DDoS Attack Trends for 2022 Q1

04/12/2022

Omer Yoachimik

15 min read

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

Welcome to our first DDoS report of 2022, and the ninth in total so far. This report includes new data points and insights both in the application-layer and network-layer sections — as observed across the global Cloudflare network between January and March 2022.

The first quarter of 2022 saw a massive spike in application-layer DDoS attacks, but a decrease in the total number of network-layer DDoS attacks. Despite the decrease, we've seen volumetric DDoS attacks surge by up to 645% QoQ, and

we mitigated a new zero-day reflection attack with an amplification factor of 220 billion percent.

In the Russian and Ukrainian cyberspace, the most targeted industries were Online Media and Broadcast Media. In our Azerbaijan and Palestinian Cloudflare data centers, we've seen enormous spikes in DDoS activity — indicating the presence of botnets operating from within.

The Highlights

The Russian and Ukrainian cyberspace

- Russian Online Media companies were the most targeted industries within Russia in Q1. The next most targeted was the Internet industry, then Cryptocurrency, and then Retail. While many attacks that targeted Russian Cryptocurrency companies originated in Ukraine or the US, another major source of attacks was from within Russia itself.
- The majority of HTTP DDoS attacks that targeted Russian companies originated from Germany, the US, Singapore, Finland, India, the Netherlands, and Ukraine. It's important to note that being able to identify where cyber attack traffic originates is not the same as being able to attribute where the attacker is located.
- Attacks on Ukraine targeted Broadcast Media and Publishing websites and seem to have been more distributed, originating from more countries — which may indicate the use of global botnets. Still, most of the attack traffic originated from the US, Russia, Germany, China, the UK, and Thailand.

Read more about what Cloudflare is doing to keep the Open Internet flowing into Russia and keep attacks from getting out.

Ransom DDoS attacks

- In January 2022, over 17% of under-attack respondents reported being targeted by ransom DDoS attacks or receiving a threat in advance.
- That figure drastically dropped to 6% in February, and then to 3% in March.
- When compared to previous quarters, we can see that in total, in Q1, only 10% of respondents reported a ransom DDoS attack; a 28% decrease YoY and 52% decrease QoQ.

Application-layer DDoS attacks

- 2022 Q1 was the busiest quarter in the past 12 months for application-layer attacks. HTTP-layer DDoS attacks increased by 164% YoY and 135% QoQ.
- Diving deeper into the quarter, in March 2022 there were more HTTP DDoS attacks than in all of Q4 combined (and Q3, and Q1).
- After four consecutive quarters in a row with China as the top source of HTTP DDoS attacks, the US stepped into the lead this quarter. HTTP DDoS attacks originating from the US increased by a staggering 6,777% QoQ and 2,225% YoY.

Network-layer DDoS attacks

- Network-layer attacks in Q1 increased by 71% YoY but decreased 58% QoQ.
- The Telecommunications industry was the most targeted by network-layer DDoS attacks, followed by Gaming and Gambling companies, and the Information Technology and Services industry.
- Volumetric attacks increased in Q1. Attacks above 10 Mpps (million packets per second) grew by over 300% QoQ, and attacks over 100 Gbps grew by 645% QoQ.

This report is based on DDoS attacks that were automatically detected and mitigated by Cloudflare's DDoS Protection systems. To learn more about how it works, check out this deep-dive blog post.

A note on how we measure DDoS attacks observed over our network
To analyze attack trends, we calculate the "DDoS activity" rate, which is either the percentage of attack traffic out of the total traffic (attack + clean) observed over our global network, or in a specific location, or in a specific category (e.g., industry or billing country). Measuring the percentages allows us to normalize data points and avoid biases reflected in absolute numbers towards, for example, a Cloudflare data center that receives more total traffic and likely, also more attacks.

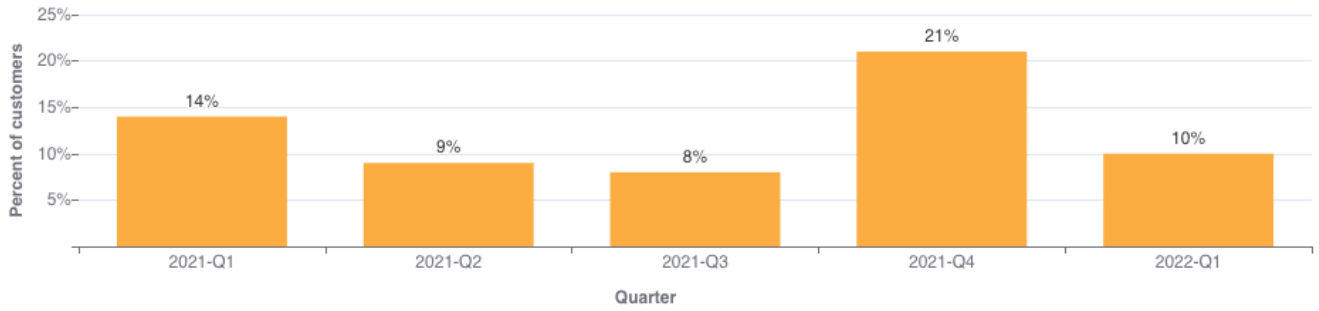
To view an interactive version of this report view it on Cloudflare Radar.

Ransom Attacks

Our 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 now, Cloudflare has been surveying attacked customers — one question on the survey being if they received a threat or a ransom note demanding payment in exchange to stop the DDoS attack. In the last quarter, 2021 Q4, we observed a record-breaking level of reported ransom DDoS attacks (one out of every five customers). This quarter, we've witnessed a drop in ransom DDoS attacks with only one out of 10 respondents reporting a ransom DDoS attack; a 28% decrease YoY and 52% decrease QoQ.

Ransom DDoS Attacks & Threats by Quarter

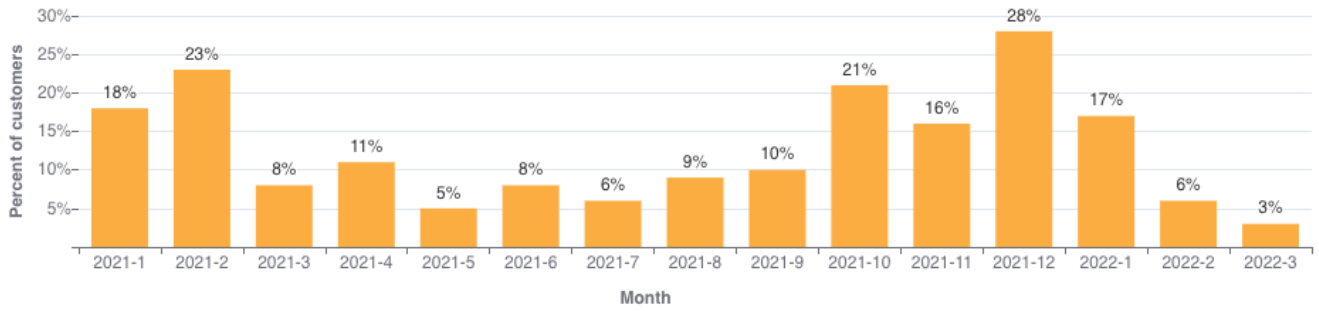


CLOUDFLARE

Source: https://radar.cloudflare.com/notebooks/ddos-2022-q1

When we break it down by month, we can see that January 2022 saw the largest number of respondents reporting receiving a ransom letter in Q1. Almost one out of every five customers (17%).

Ransom DDoS Attacks & Threats by Month

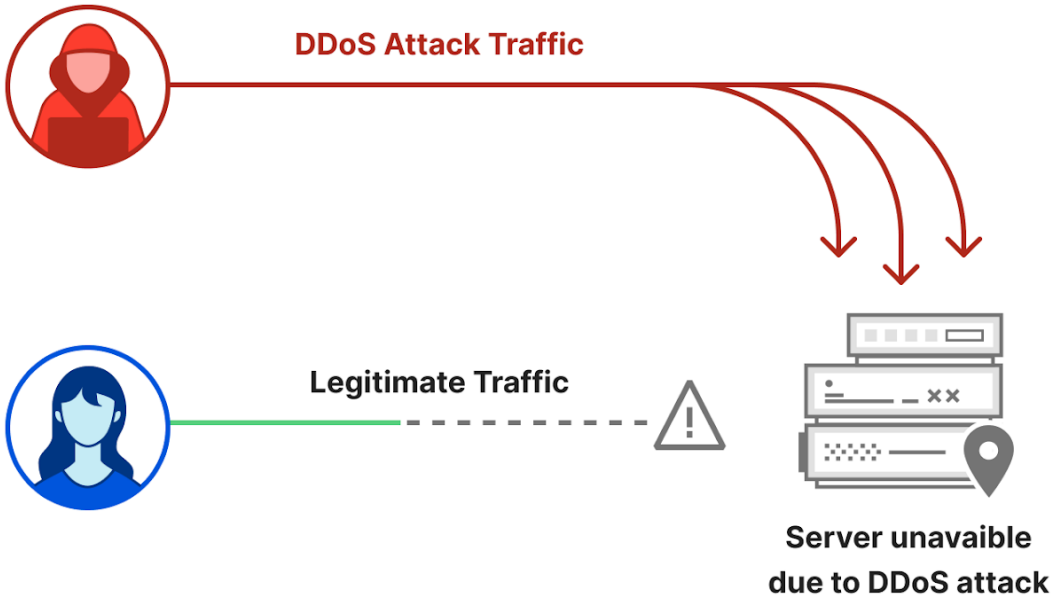


CLOUDFLARE

Source: https://radar.cloudflare.com/notebooks/ddos-2022-q1

Application-layer DDoS attacks

Application-layer DDoS attacks, specifically HTTP DDoS attacks, are attacks that usually aim to disrupt a web server by making it 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.

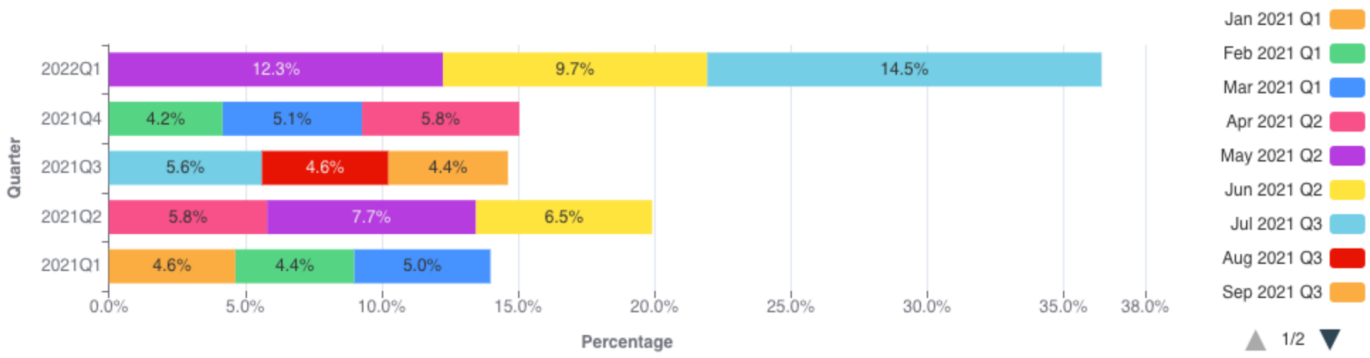


Application-layer DDoS attacks by month

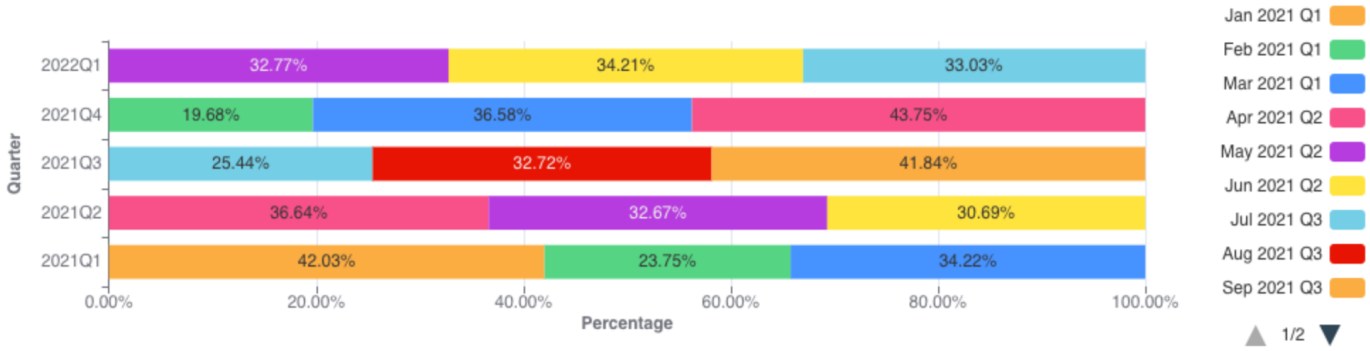
In Q1, application-layer DDoS attacks soared by 164% YoY and 135% QoQ - the busiest quarter within the past year.

Application-layer DDoS attacks increased to new heights in the first quarter of 2022. In March alone, there were more HTTP DDoS attacks than in all of 2021 Q4 combined (and Q3, and Q1).

Application-Layer DDoS Attacks - Yearly distribution by month



Network-Layer DDoS Attacks - Quarterly distribution by month



CLOUDFLARE

Source: https://radar.cloudflare.com/notebooks/ddos-2022-q1

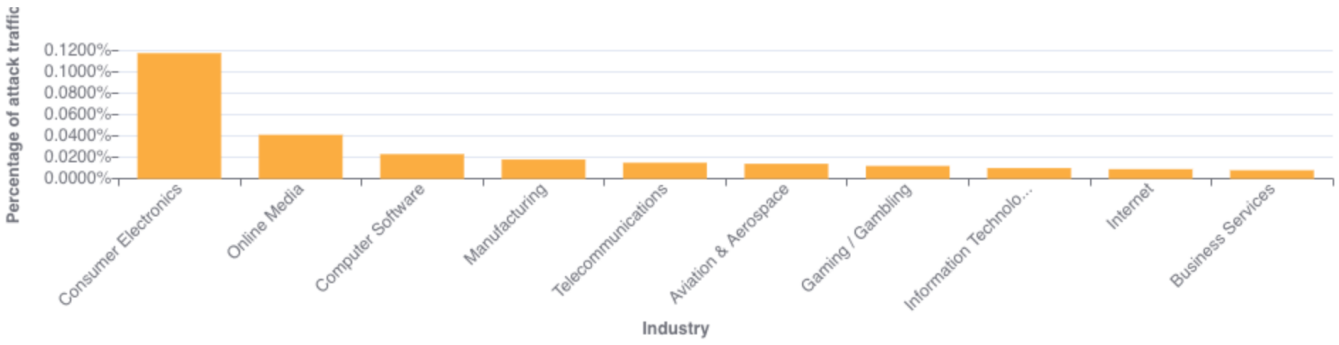
Application-layer DDoS attacks by industry

Consumer Electronics was the most targeted industry in Q1.

Globally, the Consumer Electronics industry was the most attacked with an increase of 5,086% QoQ. Second was the Online Media industry with a 2,131%

increase in attacks QoQ. Third were Computer Software companies, with an increase of 76% QoQ and 1,472 YoY.

Application-Layer DDoS Attacks - Distribution by industry

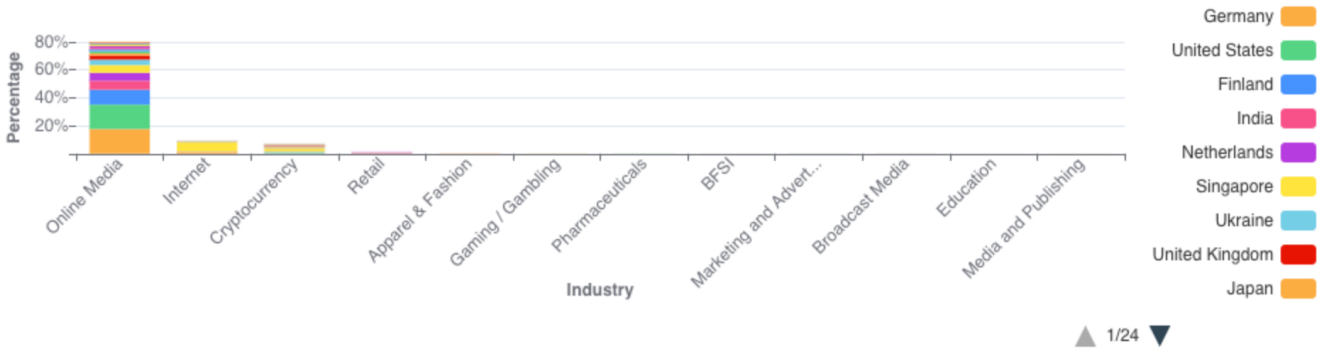


CLOUDFLARE

Source: https://radar.cloudflare.com/notebooks/ddos-2022-q1

However, if we focus only on Ukraine and Russia, we can see that Broadcast Media, Online Media companies, and Internet companies were the most targeted. Read more about what Cloudflare is doing to keep the Open Internet flowing into Russia and keep attacks from getting out.

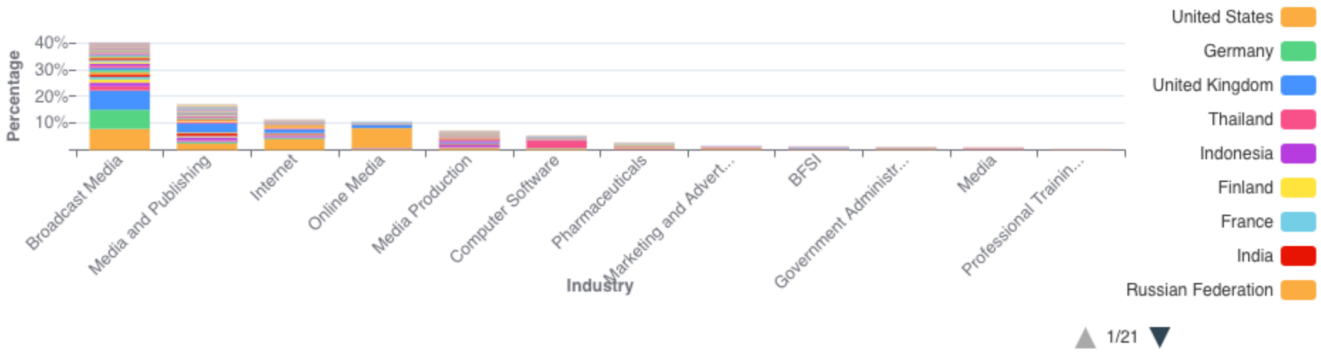
Application-Layer DDoS Attacks on Russia by Industry and Source Country



CLOUDFLARE

Source: https://radar.cloudflare.com/notebooks/ddos-2022-q1

Application-Layer DDoS Attacks on Ukraine by Industry and Source Country



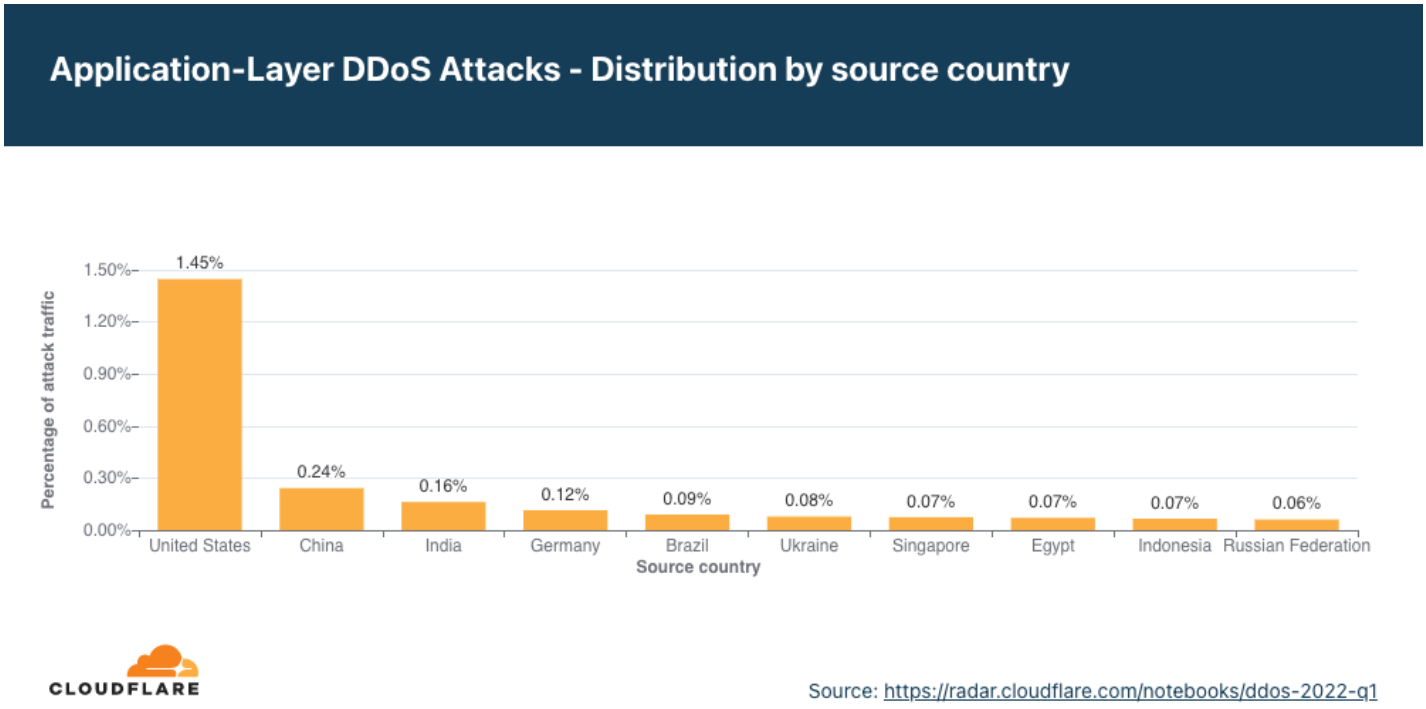
CLOUDFLARE

Source: https://radar.cloudflare.com/notebooks/ddos-2022-q1

Application-layer DDoS attacks by source country

To understand the origin of the HTTP attacks, we look at the geolocation of the source IP address belonging to the client that generated the attack HTTP requests. Unlike network-layer attacks, source IP addresses cannot be spoofed in HTTP attacks. A high percentage of DDoS activity in a given country usually indicates the presence of botnets operating from within the country's borders.

After four consecutive quarters in a row with China as the top source of HTTP DDoS attacks, the US stepped into the lead this quarter. HTTP DDoS attacks originating from the US increased by a staggering 6,777% QoQ and 2,225% YoY. Following China in second place are India, Germany, Brazil, and Ukraine.

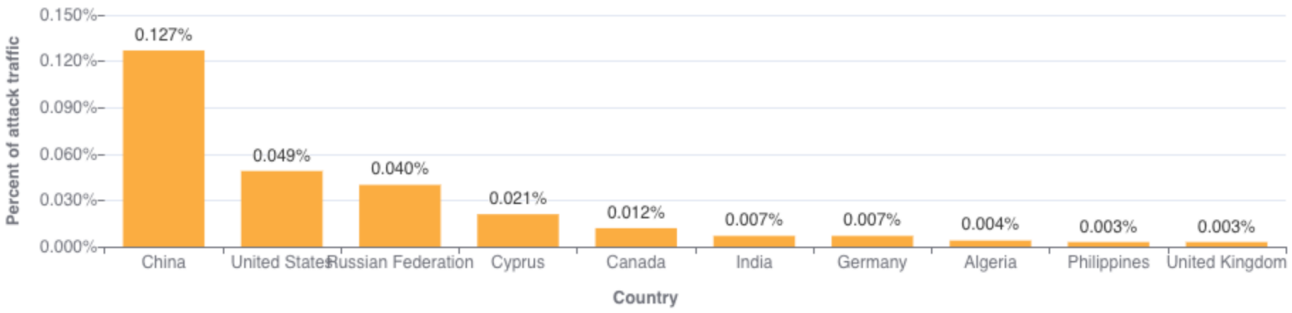


Application-layer DDoS attacks by target country

In order to identify which countries are targeted by the most HTTP DDoS attacks, we bucket the DDoS attacks by our customers' billing countries and represent it as a percentage out of all DDoS attacks.

The US drops to second place, after being first for three consecutive quarters. Organizations in China were targeted the most by HTTP DDoS attacks, followed by the US, Russia, and Cyprus.

Application-Layer DDoS Attacks - Distribution by target country

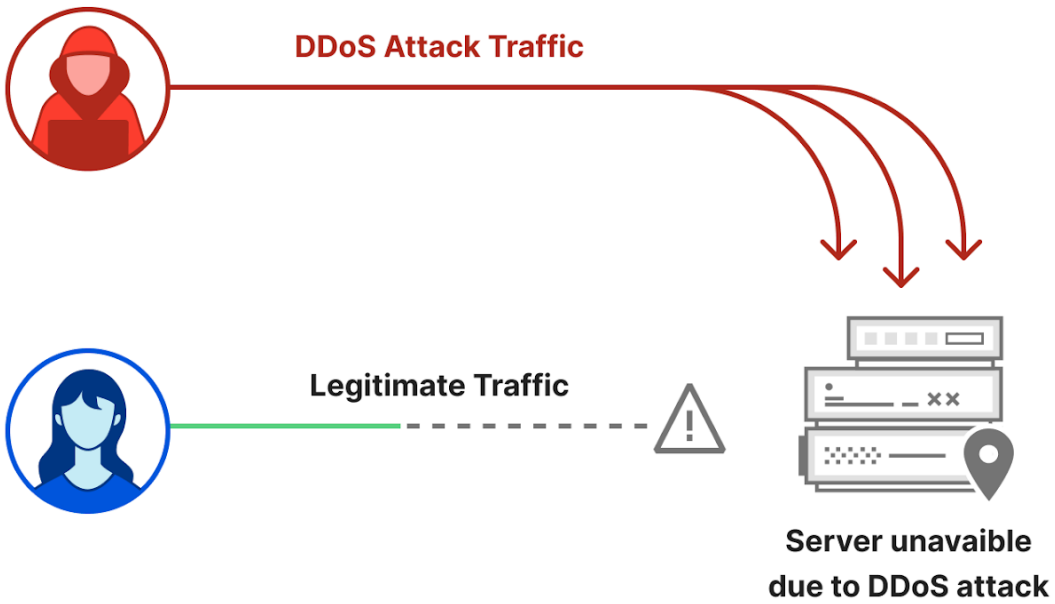


CLOUDFLARE

Source: https://radar.cloudflare.com/notebooks/ddos-2022-q1

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 attacks aim to overwhelm network infrastructure (such as in-line routers and servers) and the Internet link itself.

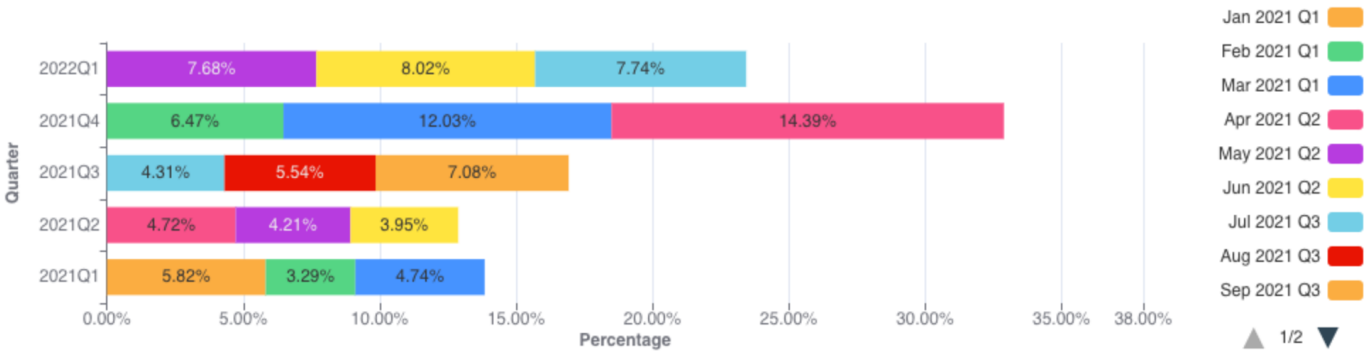


Network-layer DDoS attacks by month

While HTTP DDoS attacks soared in Q1, network-layer DDoS attacks actually decreased by 58% QoQ, but still increased by 71% YoY.

Diving deeper into Q1, we can see that the amount of network-layer DDoS attacks remained mostly consistent throughout the quarter with about a third of attacks occurring every month.

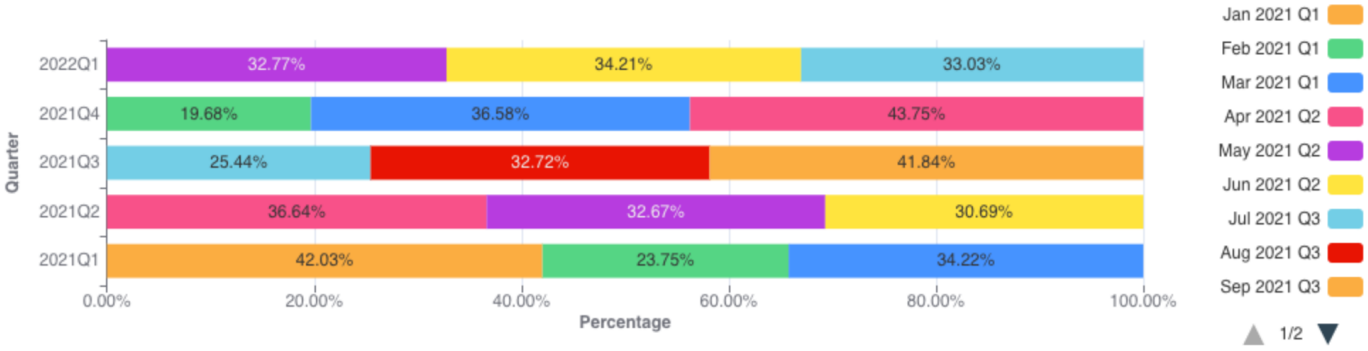
Network-Layer DDoS Attacks - Yearly distribution by month



CLOUDFLARE

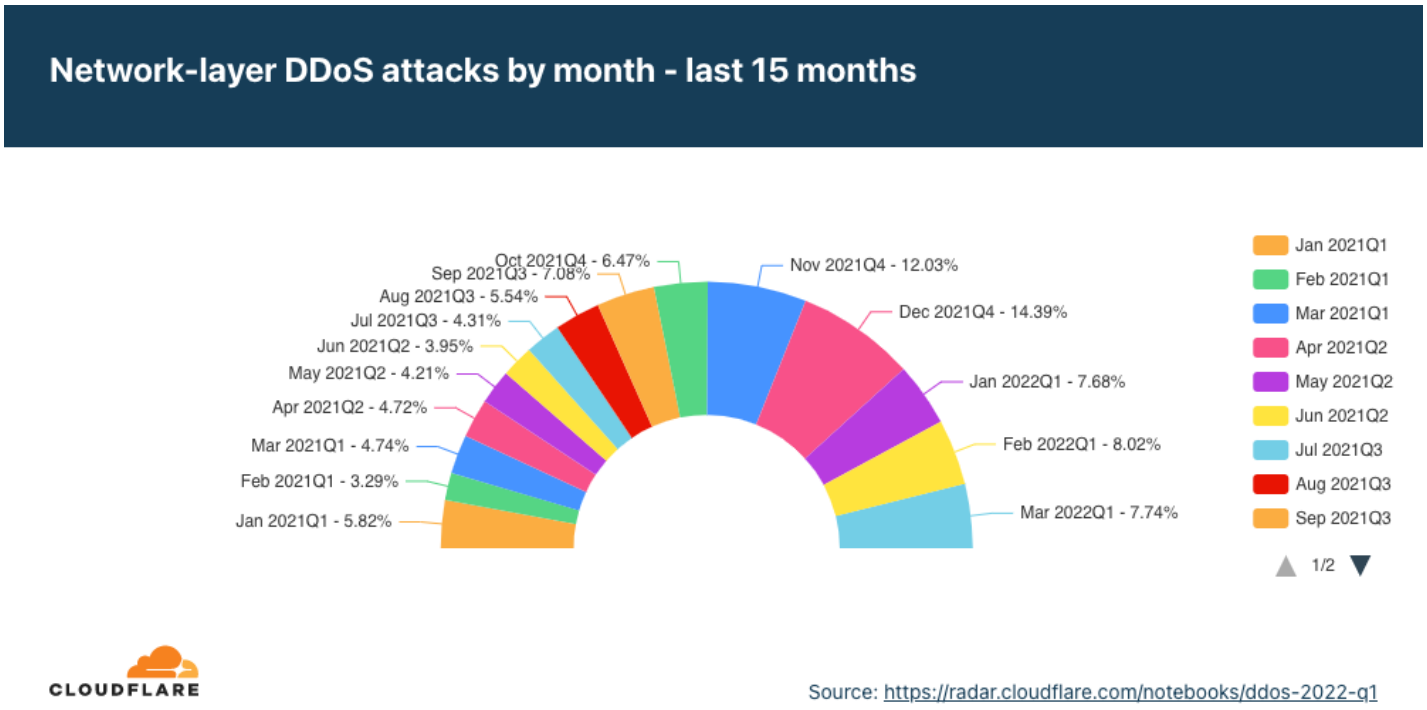
Source: https://radar.cloudflare.com/notebooks/ddos-2022-q1

Network-Layer DDoS Attacks - Quarterly distribution by month



CLOUDFLARE

Source: https://radar.cloudflare.com/notebooks/ddos-2022-q1



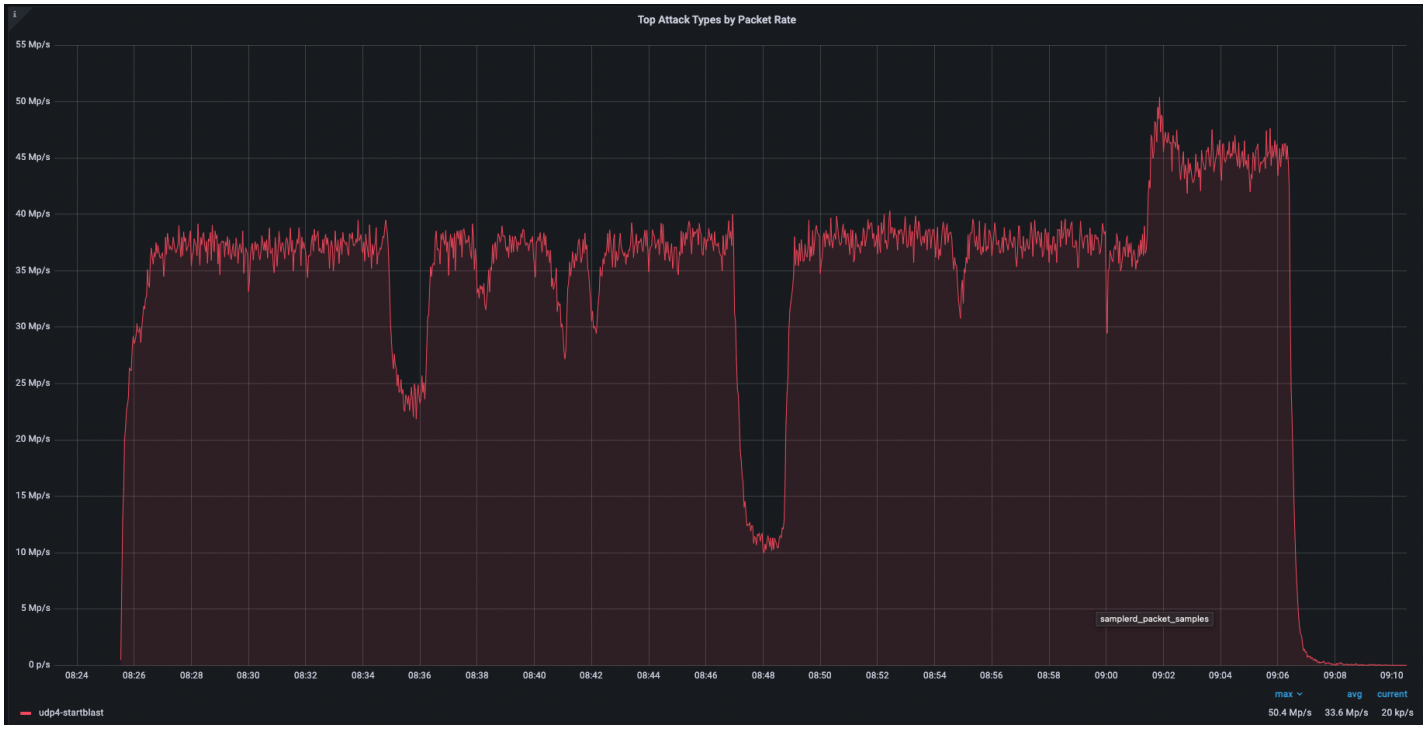
Cloudflare mitigates zero-day amplification DDoS attack

Amongst these network-layer DDoS attacks are also zero-day DDoS attacks that Cloudflare automatically detected and mitigated.

In the beginning of March, Cloudflare researchers helped investigate and expose a zero-day vulnerability in Mitel business phone systems that amongst other possible exploitations, also enables attackers to launch an amplification DDoS attack. This type of attack reflects traffic off vulnerable Mitel servers to victims, amplifying the amount of traffic sent in the process by **an amplification factor of 220 billion percent** in this specific case. You can read more about it in our recent blog post.

We observed several of these attacks across our network. One of them targeted a North American cloud provider using the Cloudflare Magic Transit service. The attack originated from 100 source IPs mainly from the US, UK, Canada, Netherlands, Australia, and approximately 20 other countries. It peaked above 50

Mpps (~22 Gbps) and was automatically detected and mitigated by Cloudflare systems.



Network-layer DDoS attacks by industry

Many network-layer DDoS attacks target Cloudflare's IP ranges directly. These IP ranges serve our WAF/CDN customers, Cloudflare authoritative DNS, Cloudflare public DNS resolver 1.1.1.1, Cloudflare Zero Trust products, and our corporate offices, to name a few. Additionally, we also allocate dedicated IP addresses to customers via our Spectrum product and advertise the IP prefixes of other companies via our Magic Transit, Magic WAN, and Magic Firewall Products for L3/4 DDoS protection.

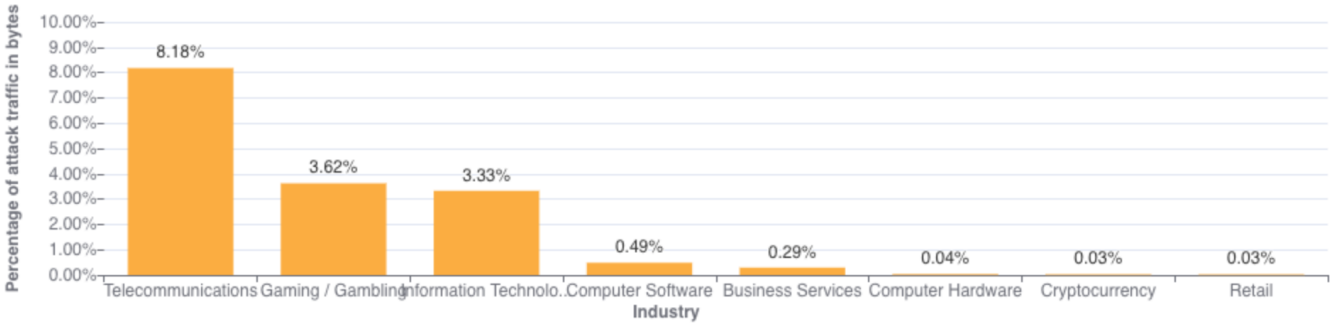
In this report, for the first time, we've begun classifying network-layer DDoS attacks according to the industries of our customers using the Spectrum and Magic products. This classification allows us to understand which industries are targeted the most by network-layer DDoS attacks.

When we look at Q1 statistics, we can see that in terms of attack packets and attack bytes launched towards Cloudflare customers, the Telecommunications

industry was targeted the most. More than 8% of all attack bytes and 10% of all attack packets that Cloudflare mitigated targeted Telecommunications companies.

Following not too far behind, in second and third place were the Gaming / Gambling and Information Technology and Services industries.

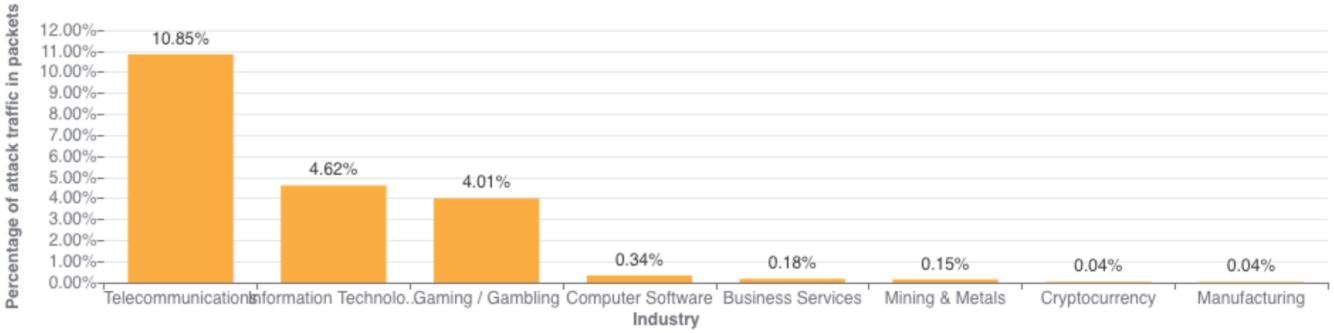
Network-Layer DDoS Attacks - Distribution of bytes by industry



CLOUDFLARE

Source: https://radar.cloudflare.com/notebooks/ddos-2022-q1

Network-Layer DDoS Attacks - Distribution of packets by industry



CLOUDFLARE

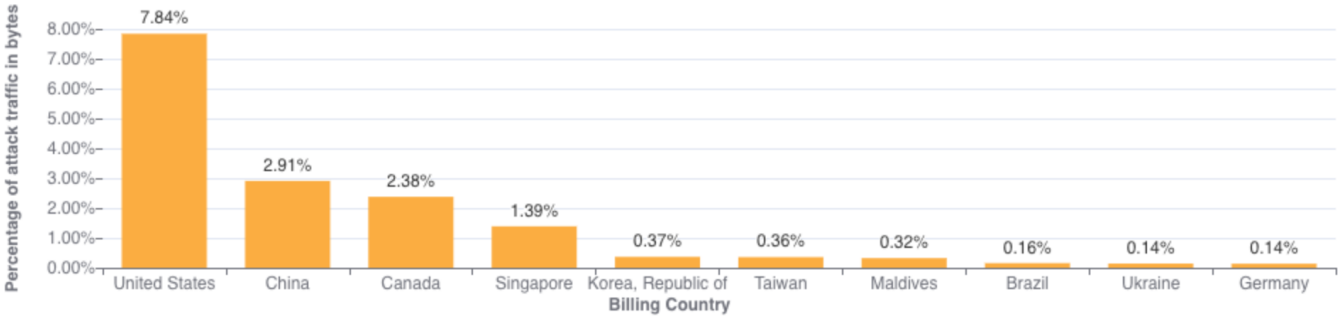
Source: https://radar.cloudflare.com/notebooks/ddos-2022-q1

Network-layer DDoS attacks by target country

Similarly to the classification by our customers' industry, we can also bucket attacks by our customers' billing country as we do for application-layer DDoS attacks, to identify the top attacked countries.

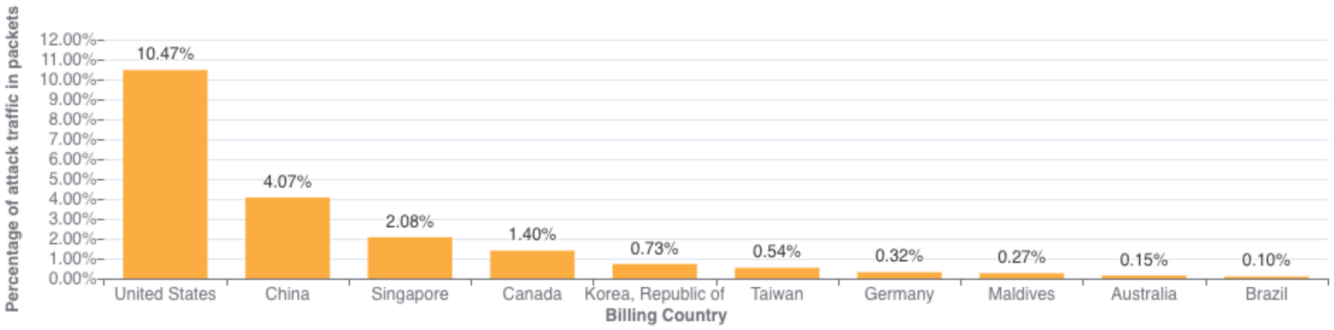
Looking at Q1 numbers, we can see that the US was targeted by the highest percentage of DDoS attacks traffic — over 10% of all attack packets and almost 8% of all attack bytes. Following the US is China, Canada, and Singapore.

Network-Layer DDoS Attacks - Distribution of bytes by target country



CLOUDFLARE

Source: https://radar.cloudflare.com/notebooks/ddos-2022-q1



CLOUDFLARE

Source: https://radar.cloudflare.com/notebooks/ddos-2022-q1

Network-layer DDoS attacks by ingress country

When trying to understand where network-layer DDoS attacks originate, we cannot use the same method as we use for the application-layer attack analysis. To launch an application-layer DDoS attack, successful handshakes must occur between the client and the server in order to establish an HTTP/S connection. For a successful handshake to occur, the attacker cannot spoof their source IP address. While the attacker may use botnets, proxies, and other methods to obfuscate their identity, the attacking client's source IP location does sufficiently represent the attack source of application-layer DDoS attacks.

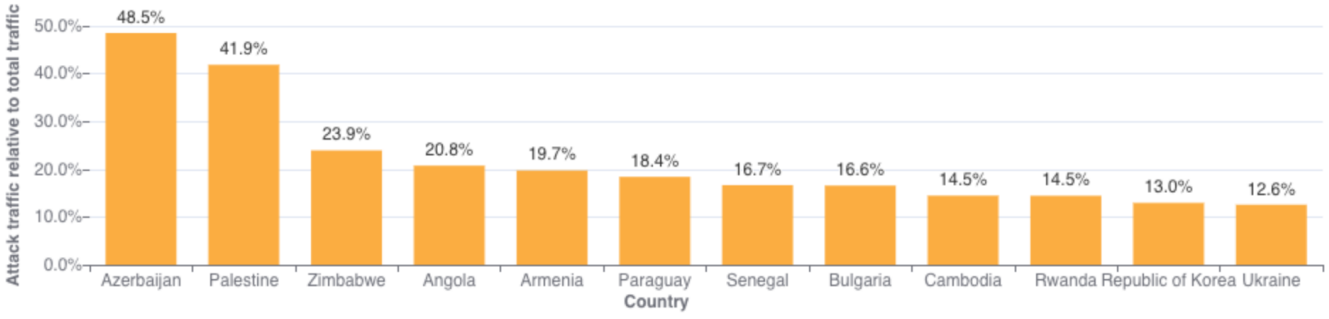
On the other hand, to launch network-layer DDoS attacks, in most cases, no handshake is needed. Attackers can spoof the source IP address in order to obfuscate the attack source and introduce randomness into the attack properties, which can make it harder for simple DDoS protection systems to block the attack. So if we were to derive the source country based on a spoofed source IP, we would get a 'spoofed country'.

For this reason, when analyzing network-layer DDoS attack sources, we bucket the traffic by the Cloudflare edge data center locations where the traffic was ingested, and not by the (potentially) spoofed source IP to get an understanding of where the attacks originate from. We are able to achieve geographical accuracy in our report because we have data centers in over 270 cities around the world. However, even this method is not 100% accurate, as traffic may be back hauled and routed via various Internet Service Providers and countries for reasons that vary from cost reduction to congestion and failure management.

In Q1, the percentage of attacks detected in Cloudflare's data centers in Azerbaijan increased by 16,624% QoQ and 96,900% YoY, making it the country with the highest percentage of network-layer DDoS activity (48.5%).

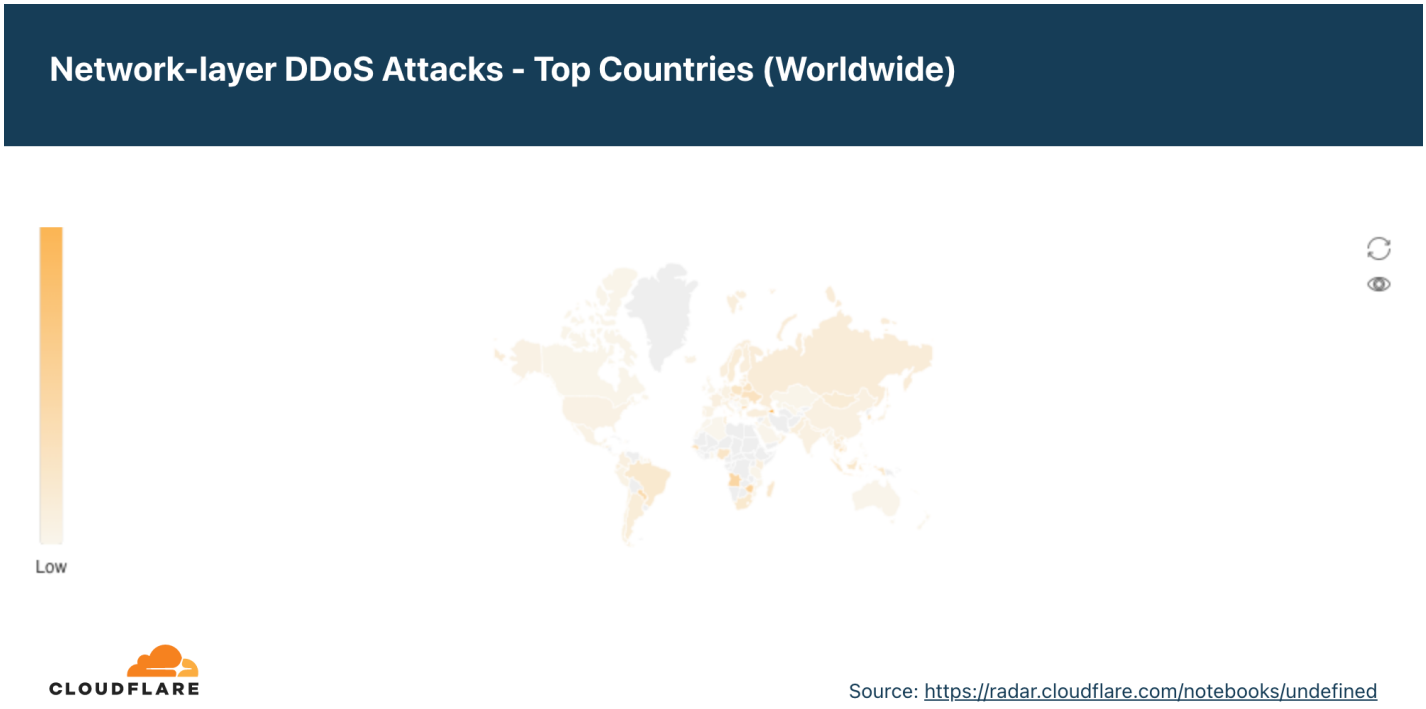
Following our Azerbaijanian data center is our Palestinian data center where a staggering 41.9% of all traffic was DDoS traffic. This represents a 10,120% increase QoQ and 46,456% YoY.

Network-Layer DDoS Attacks - Distribution by ingress country



CLOUDFLARE

Source: https://radar.cloudflare.com/notebooks/ddos-2022-q1



To view all regions and countries, check out the interactive map.

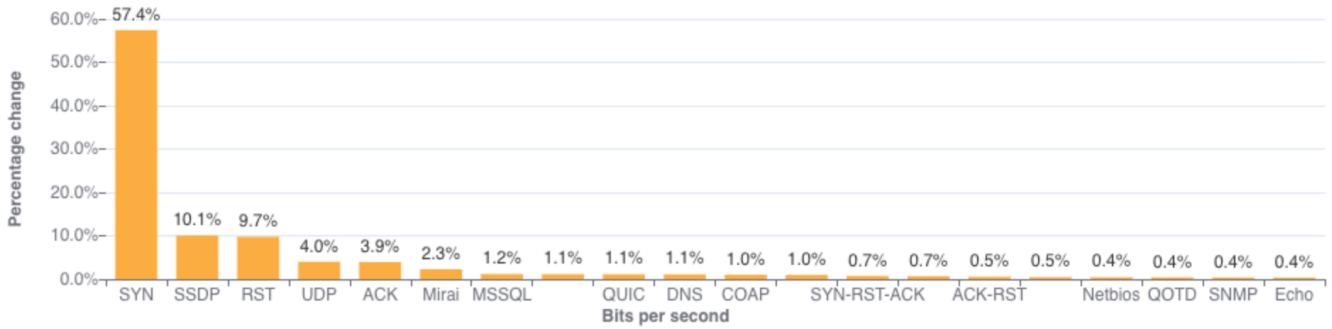
Attack vectors

SYN Floods remain the most popular DDoS attack vector, while use of generic UDP floods drops significantly in Q1.

An attack vector is a term used to describe the method that the attacker uses to launch their DDoS attack, i.e., the IP protocol, packet attributes such as TCP flags, flooding method, and other criteria.

In Q1, SYN floods accounted for 57% of all network-layer DDoS attacks, representing a 69% increase QoQ and a 13% increase YoY. In second place, attacks over SSDP surged by over 1,100% QoQ. Following were RST floods and attacks over UDP. Last quarter, generic UDP floods took the second place, but this time, generic UDP DDoS attacks plummeted by 87% QoQ from 32% to a mere 3.9%.

Network-Layer DDoS Attacks - Distribution by top attack vectors



CLOUDFLARE

Source: https://radar.cloudflare.com/notebooks/ddos-2022-q1

Emerging threats

Identifying the top attack vectors helps organizations understand the threat landscape. In turn, this may help them improve their security posture to protect against those threats. Similarly, learning about new emerging threats that may not yet account for a significant portion of attacks, can help mitigate them before they become a significant force.

When we look at new emerging attack vectors in Q1, we can see increases in DDoS attacks reflecting off of Lantronix services (+971% QoQ) and SSDP reflection attacks (+724% QoQ). Additionally, SYN-ACK attacks increased by 437% and attacks by Mirai botnets by 321% QoQ.

Attacker reflecting traffic off of Lantronix Discovery Service

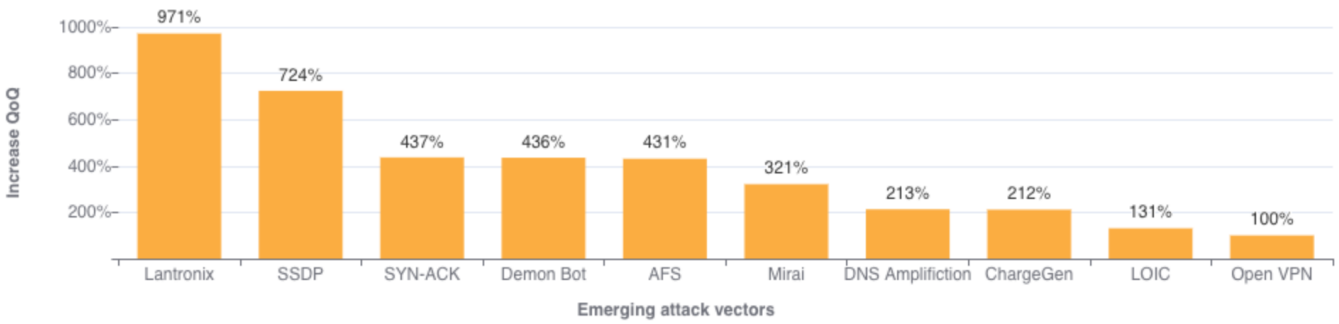
Lantronix is a US-based software and hardware company that provides solutions for Internet of Things (IoT) management amongst their vast offering. One of the tools that they provide to manage their IoT components is the Lantronix Discovery Protocol. It is a command-line tool that helps to search and find

Lantronix devices. The discovery tool is UDP-based, meaning that no handshake is required. The source IP can be spoofed. So an attacker can use the tool to search for publicly exposed Lantronix devices using a 4 byte request, which will then in turn respond with a 30 byte response from port 30718. By spoofing the source IP of the victim, all Lantronix devices will target their responses to the victim — resulting in a reflection/amplification attack.

Simple Service Discovery Protocol used for reflection DDoS attacks

The Simple Service Discovery Protocol (SSDP) protocol works similarly to the Lantronix Discovery protocol, but for Universal Plug and Play (UPnP) devices such as network-connected printers. By abusing the SSDP protocol, attackers can generate a reflection-based DDoS attack overwhelming the target's infrastructure and taking their Internet properties offline. You can read more about SSDP-based DDoS attacks here.

Network-Layer DDoS Attacks - Distribution by top emerging threats



CLOUDFLARE

Source: https://radar.cloudflare.com/notebooks/ddos-2022-q1

Network-layer DDoS attacks by attack rate

In Q1, we observed a massive uptick in volumetric DDoS attacks — both from the packet rate and bitrate perspective. Attacks over 10 Mpps grew by over 300% QoQ, and attacks over 100 Gbps grew by 645% QoQ.

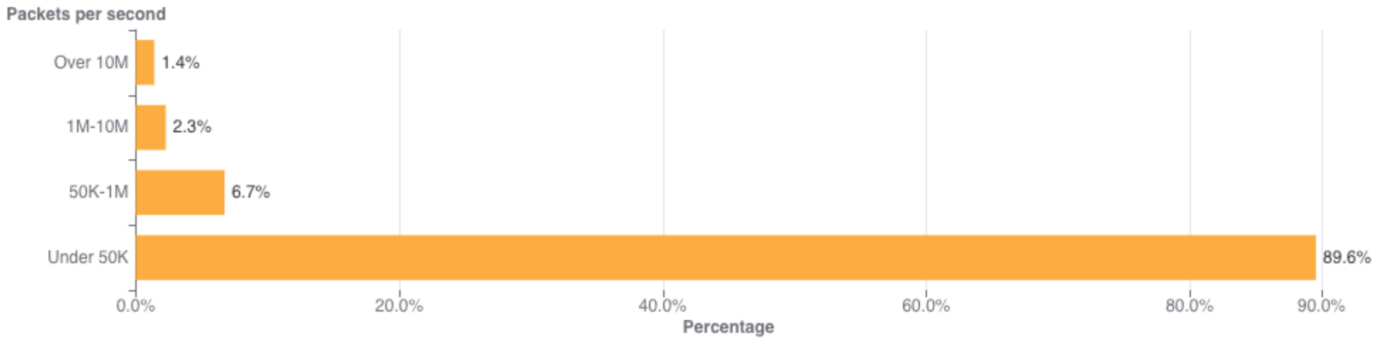
There are different ways of measuring the size of an L3/4 DDoS attack. One is the volume of traffic it delivers, measured as the bit rate (specifically, terabits per second or gigabits per second). Another is the number of packets it delivers, measured as the packet rate (specifically, millions of packets per second).

Attacks with high bit rates attempt to cause a denial-of-service event by clogging the Internet link, while attacks with high packet rates attempt to overwhelm the servers, routers, or other in-line hardware appliances. These devices dedicate a certain amount of memory and computation power to process each packet. Therefore, by bombarding it with many packets, the appliance can be left with no further processing resources. In such a case, packets are "dropped," i.e., the appliance is unable to process them. For users, this results in service disruptions and denial of service.

Distribution by packet rate

The majority of network-layer DDoS attacks remain below 50,000 packets per second. While 50 kpps is on the lower side of the spectrum at Cloudflare scale, it can still easily take down unprotected Internet properties and congest even a standard Gigabit Ethernet connection.

Network-Layer DDoS Attacks - Distribution by packet rate

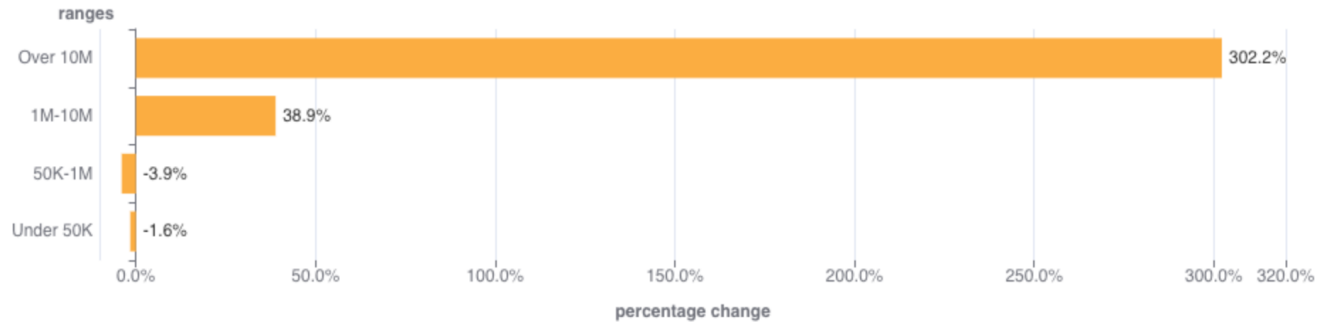


CLOUDFLARE

Source: https://radar.cloudflare.com/notebooks/ddos-2022-q1

When we look at the changes in the attack sizes, we can see that attacks of over 10 Mpps grew by over 300% QoQ. Similarly, attacks of 1-10 Mpps grew by almost 40% QoQ.

Network-Layer DDoS Attacks - QoQ change in packet rate



CLOUDFLARE

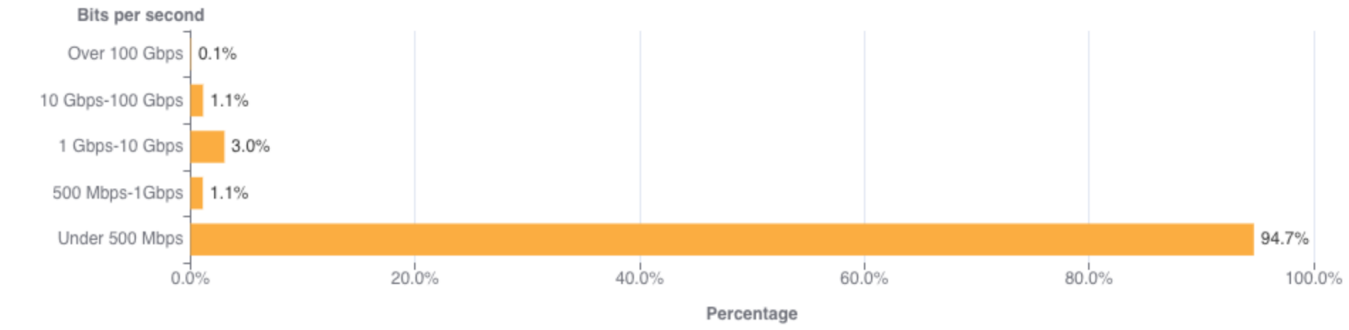
Source: https://radar.cloudflare.com/notebooks/ddos-2022-q1

Distribution by bitrate

In Q1, most of the network-layer DDoS attacks remain below 500 Mbps. This too is a tiny drop in the water at Cloudflare scale, but can very quickly shut down

unprotected Internet properties with less capacity or at the very least congest, even a standard Gigabit Ethernet connection.

Network-Layer DDoS Attacks - Distribution by bit rate



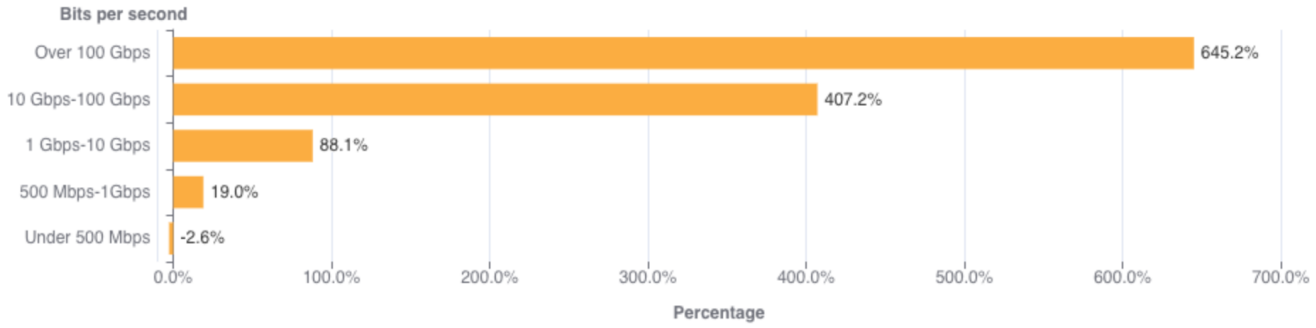
CLOUDFLARE

Source: https://radar.cloudflare.com/notebooks/ddos-2022-q1

Graph of the distribution of network-layer DDoS attacks by bit rate in 2022 Q1

Similarly to the trends observed in the packet-per-second realm, here we can also see large increases. The amount of DDoS attacks that peaked over 100 Gbps increased by 645% QoQ; attacks peaking between 10 Gbps to 100 Gbps increased by 407%; attacks peaking between 1 Gbps to 10 Gbps increased by 88%; and even attacks peaking between 500 Mbps to 1 Gbps increased by almost 20% QoQ.

Network-Layer DDoS Attacks - QoQ change in bit rate



CLOUDFLARE

Source: https://radar.cloudflare.com/notebooks/ddos-2022-q1

Network-layer DDoS attacks by duration

Most attacks remain under one hour in duration, reiterating the need for automated always-on DDoS mitigation solutions.

We measure the duration of an attack by recording the difference between when it is first detected by our systems as an attack and the last packet we see with that attack signature towards that specific target.

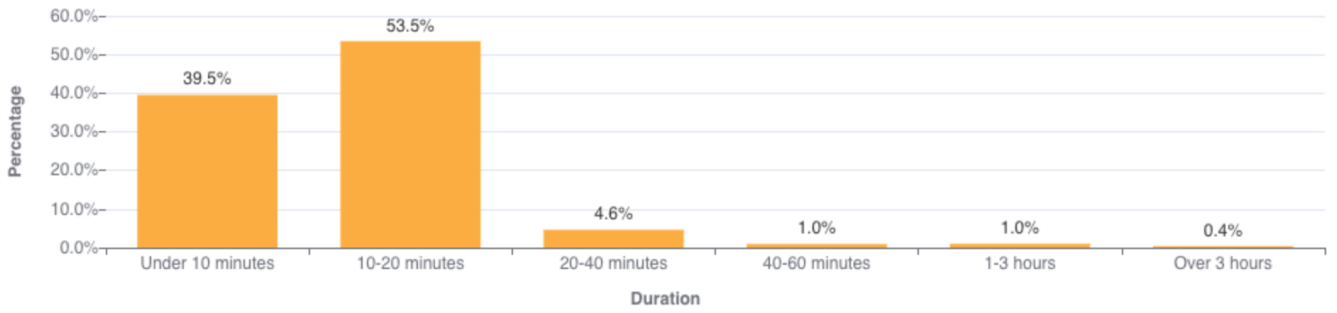
In previous reports, we provided a breakdown of 'attacks under an hour', and larger time ranges. However, in most cases over 90 percent of attacks last less than an hour. So starting from this report, we broke down the short attacks and grouped them by shorter time ranges to provide better granularity.

One important thing to keep in mind is that even if an attack lasts only a few minutes, if it is successful, the repercussions could last well beyond the initial attack duration. IT personnel responding to a successful attack may spend hours and even days restoring their services.

In the first quarter of 2022, more than half of the attacks lasted 10-20 minutes, approximately 40% ended within 10 minutes, another ~5% lasted 20-40 minutes,

and the remaining lasted longer than 40 minutes.

Network-Layer DDoS Attacks - Distribution by duration



CLOUDFLARE

Source: https://radar.cloudflare.com/notebooks/ddos-2022-q1

Short attacks can easily go undetected, especially burst attacks that, within seconds, bombard a target with a significant number of packets, bytes, or requests. In this case, DDoS protection services that rely on manual mitigation by security analysis have no chance in mitigating the attack in time. They can only learn from it in their post-attack analysis, then deploy a new rule that filters the attack fingerprint and hope to catch it next time. Similarly, using an "on-demand" service, where the security team will redirect traffic to a DDoS provider during the attack, is also inefficient because the attack will already be over before the traffic routes to the on-demand DDoS provider.

It's recommended that companies use automated, always-on DDoS protection services that analyze traffic and apply real-time fingerprinting fast enough to block short-lived attacks.

Summary

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. As part of our mission, since 2017, we've been providing unmetered and unlimited DDoS protection for free to all of our customers. Over the years, it has become increasingly easier for attackers to launch DDoS attacks. But as easy as it has become, we want to make sure that it is even easier — and free — for organizations of all sizes to protect themselves against DDoS attacks of all types.

Not using Cloudflare yet? Start now with our Free and Pro plans to protect your websites, or contact us for comprehensive DDoS protection for your entire network using Magic Transit.

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 DDoS Reports Attacks Trends Cloudflare Radar