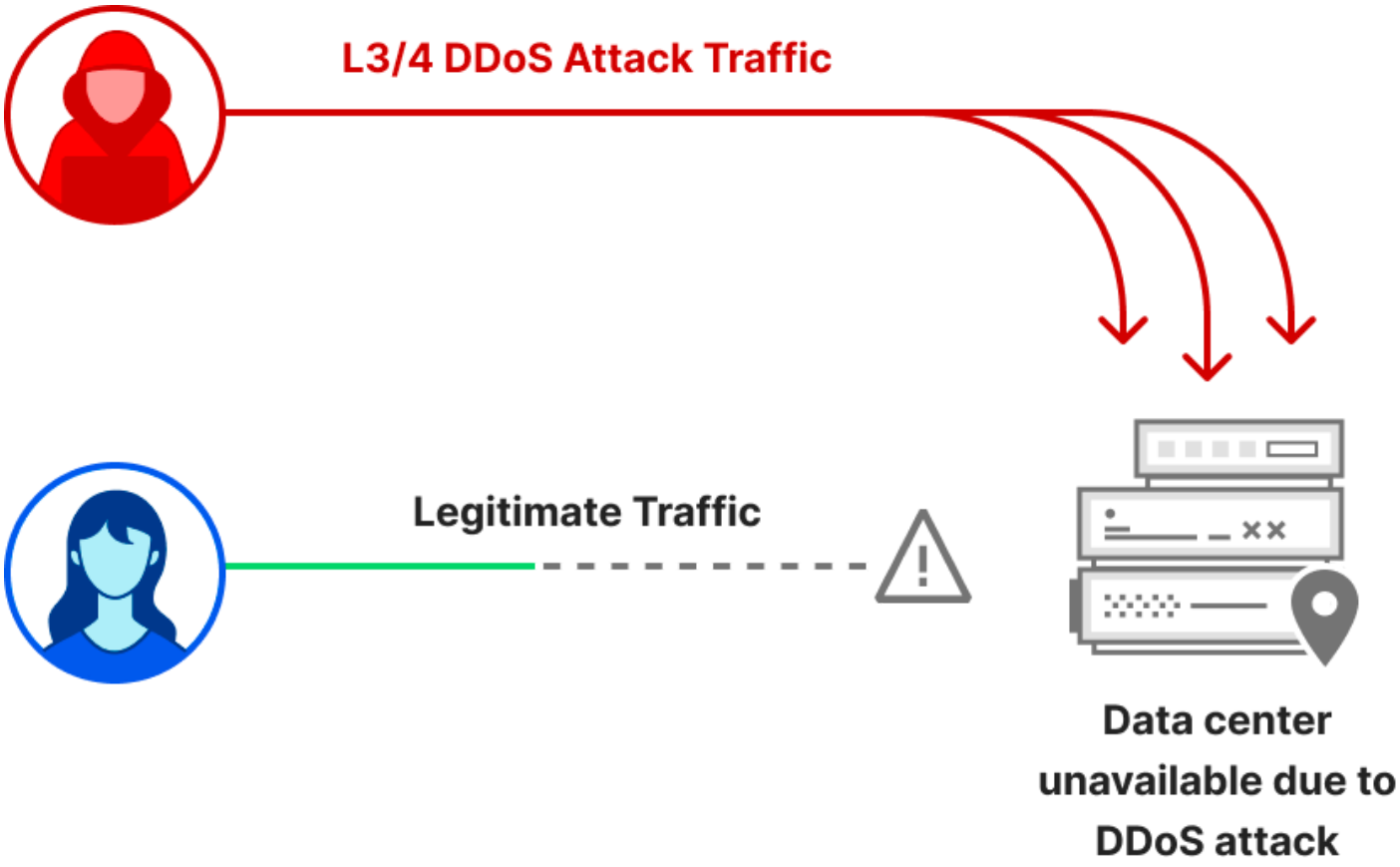
In Q4, almost 20% of all HTTP traffic originating from Libya was part of HTTP DDoS attacks. Similarly, 18% of traffic originating from Timor-Leste, an island country in Southeast Asia just north of Australia, was attack traffic. DDoS attack traffic also accounted for 17% of all traffic originating from the British Virgin Islands and 14% of all traffic originating from Afghanistan.



Top source countries of HTTP DDoS attacks in 2022 Q4

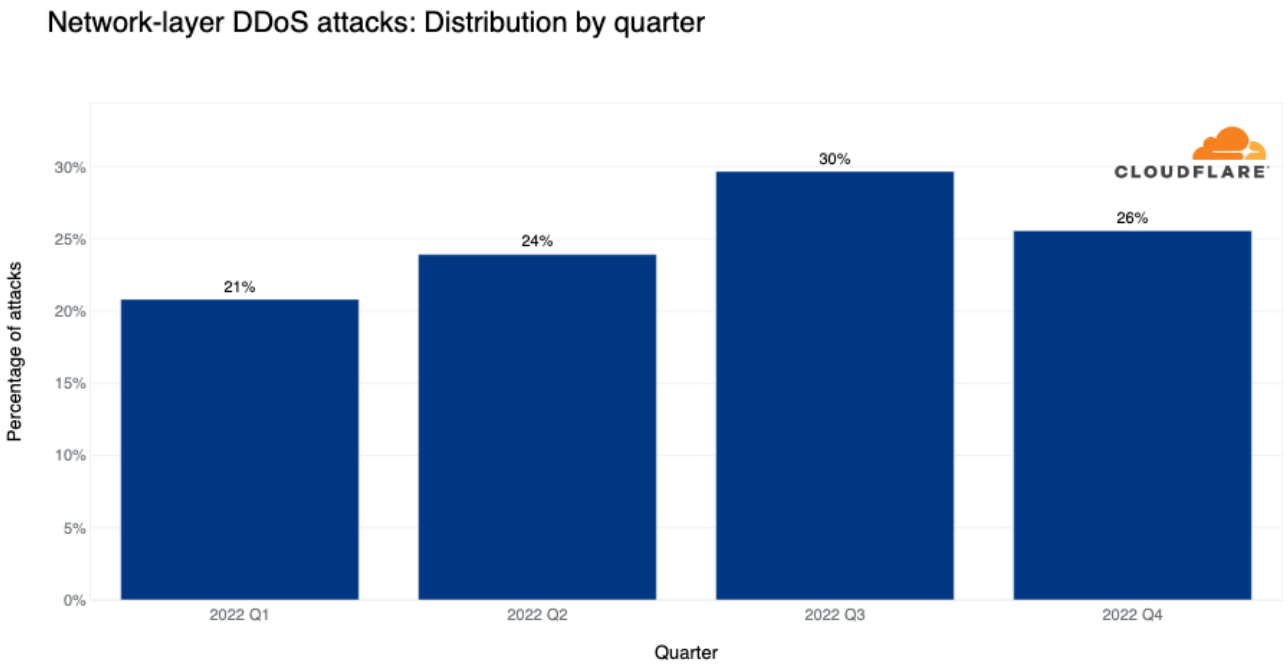
Network-layer DDoS attacks

While application-layer attacks target the application (Layer 7 of the OSI model) running the service that end users are trying to access (HTTP/S in our case), network-layer DDoS attacks aim to overwhelm network infrastructure, such as in-line routers and servers, and the Internet link itself.



Network-layer DDoS attack trends

After a year of steady increases in network-layer DDoS attacks, in the fourth and final quarter of the year, the amount of attacks actually decreased by 14% QoQ and 13% YoY.

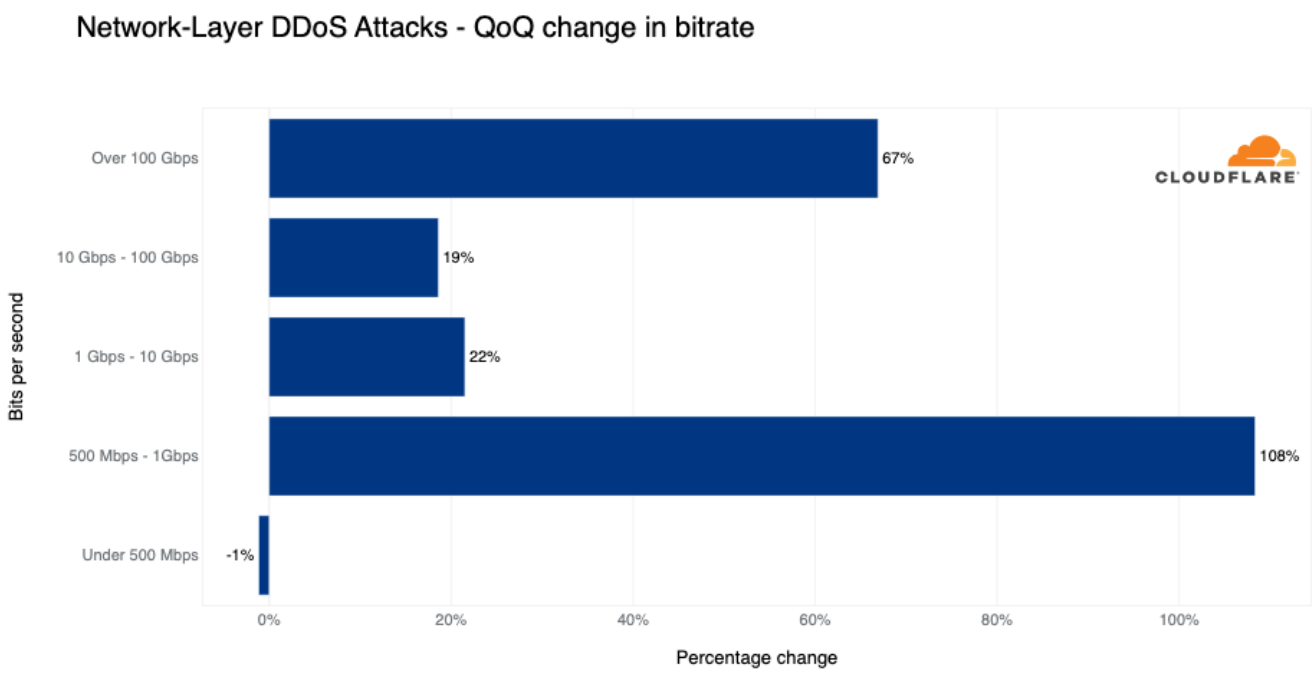


Distribution of Network-layer DDoS attacks over the last year by quarter

Now let's dive a little deeper to understand the various attack properties such as the attack volumetric rates, durations, attack vectors, and emerging threats.

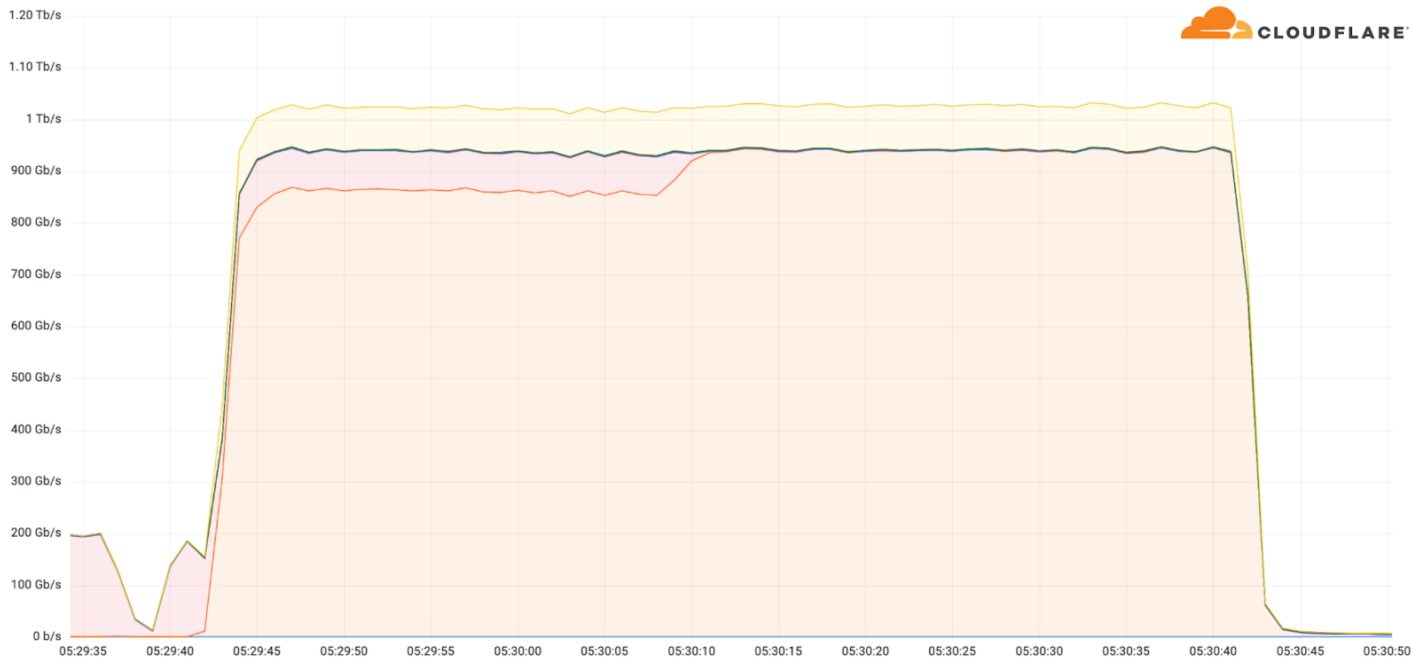
DDoS attack rate

While the vast majority of attacks are relatively short and small, we did see a spike in longer and larger attacks this quarter. The amount of volumetric network-layer DDoS attacks with a rate exceeding 100 Gbps increased by 67% QoQ. Similarly, attacks in the range of 1-100 Gbps increased by ~20% QoQ, and attacks in the range of 500 Mbps to 1 Gbps increased by 108% QoQ.



QoQ change in DDoS attack rates in 2022 Q4

Below is an example of one of those attacks exceeding 100 Gbps that took place the week after Thanksgiving. This was a 1 Tbps DDoS attack targeted at a Korean-based hosting provider. This particular attack was an ACK flood, and it lasted roughly one minute. Since the hosting provider was using Magic Transit, Cloudflare's L3 DDoS protection service, the attack was automatically detected and mitigated.

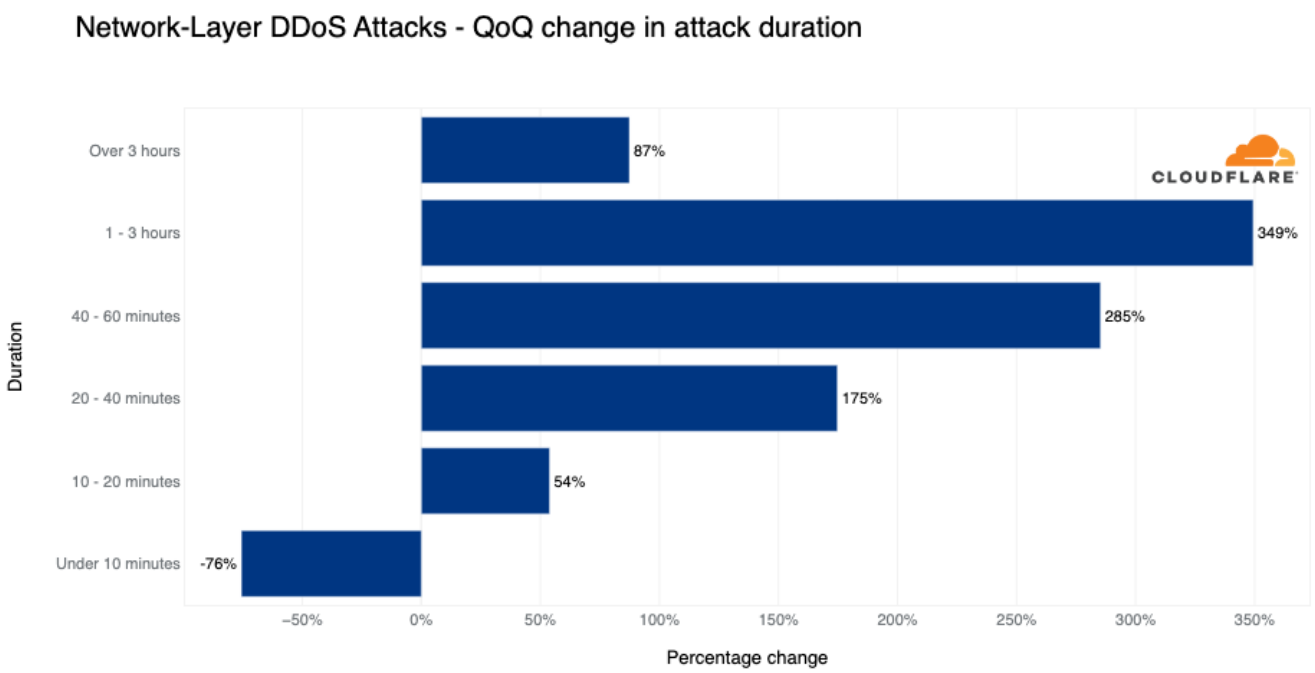


Graph of a 1 Tbps DDoS attack

While bit-intensive attacks usually aim to clog up the Internet connection to cause a denial of service event, packet-intensive attacks attempt to crash in-line devices. If an attack sends more packets than you can handle, the servers and other in-line appliances might not be able to process legitimate user traffic, or even crash altogether.

DDoS attack duration

In Q4, the amount of shorter attacks lasting less than 10 minutes decreased by 76% QoQ, and the amount of longer attacks increased. Most notably, attacks lasting 1-3 hours increased by 349% QoQ and the amount of attacks lasting more than three hours increased by 87% QoQ. Most of the attacks, over 67% of them, lasted 10-20 minutes.

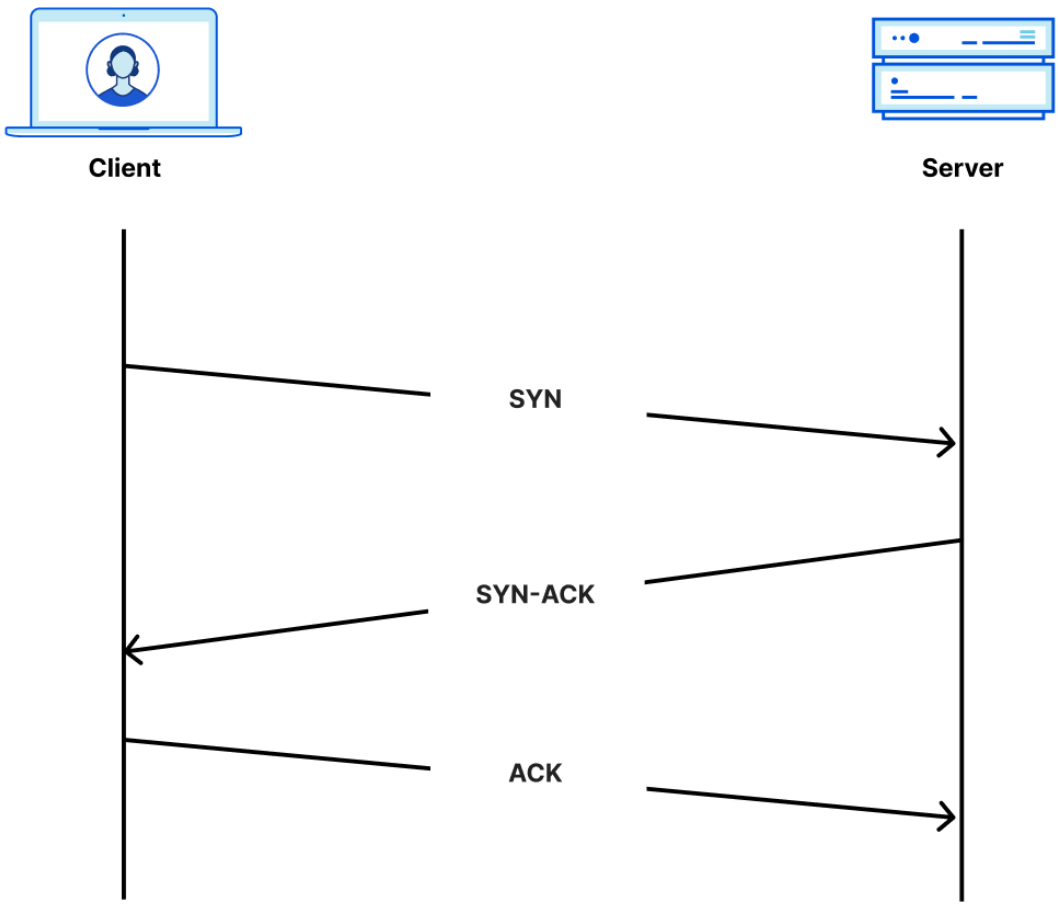


QoQ change in the duration of DDoS attacks in 2022 Q4

DDoS attack vectors

The attack vector is a term used to describe the attack method. In Q4, SYN floods remained the attacker's method of choice — in fact, almost half of all network-layer DDoS attacks were SYN floods.

As a recap, SYN floods are a flood of SYN packets (TCP packets with the *Synchronize* flag turned on, i.e., the bit set to 1). SYN floods take advantage of the statefulness of the Three-way TCP handshake — which is the way to establish a connection between a server and a client.

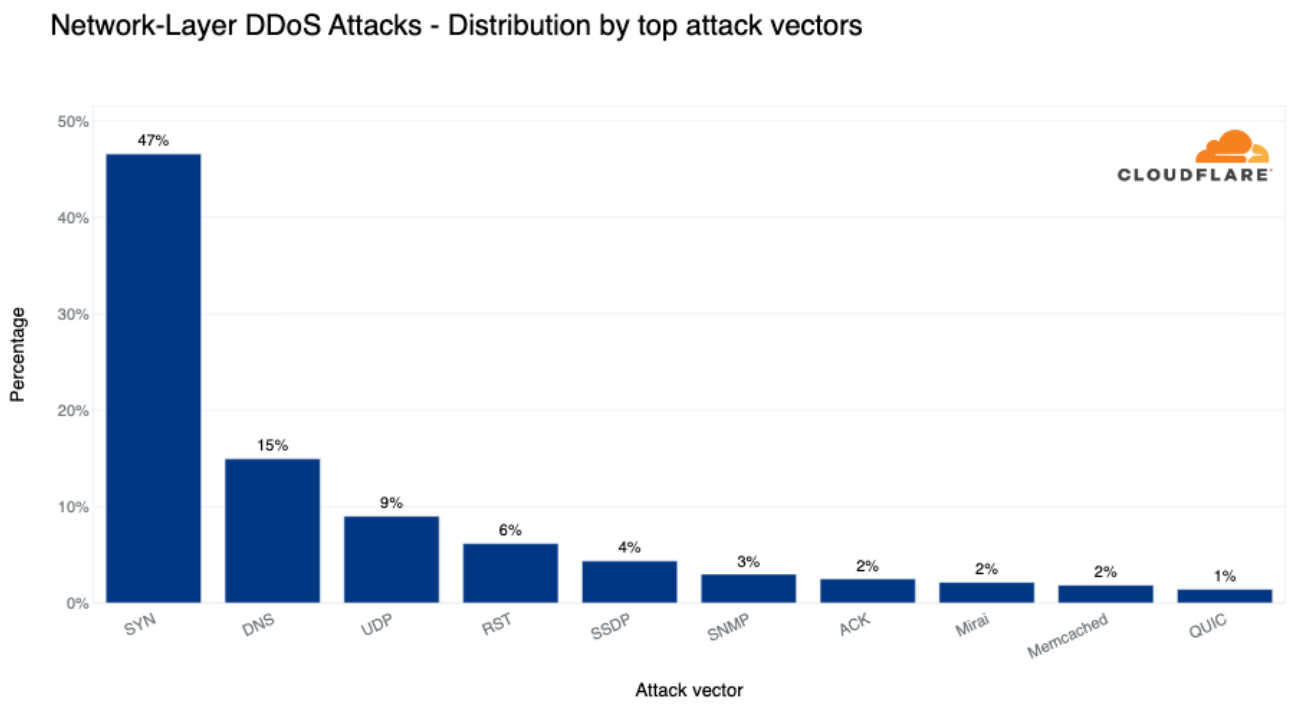


The Three-way TCP Handshake

The client starts off by sending a SYN packet, the server responds with a Synchronize-acknowledgement (SYN/ACK) packet and waits for the client's Acknowledgement (ACK) packet. For every connection, a certain amount of memory is allocated. In the SYN flood, the source IP addresses may be spoofed (altered) by the attacker, causing the server to respond with the SYN/ACK packets to the spoofed IP addresses — which most likely ignore the packet. The server then naively waits for the never arriving ACK packets to complete the handshake. After a while, the server times out and releases those resources. However, given a sufficient amount of SYN packets in a short amount of time,

they may be enough to drain the server's resources and render it unable to handle legitimate user connections or even crash altogether.

After SYN floods, with a massive drop in share, DNS floods and amplification attacks came in second place, accounting for ~15% of all network-layer DDoS attacks. And in third UDP-based DDoS attacks and floods with a 9% share.



Top attack vectors in 2022 Q4

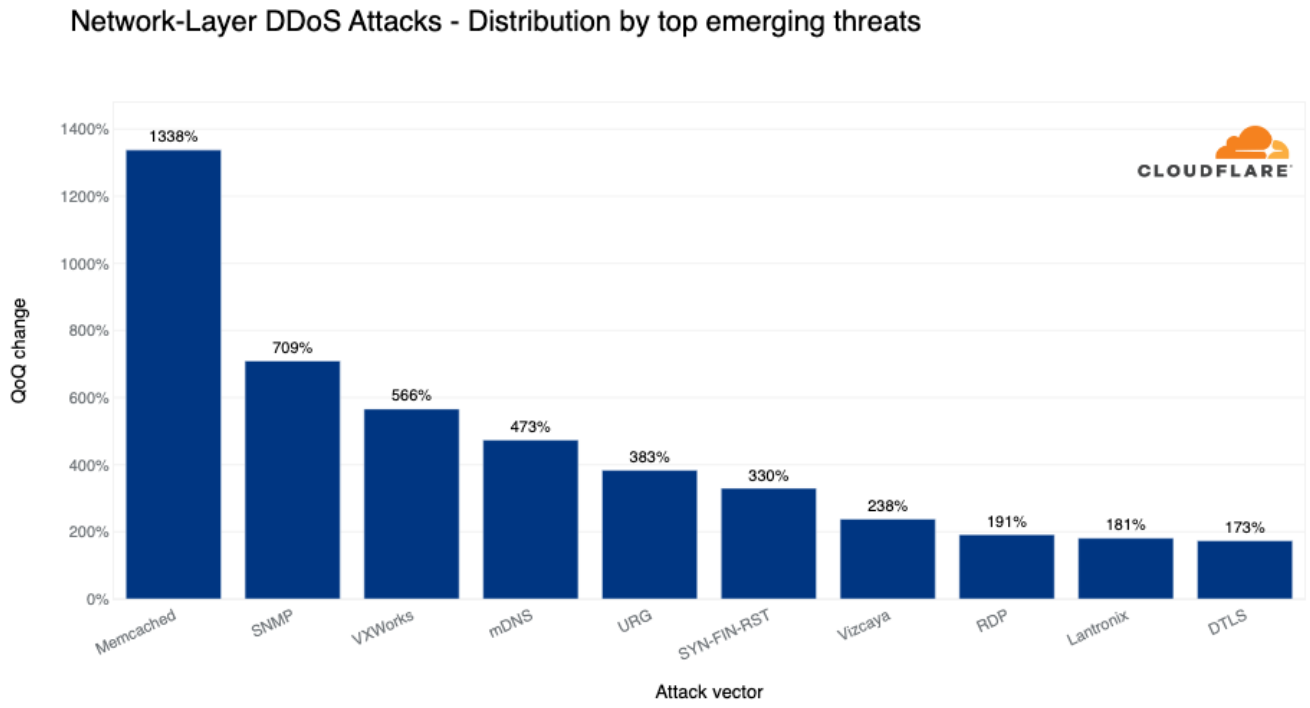
Emerging DDoS threats

In Q4, Memcached-based DDoS attacks saw the highest growth — a 1,338% increase QoQ. Memcached is a database caching system for speeding up websites and networks. Memcached servers that support UDP can be abused to launch amplification/reflection DDoS attacks. In this case, the attacker would request content from the caching system and spoof the victim's IP address as the source IP in the UDP packets. The victim will be flooded with the Memcache responses which can be amplified by a factor of up to 51,200x.

In second place, SNMP-based DDoS attacks increased by 709% QoQ. Simple Network Management Protocol (SNMP) is a UDP-based protocol that is often

used to discover and manage network devices such as printers, switches, routers, and firewalls of a home or enterprise network on UDP well-known port 161. In an SNMP reflection attack, the attacker sends out numerous SNMP queries while spoofing the source IP address in the packet as the targets to devices on the network that, in turn, reply to that target's address. Numerous responses from the devices on the network results in the target network being DDoSed.

In third place, VxWorks-based DDoS attacks increased by 566% QoQ. VxWorks is a real-time operating system (RTOS) often used in embedded systems such as Internet of Things (IoT) devices. It also is used in networking and security devices, such as switches, routers, and firewalls. By default, it has a debug service enabled which not only allows anyone to do pretty much anything to those systems, but it can also be used for DDoS amplification attacks. This exploit (CVE-2010-2965) was exposed as early as 2010 and as we can see it is still being used in the wild to generate DDoS attacks.

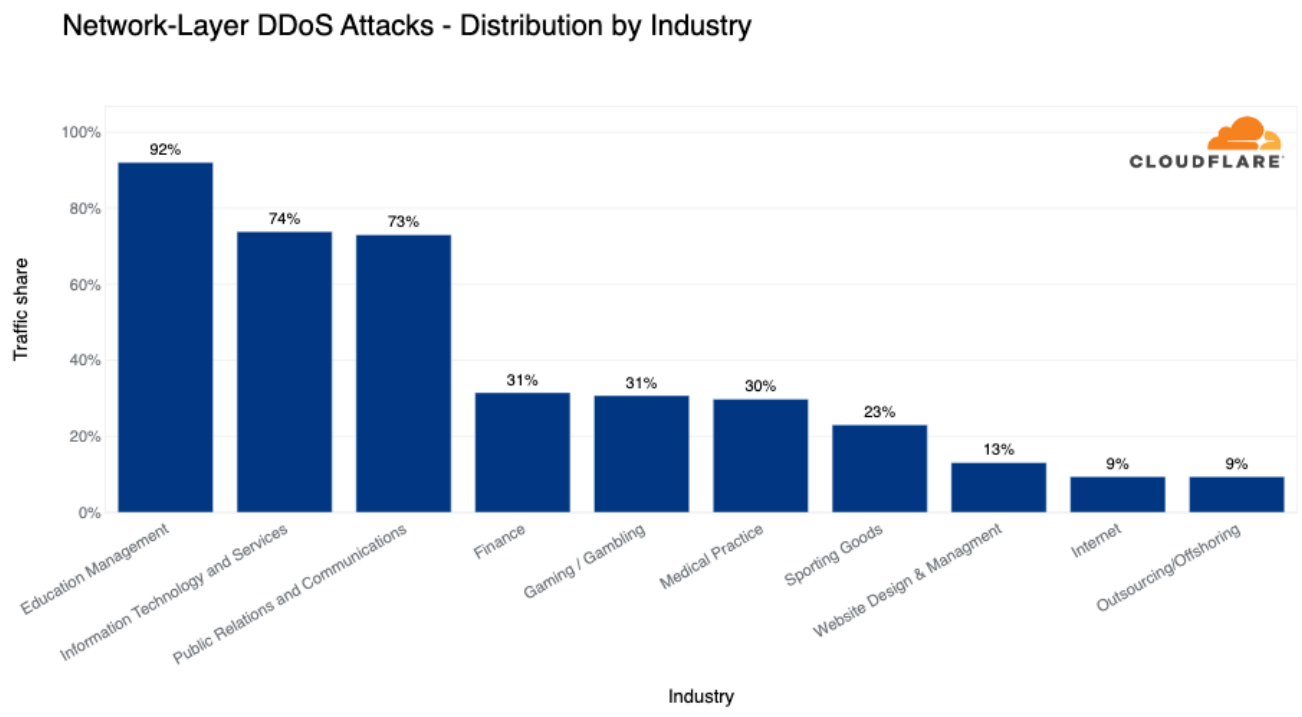


Top emerging threats in 2022 Q4

Target industries of network-layer DDoS attacks

In Q4, the Education Management industry saw the highest percentage of network-layer DDoS attack traffic — 92% of all traffic routed to the industry was network-layer DDoS attack traffic.

Not too far behind, in the second and third places, the Information Technology and Services alongside the Public Relations and Communications industries also saw a significant amount of network-layer DDoS attack traffic (~73%). With a high margin, the Finance, Gaming / Gambling, and Medical Practice industries came in next with approximately a third of their traffic flagged as attack traffic.



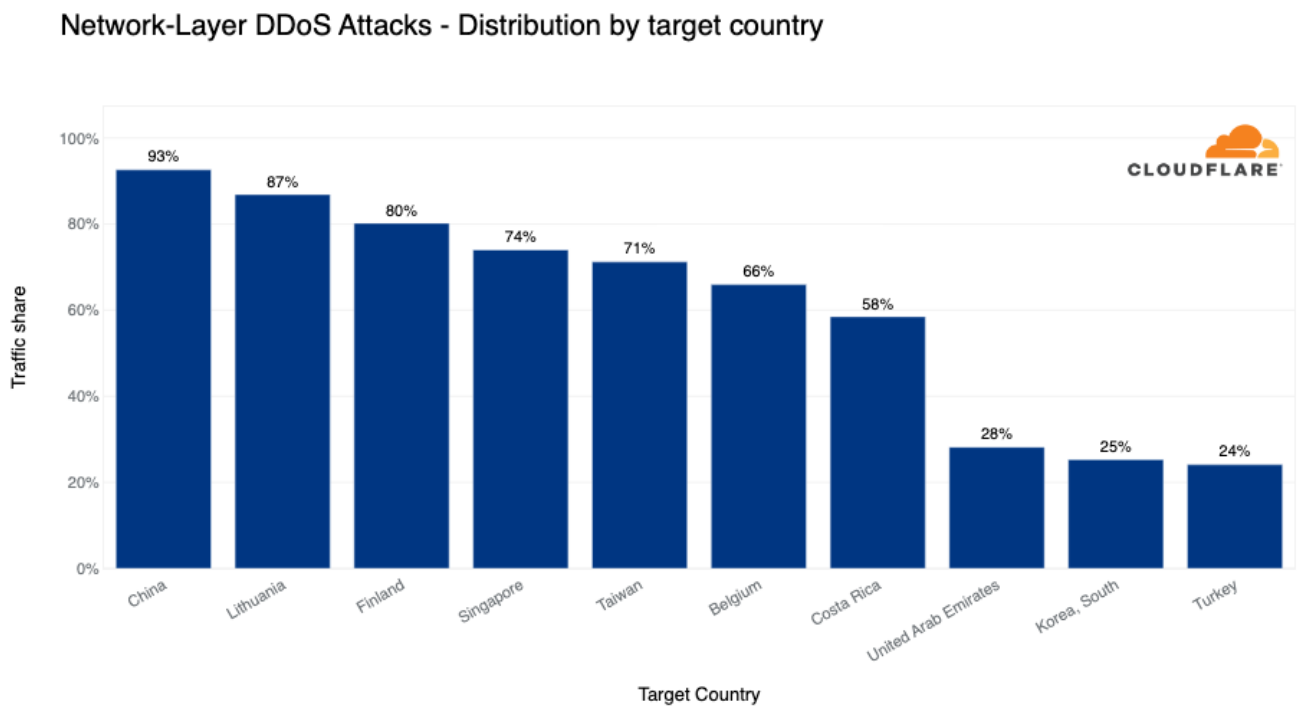
Top industries targeted by network-layer DDoS attacks in 2022 Q4

Target countries of network-layer DDoS attacks

Grouping attacks by our customers' billing country lets us understand which countries are subject to more attacks. In Q4, a staggering 93% of traffic to

Chinese Internet properties behind Cloudflare was network-layer DDoS attack traffic.

In second place, Lithuanian Internet properties behind Cloudflare saw 87% of their traffic belonging to network-layer DDoS attack traffic. Following were Finland, Singapore, and Taiwan with the highest percentage of attack traffic.

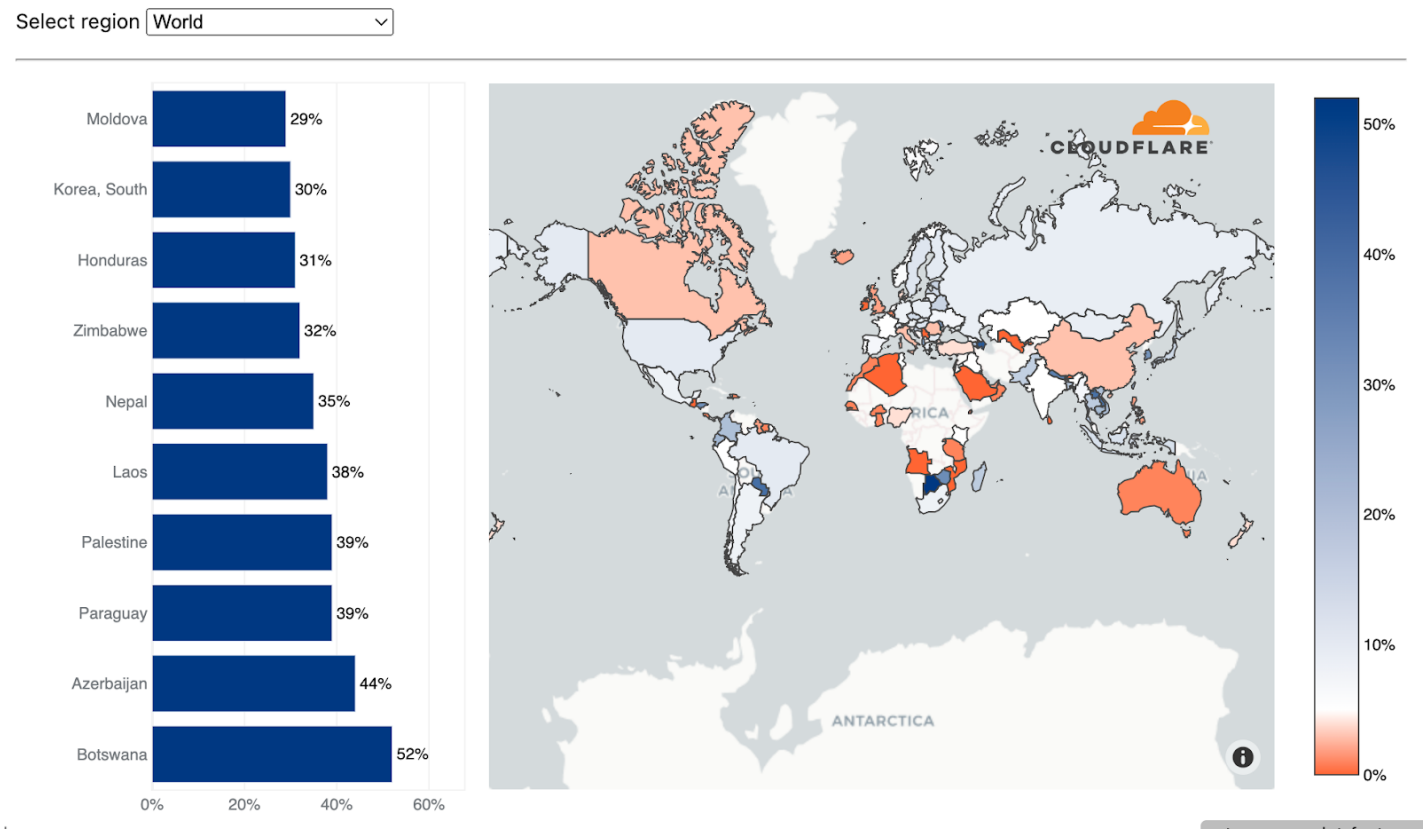


Top countries targeted by network-layer DDoS attacks in 2022 Q4

Source of network-layer DDoS attacks

In the application-layer, we used the attacking IP addresses to understand the origin country of the attacks. That is because at that layer, IP addresses cannot be spoofed (i.e., altered). However, in the network layer, source IP addresses *can* be spoofed. So, instead of relying on IP addresses to understand the source, we instead use the location of our data centers where the attack packets were ingested. We're able to get geographical accuracy due to our large global coverage in over 275+ locations around the world.

In Q4, over 52% of the traffic we ingested in our Botswana-based data center was attack traffic. Not too far behind, over 43% of traffic in Azerbaijan was attack traffic, followed by Paraguay, Palestine, Laos, and Nepal.



Top Cloudflare data center locations with the highest percentage of DDoS attack traffic in 2022 Q4

Please note: Internet Service Providers may sometimes route traffic differently which may skew results. For example, traffic from China may be hauled through California due to various operational considerations.

Understanding the DDoS threat landscape

This quarter, longer and larger attacks became more frequent. Attack durations increased across the board, volumetric attacks surged, and Ransom DDoS attacks continued to rise. During the 2022 holiday season, the top targeted industries for DDoS attacks at the application-layer were Aviation/Aerospace and Events Services. Network-layer DDoS attacks targeted Gaming/Gambling, Finance, and Education Management companies. We also saw a shift in the top

emerging threats, with Memcached-based DDoS attacks continuing to increase in prevalence.

Defending against DDoS attacks is critical for organizations of all sizes. While attacks may be initiated by humans, they are executed by bots — and to play to win, you must fight bots with bots. Detection and mitigation must be automated as much as possible, because relying solely on humans puts defenders at a disadvantage. Cloudflare's automated systems constantly detect and mitigate DDoS attacks for our customers, so they don't have to.

Over the years, it has become easier, cheaper, and more accessible for attackers and attackers-for-hire to launch DDoS attacks. But as easy as it has become for the attackers, we want to make sure that it is even easier - and free - for defenders of organizations of all sizes to protect themselves against DDoS attacks of all types. We've been providing unmetered and unlimited DDoS protection for free to all of our customers since 2017 — when we pioneered the concept. Cloudflare's mission is to help build a better Internet. A better Internet is one that is more secure, faster, and reliable for everyone - even in the face of DDoS attacks.

Sign up to the DDoS Trends Webinar to learn more about the emerging threats and how to defend against them.

We protect entire corporate networks, help customers build Internet-scale applications efficiently, accelerate any website or Internet application, ward off DDoS attacks, keep 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.

DDoS | Cloudflare Radar | DDoS Reports | Insights | Trends