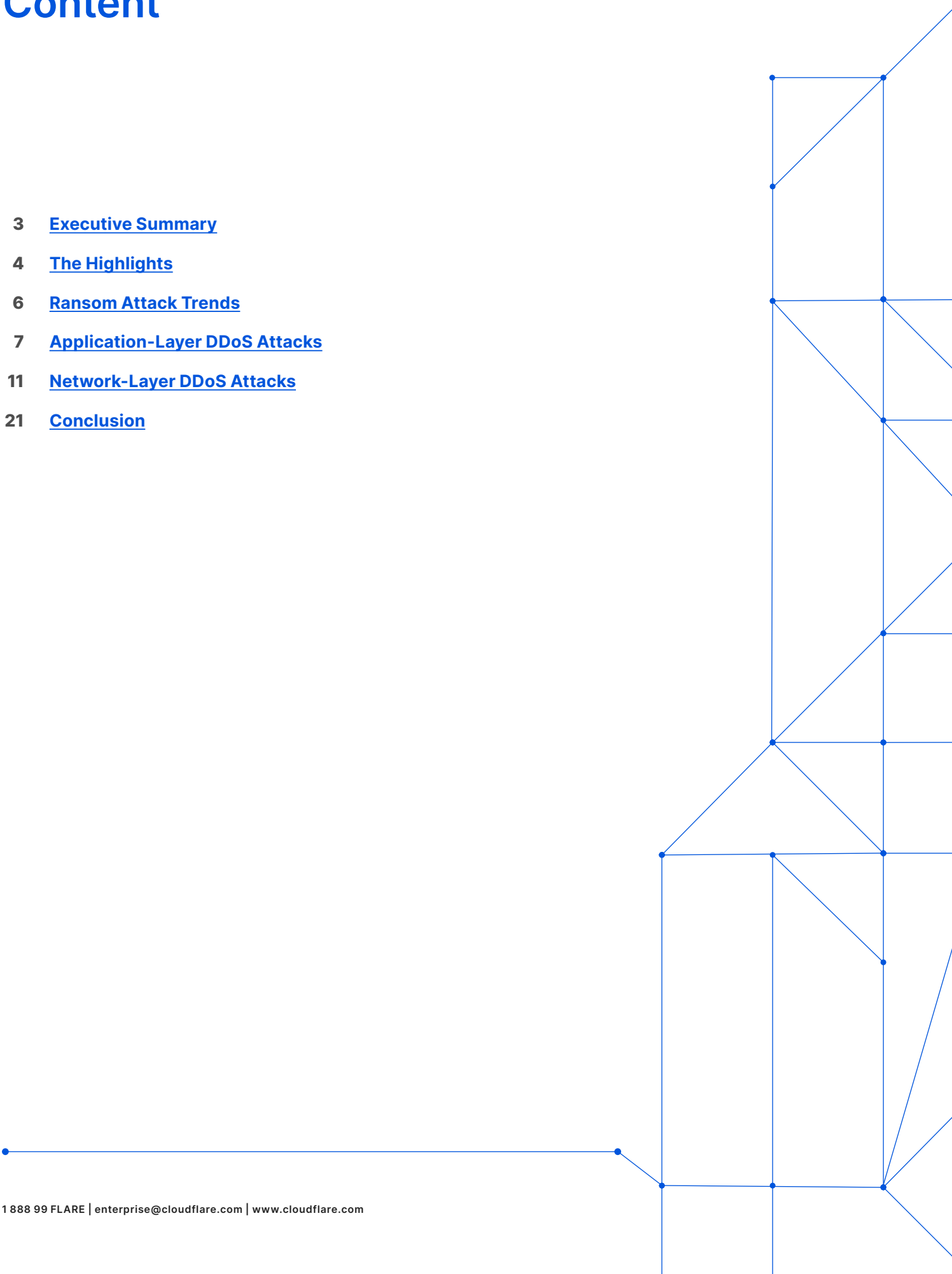
CLOUDFLARE

THREAT REPORT

DDoS Attack Threat Landscape

DDoS trends from Q2 2022

Content



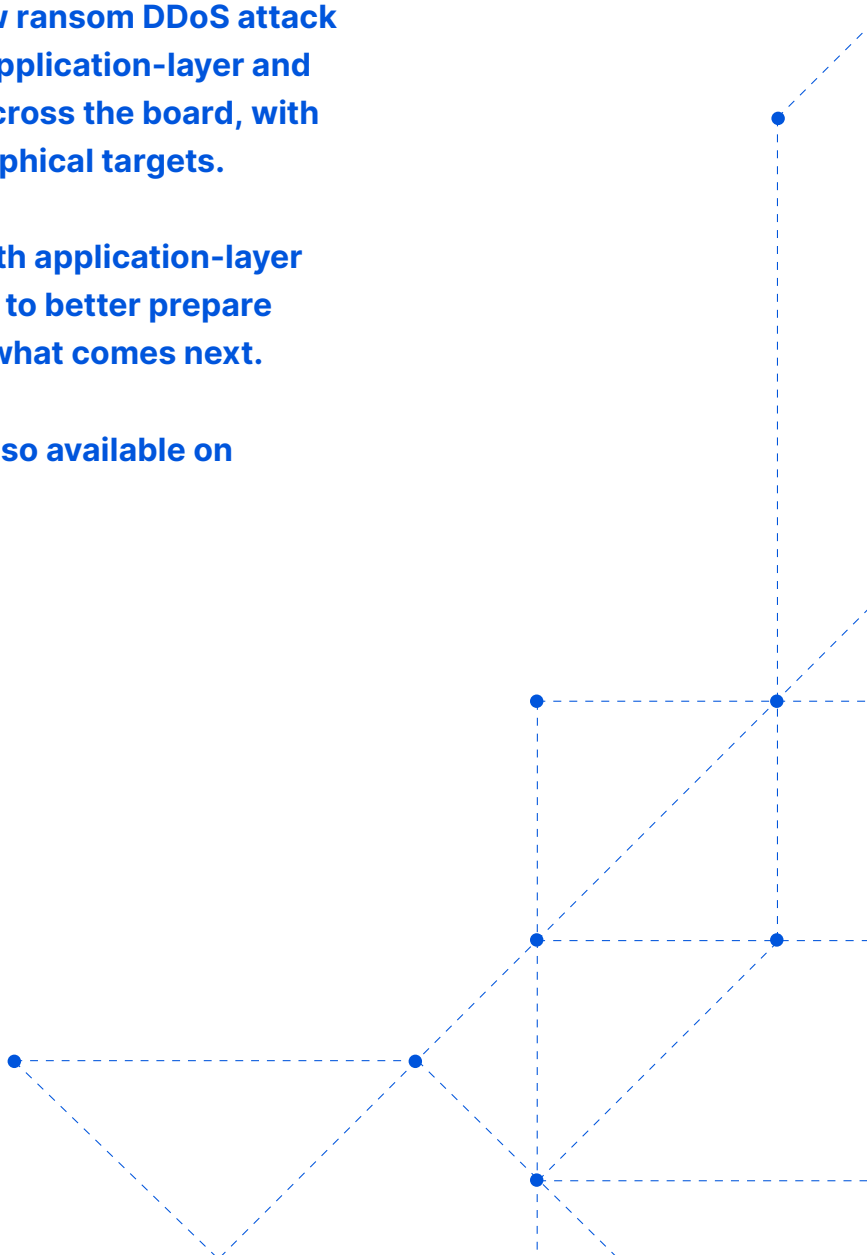
Executive Summary

Welcome to the Cloudflare quarterly DDoS report. This report uncovers insights and trends about the DDoS threat landscape observed across the global Cloudflare network in the second quarter of 2022.

During this time period, we recorded some of the largest attacks the world has ever seen, including a 26 million request per second HTTPS DDoS attack that Cloudflare automatically detected and mitigated. Attacks against Ukraine and Russia continued and a new ransom DDoS attack campaign emerged. Increases of both application-layer and network-layer attacks were observed across the board, with notable changes in industry and geographical targets.

In the sections below, we will outline both application-layer and network-layer DDoS attack insights to better prepare and inform organizations like yours for what comes next.

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



The Highlights

① Ukrainian and Russian Internet

- The war on the ground is accompanied by attacks targeting the spread of information.
- Broadcast media companies in the Ukraine were the most targeted in Q2 by DDoS attacks. In fact, all the top six most attacked industries are all in online/Internet media, publishing, and broadcasting.
- In Russia, on the other hand, online media dropped to the third-most attacked industry. Making their way to the top, banking, financial services and insurance (BFSI) companies in Russia were the most targeted in Q2.
- Almost 45% of all application-layer DDoS attacks targeted the BFSI sector. Cryptocurrency companies in Russia were the second-most attacked.

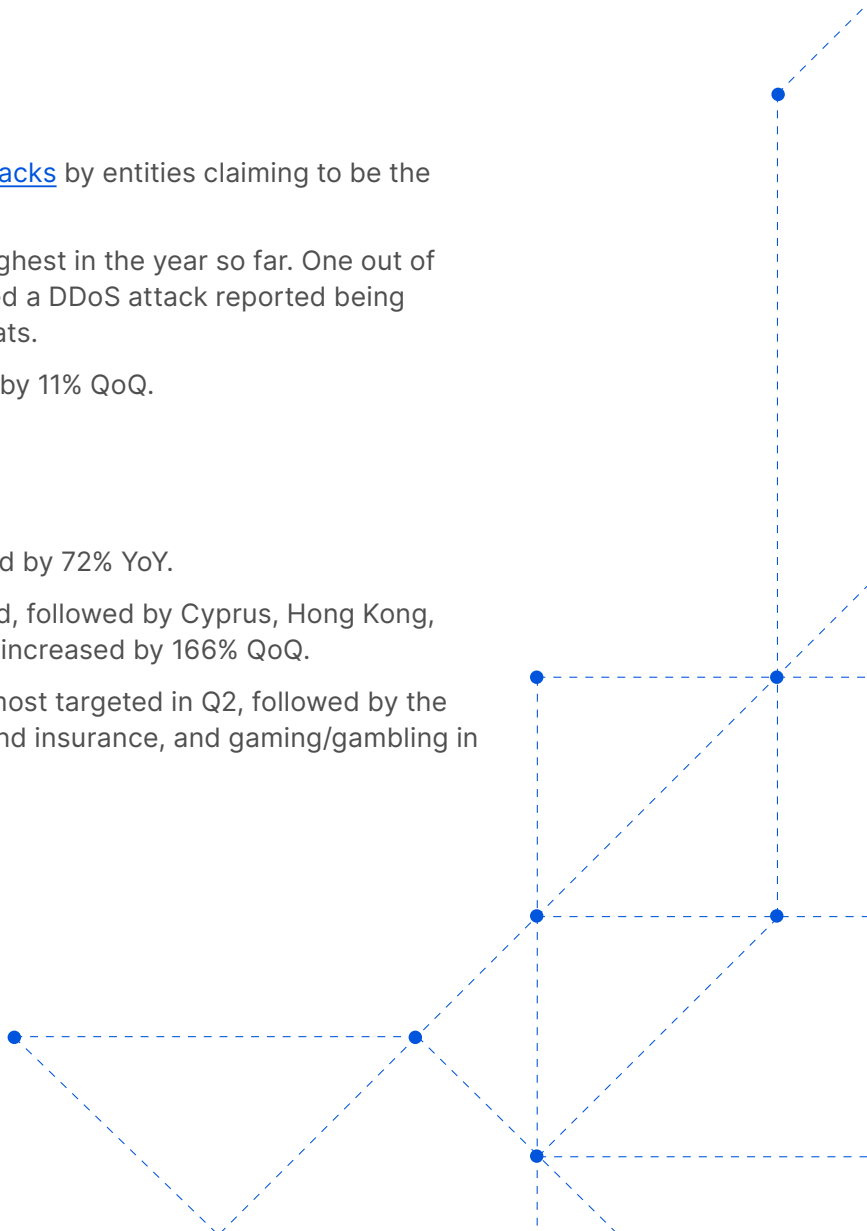
Read more about what Cloudflare is doing to keep the open Internet flowing into Russia and keep attacks from getting out.

② Ransom DDoS attacks

- We have seen a new wave of ransom DDoS attacks by entities claiming to be the Fancy Lazarus.
- In June 2022, ransom attacks peaked to the highest in the year so far. One out of every five survey respondents who experienced a DDoS attack reported being subject to a ransom DDoS attack or other threats.
- Overall in Q2, ransom DDoS attacks increased by 11% QoQ.

③ Application-layer DDoS attacks

- In Q2, application-layer DDoS attacks increased by 72% YoY.
- Organizations in the US were the most targeted, followed by Cyprus, Hong Kong, and China. Attacks on organizations in Cyprus increased by 166% QoQ.
- The aviation and aerospace industry was the most targeted in Q2, followed by the Internet industry, banking, financial Services and insurance, and gaming/gambling in fourth place.



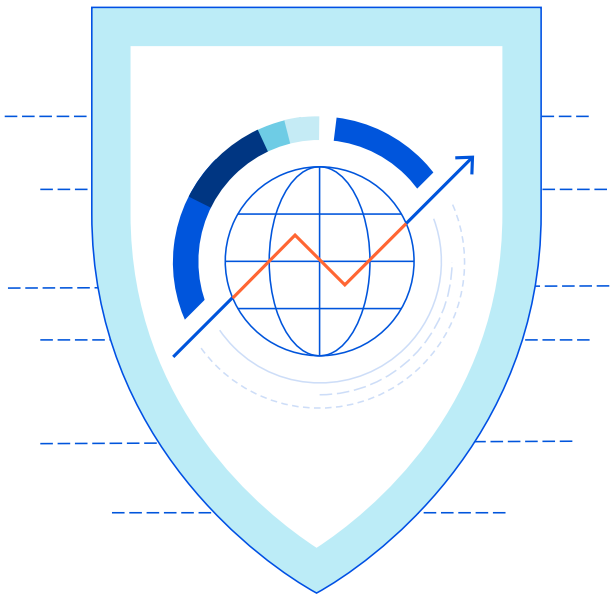
④ Network-layer DDoS attacks

- In Q2, network-layer DDoS attacks increased by 109% YoY.
- Attacks of 100 Gbps and larger increased by 8% QoQ.
- Attacks lasting more than three hours increased by 12% QoQ.
- The top attacked industries were telecommunications, gaming/gambling, and information technology and services.
- Organizations in the US were the most targeted followed by China, Singapore and Germany.

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

A note on how we measure DDoS attacks observed over our network

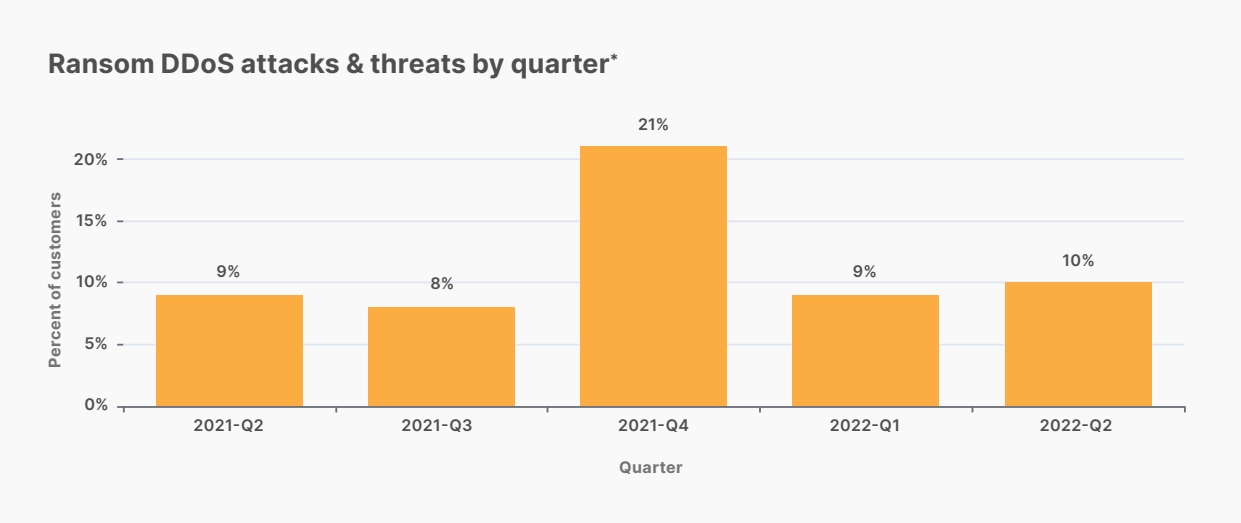
To analyze attack trends, we calculate the "DDoS activity" rate, which is either the percentage of attack traffic out of the total traffic (attack + clean) observed over our global network, or in a specific location, or in a specific category (e.g., industry or billing country). Measuring the percentages 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.



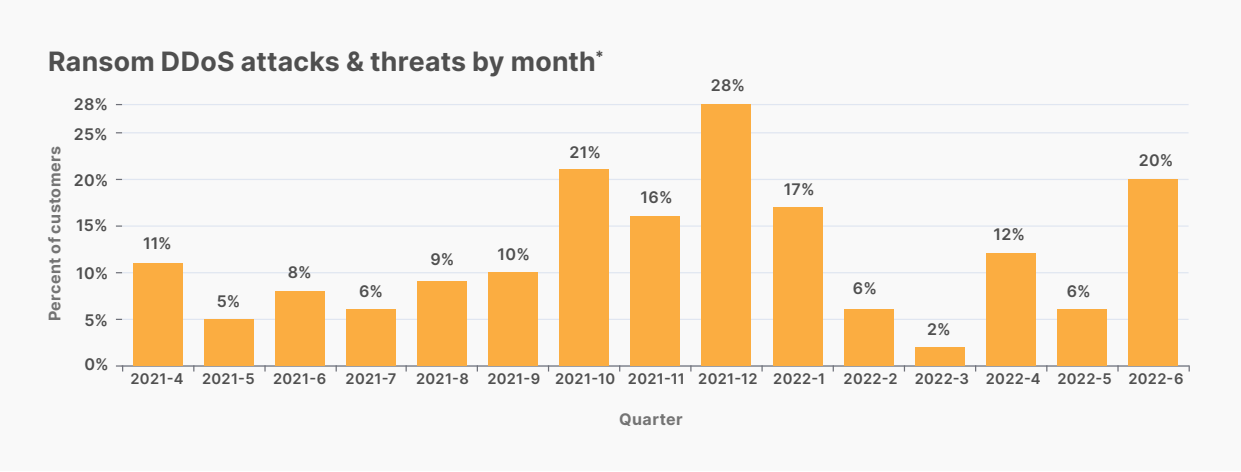
Ransom Attack Trends

Our systems constantly analyze traffic and automatically detect and mitigate DDoS attacks. Each impacted customer is prompted with an automated survey to help us better understand the nature of the attack and the success of the mitigation. One of the questions on the survey asked if the respondents received a threat or a ransom note demanding payment in exchange to stop the DDoS attack.

The number of respondents reporting threats or ransom notes in Q2 increased by 11% QoQ and YoY. During this quarter, we've been mitigating ransom DDoS attacks that have been launched by entities claiming to be the Advanced Persistent Threat (APT) group Fancy Lazarus. The campaign was found to have been focused on financial institutions and cryptocurrency companies.



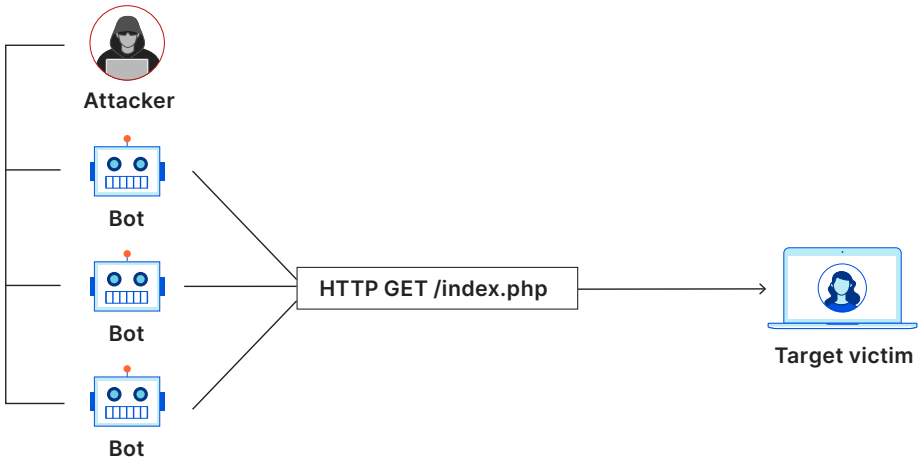
In June, one out of every five respondents reported receiving a ransom DDoS attack or threat — the highest rate since December 2021.



*Source: https://radar.cloudflare.com/notebooks/ddos-2022-q2

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.

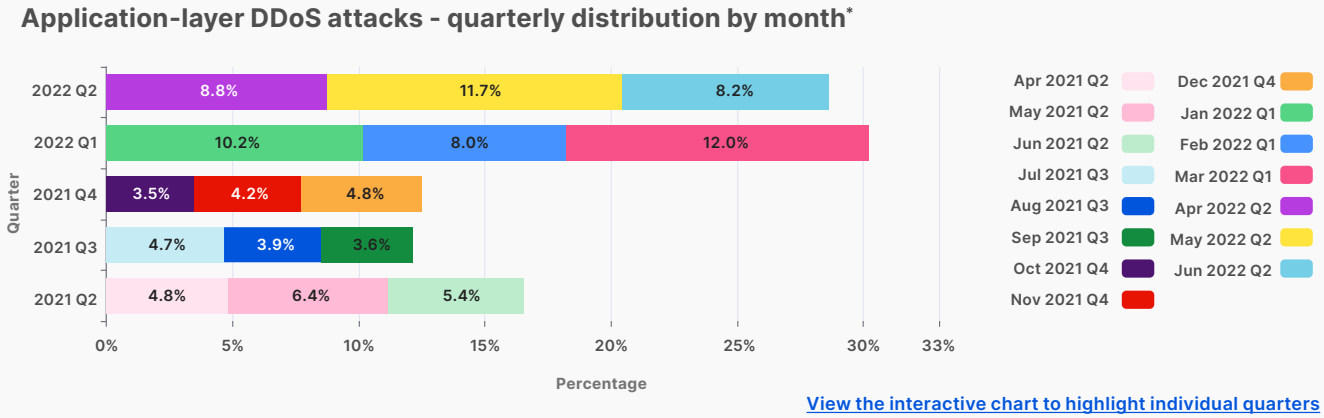


Application-layer DDoS attack

Application-layer DDoS attacks by month

In Q2, application-layer DDoS attacks increased by 72% YoY.

Overall, in Q2, the volume of application-layer DDoS attacks increased by 72% YoY, but decreased 5% QoQ. May was the busiest month in the quarter. Almost 41% of all application-layer DDoS attacks took place in May. The lowest volume of attacks, just 28%, occured in June.



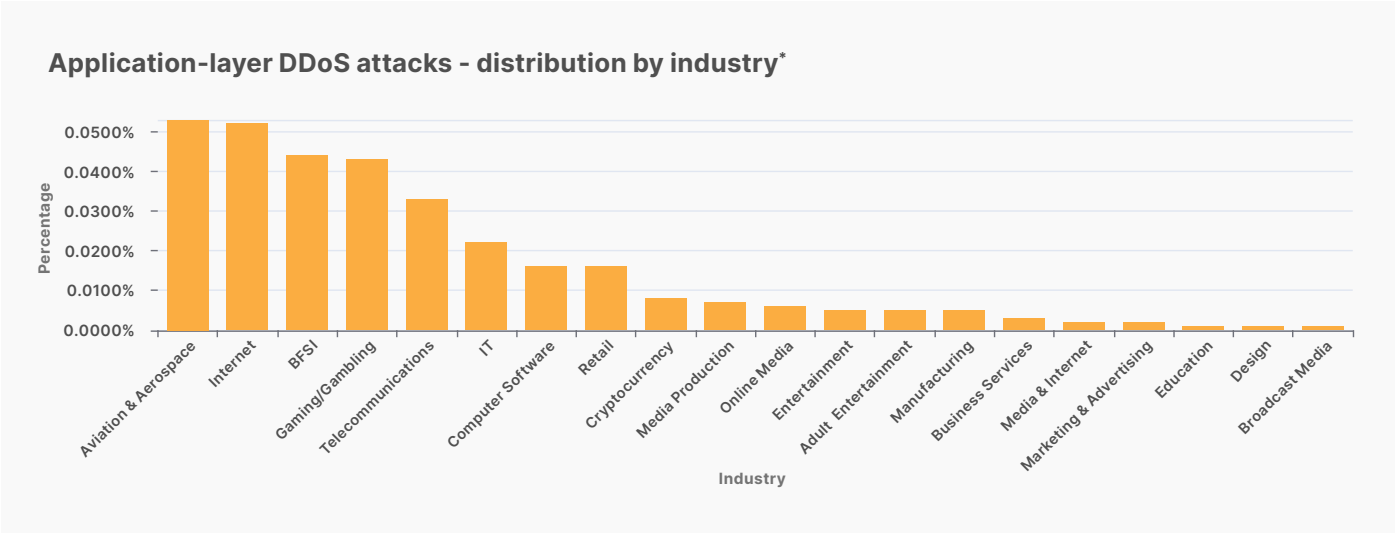
View the interactive chart to highlight individual quarters

*Source: https://radar.cloudflare.com/notebooks/ddos-2022-q2

Application-layer DDoS attacks by industry

Attacks on the aviation and aerospace industry increased by 493% QoQ.

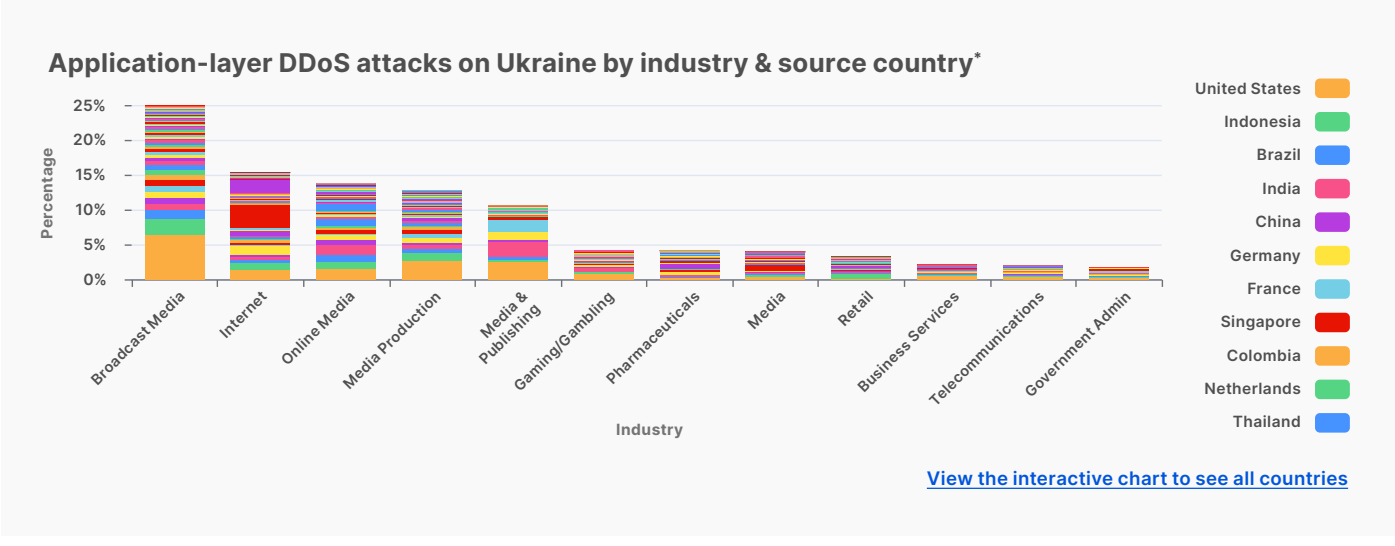
In Q2, aviation and aerospace was the most targeted industry by application-layer DDoS attacks. In sequential order, other highly-targeted industries included banking, financial institutions and insurance (BFSI), and gaming/gambling.



Ukraine and Russia cyberspace

Media and publishing companies are the most targeted in Ukraine.

Just as the war in Ukraine continued on the ground, in the air, and on the water, it also continued to unfold in cyberspace. Entities targeting Ukrainian companies appear to be trying to silence information, as the top six most attacked industries in Ukraine all belonged to broadcasting, Internet, online media, and publishing. These industries alone accounted for almost 80% of all DDoS attacks targeting Ukraine.

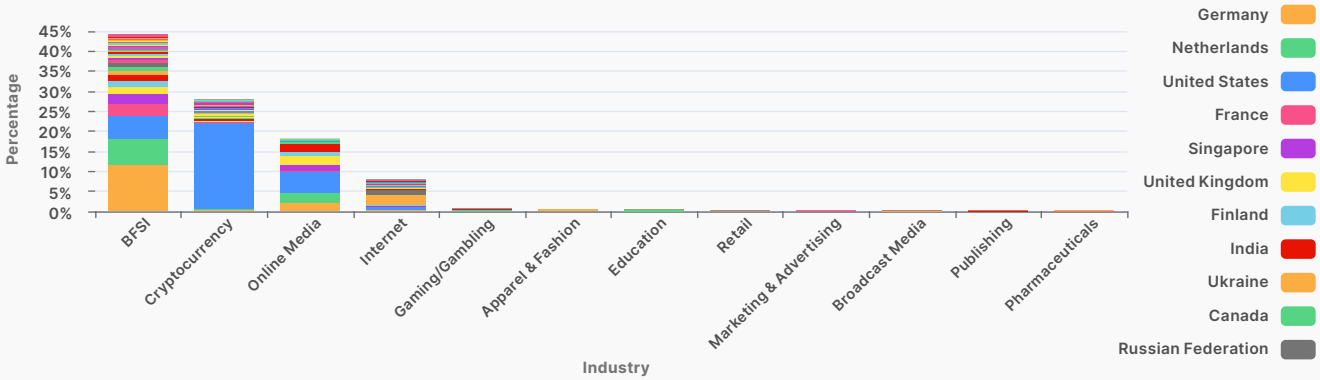


View the interactive chart to see all countries

*Source: https://radar.cloudflare.com/notebooks/ddos-2022-q2

On the other side of the war, the Russian banks, financial institutions and insurance (BFSI) companies came under the most attacks. In fact, almost 45% of all DDoS attacks targeted the BFSI sector. The second most targeted was the cryptocurrency industry, followed by online media.

Application-layer DDoS attacks on Russia by industry & source country*



View the interactive chart to see all countries

On both sides of the war, we can see that the attacks are highly distributed, indicating the use of globally distributed botnets.

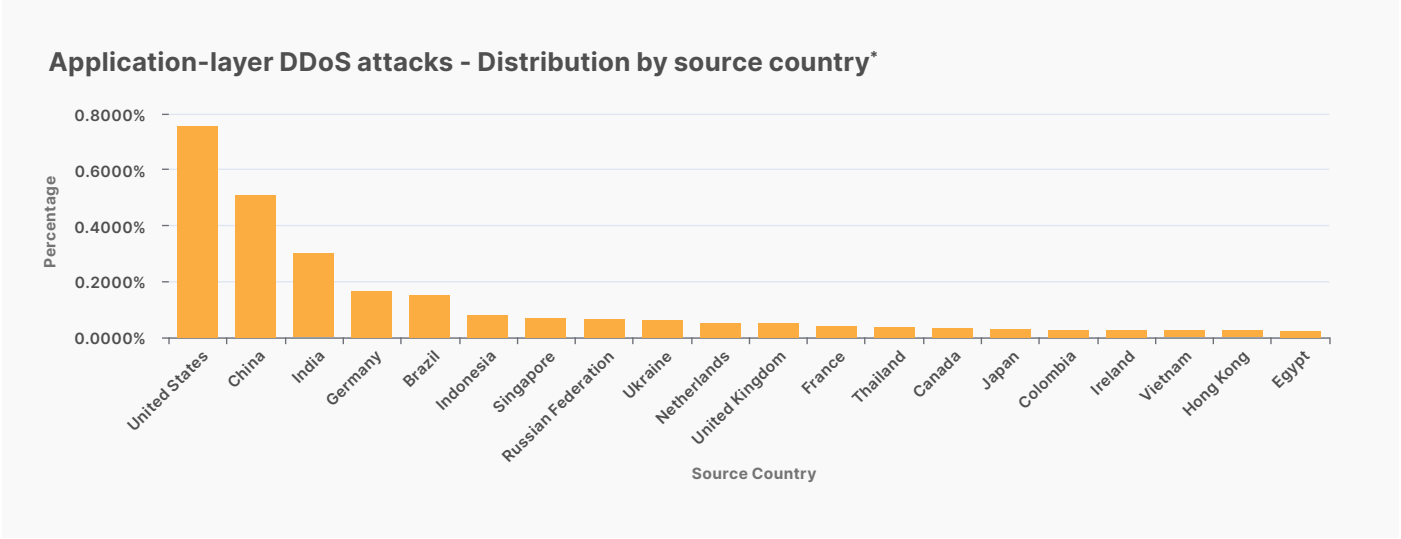
Application-layer DDoS attacks by source country

In Q2, attacks from China decreased by 78%, while attacks from the US shrank by 43%.

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 doesn't mean that specific country is launching the attacks. Rather, it indicates the presence of botnets operating from within the country's borders.

For the second quarter in a row, the US tops the charts as the main source of HTTP DDoS attacks, followed by China, India, and Germany. Interestingly, even though the US ranked first for two consecutive quarters, attacks originating from the US shrank by 48% QoQ while attacks from other regions grew. Attacks originating from India grew by 87%, from Germany by 33%, and from Brazil by 67%.

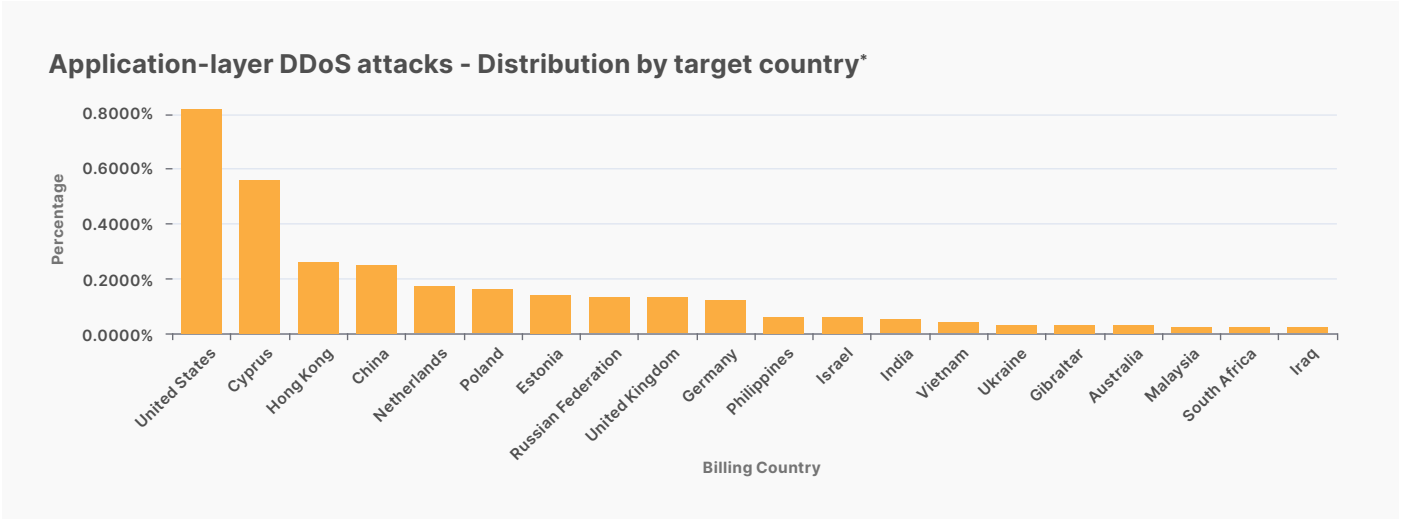
*Source: https://radar.cloudflare.com/notebooks/ddos-2022-q2



Application-layer DDoS attacks by target country

In order to identify which countries are targeted by the most HTTP DDoS attacks, we bucketed the DDoS attacks by our customers' billing countries and represented them as a percentage of all DDoS attacks.

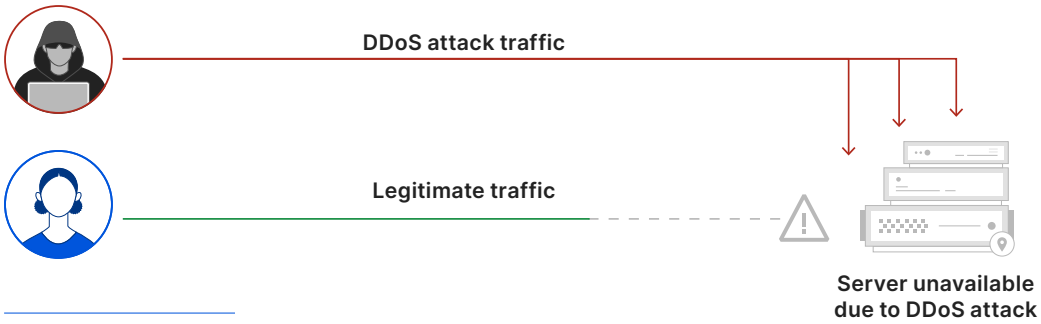
HTTP DDoS attacks on US-based targets increased by 67% QoQ, pushing the US into first place as the main target country of application-layer DDoS attacks. Attacks on Chinese companies plunged by 80% QoQ, dropping China from first place to fourth. Attacks on Cyprus increased by 167%, which made it the second-most attacked country in Q2 followed by Hong Kong, China, and the Netherlands.



*Source: https://radar.cloudflare.com/notebooks/ddos-2022-q2

Network-Layer DDoS Attacks

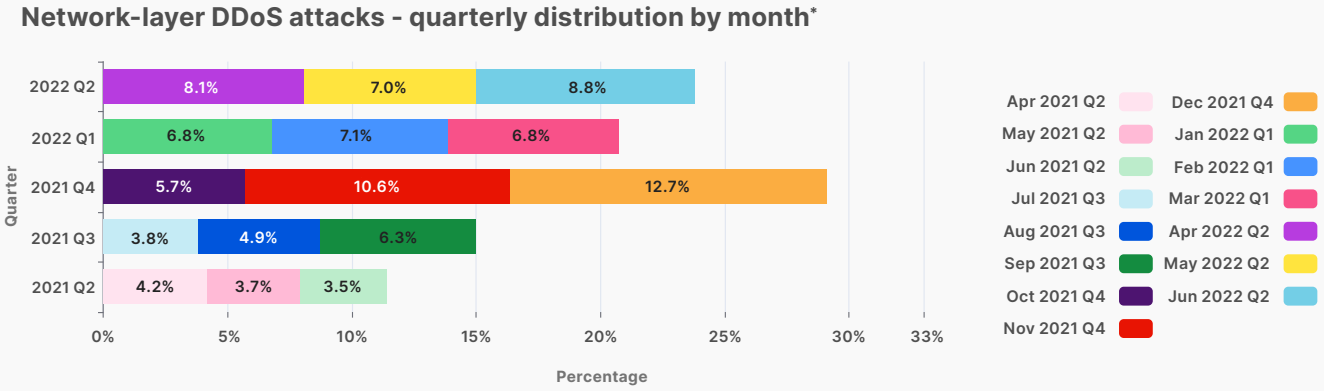
Application-layer attacks target the application (Layer 7 of the OSI model) running the service that end users are trying to access (in this case, HTTP/S). By contrast, network-layer attacks aim to overwhelm network infrastructure — such as inline routers and servers — and the Internet link itself.



DDoS attack denying service to legitimate users

Network-layer DDoS attacks by month

In Q2, network-layer DDoS attacks increased by 109% YoY, and volumetric attacks of 100 Gbps and larger increased by 8% QoQ.



View the interactive chart to highlight individual quarters

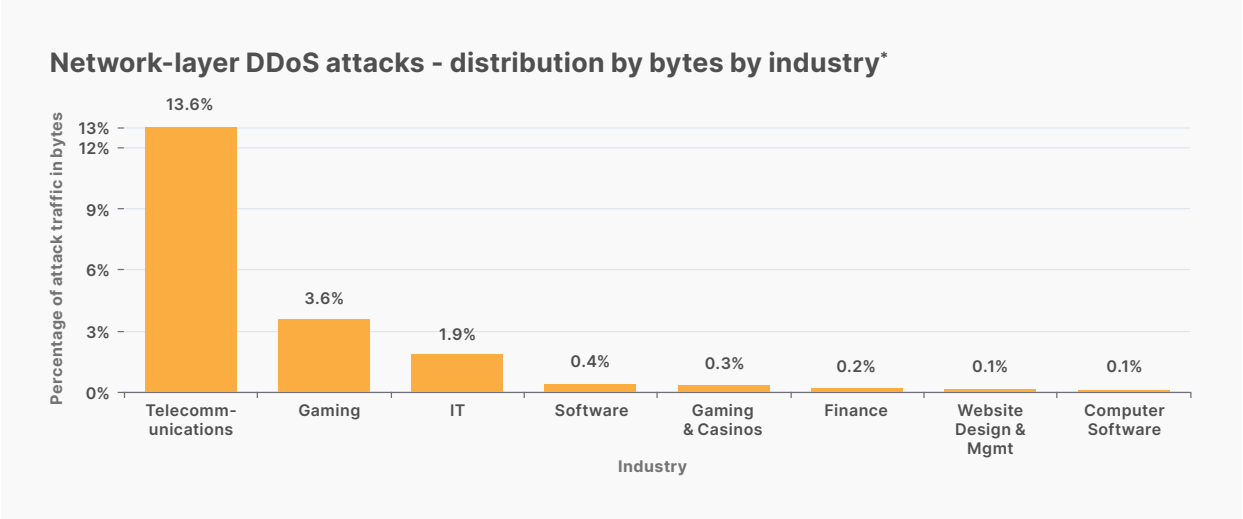
In Q2, the total amount of network-layer DDoS attacks increased by 109% YoY and 15% QoQ. June alone saw almost 36% of all network-layer attacks.

*Source: https://radar.cloudflare.com/notebooks/ddos-2022-q2

Network-layer DDoS attacks by industry

In Q2, attacks on telecommunication companies grew by 66% QoQ.

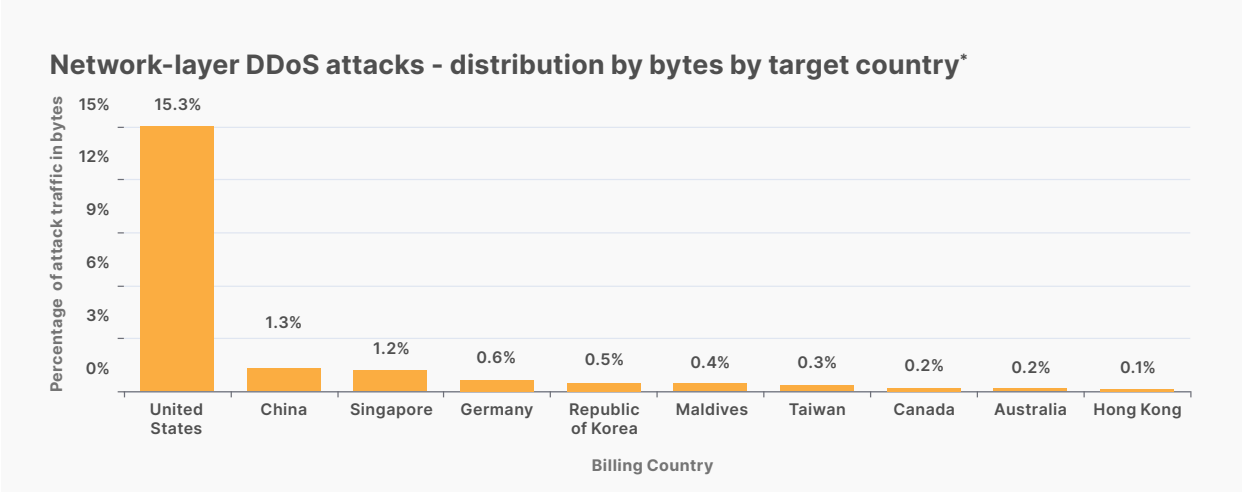
For the second consecutive quarter, the telecommunications industry was the most targeted by network-layer DDoS attacks. Moreover, attacks on telecommunication companies grew by 66% QoQ. The gaming industry ranked second, followed by information technology and services.



Network-layer DDoS attacks by target country

Attacks on US networks grew by 95% QoQ.

In Q2, the US remained the most attacked country by a wide margin, followed by China, Singapore, and Germany.



*Source: https://radar.cloudflare.com/notebooks/ddos-2022-q2

Network-layer DDoS attacks by ingress country

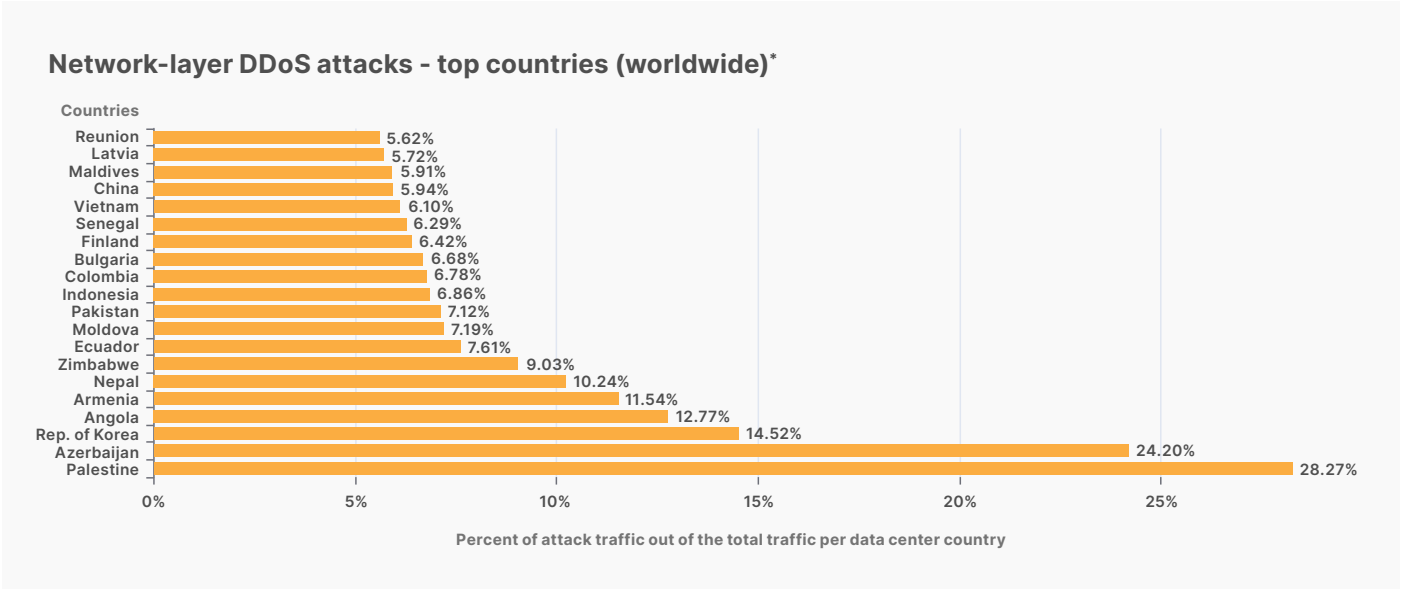
In Q2, almost a third of the traffic Cloudflare observed in Palestine and a fourth of the traffic in Azerbaijan was part of a network-layer DDoS attack.

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 attacks 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.

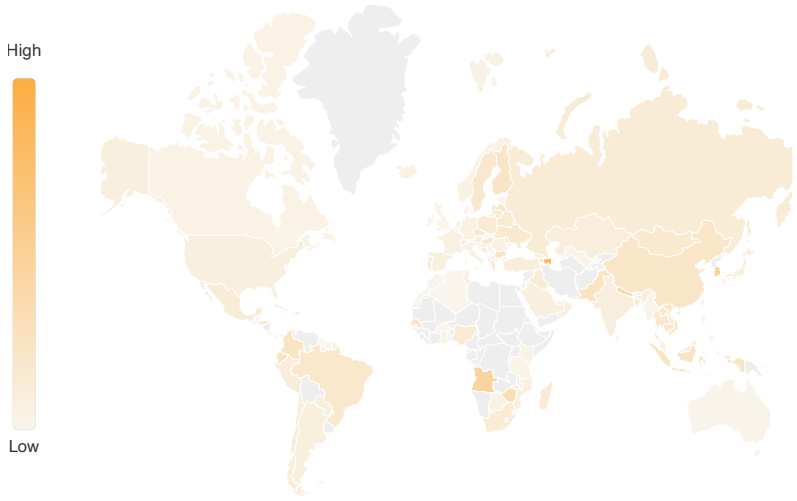
By contrast, launching most network-layer DDoS attacks does not require a handshake. Attackers can spoof the source IP address in order to obfuscate the attack source and introduce randomness into the attack properties. Techniques like this can make it harder for simple DDoS protection systems to block the attack. 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 data center locations where the traffic was ingested (and not by the potentially spoofed source IP) to get an understanding of where the attacks originated 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 backhauled and routed via various Internet service providers and countries for reasons that can vary from cost reduction to congestion and failure management.

In Q2, Palestine jumped from the second to the first place as the Cloudflare location with the highest percentage of network-layer DDoS attacks. Following Palestine was Azerbaijan, South Korea, and Angola.



*Source: https://radar.cloudflare.com/notebooks/ddos-2022-q2



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

Attack vectors

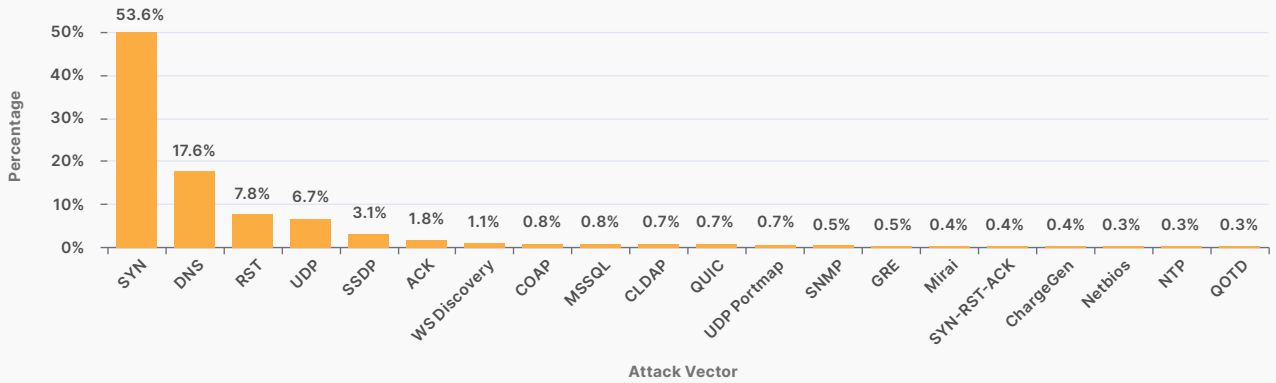
In Q2, DNS attacks increased, making it the second-most common attack vector.

An attack vector is the method that an attacker uses to launch an attack (e.g. the IP protocol, packet attributes, flooding methods, and other criteria).

In Q2, SYN floods comprised 53% of all network-layer attacks. SYN floods abuse the initial connection request of the stateful TCP handshake. During this initial connection request, servers don't have any context about the new TCP connection and cannot mitigate a flood of initial connection requests. This allows the attacker to consume an unprotected server's resources.

Following SYN floods, attacks targeting DNS infrastructure ranked second, followed by RST floods abusing TCP connection flow and generic attacks over UDP.

Network-layer DDoS attacks - distribution by top attack vectors*



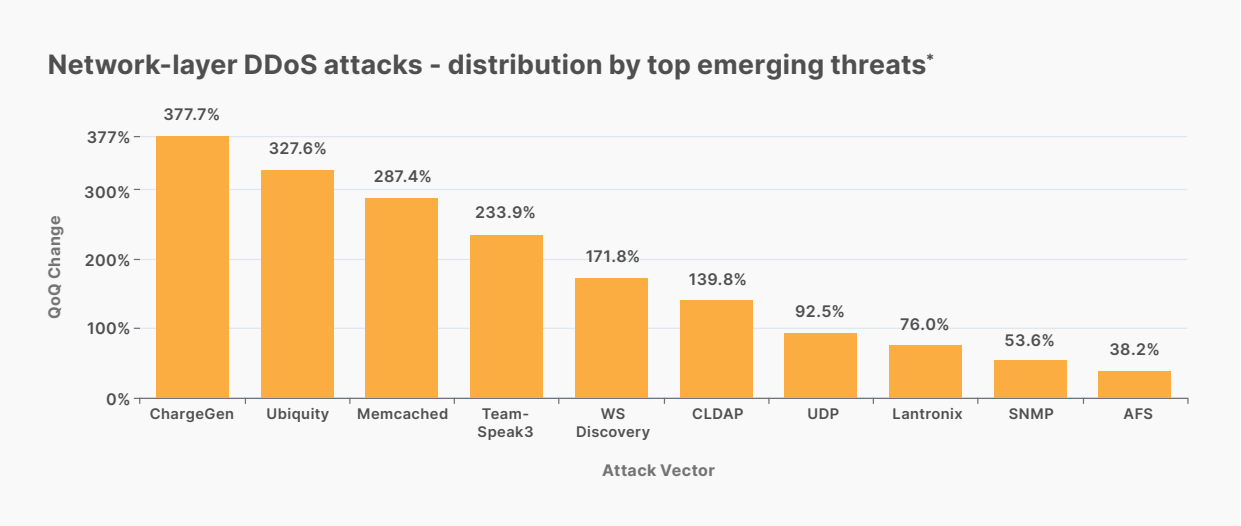
*Source: https://radar.cloudflare.com/notebooks/ddos-2022-q2

Emerging threats

In Q2, the top emerging threats included attacks over CHARGEN, Ubiquiti, and Memcached.

Identifying the top attack vectors helps organizations better understand the threat landscape and, in turn, improve their security posture. Similarly, learning about emerging threats — even those that may not yet account for a significant portion of attacks — can help organizations proactively protect their networks and data.

In Q2, the top emerging threats were amplification attacks abusing the character generator protocol (CHARGEN), amplification attacks reflecting traffic off of exposed Ubiquiti devices, and the notorious Memcached attack.



Abusing the CHARGEN protocol to launch amplification attacks

In Q2, attacks abusing the CHARGEN protocol increased by 378% QoQ.

Initially defined in RFC 864 (1983), the character generator protocol (CHARGEN) is a service of the Internet Protocol Suite that generates characters arbitrarily and doesn't stop sending them to the client until the client closes the connection. While CHARGEN was initially developed to assist with testing and debugging, it is more frequently used to generate amplification/reflection attacks.

In an amplification/reflection attack, an attacker spoofs the source IP of their victim and forces supporting servers around the world to direct a stream of arbitrary characters "back" to the victim's servers. Given enough simultaneous CHARGEN streams, the victim's servers (if unprotected) are flooded with malicious traffic and are unable to cope with legitimate traffic — resulting in a denial-of-service event for users.

*Source: https://radar.cloudflare.com/notebooks/ddos-2022-q2

Amplification attacks exploiting the Ubiquiti discovery protocol

In Q2, attacks over Ubiquiti increased by 327% QoQ.

Ubiquiti is a US-based company that provides networking and Internet of Things (IoT) devices for consumers and businesses. Ubiquiti devices can be discovered on a network using the Ubiquiti discovery protocol over UDP/TCP port 10001.

Similar to the CHARGEN attack vector, attackers spoof the source IP and spray IP addresses that have port 10001 open. If the volume is sufficient, those IPs then respond to the victim and flood it with malicious traffic.

Memcached DDoS attacks

In Q2, Memcached DDoS attacks increased by 287% QoQ.

Memcached is a database caching system for speeding up websites and networks. Similar to CHARGEN and Ubiquiti, Memcached servers that support UDP can be abused to launch amplification/reflection DDoS attacks. In a Memcached attack, the attacker requests content from the caching system and spoofs the victim's IP address as the source IP inside the UDP packets. The victim is then flooded with the Memcached responses, which can be amplified by a factor of up to 51,200 times.

Network-layer DDoS attacks by attack rate

Volumetric attacks of over 100 Gbps increased by 8% QoQ.

There are different ways of measuring the size of an L3/4 DDoS attack.

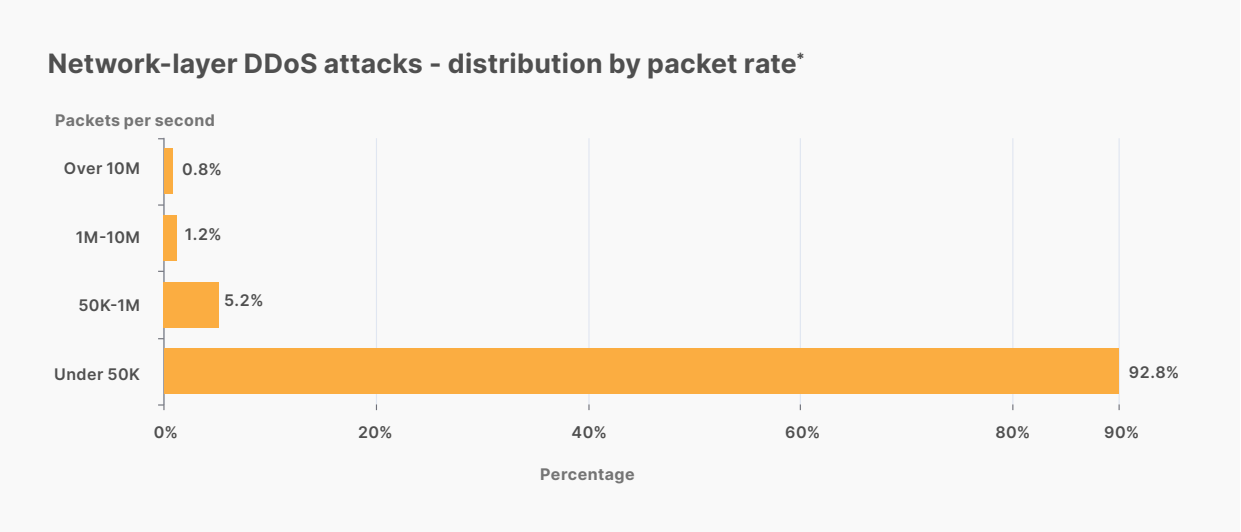
One way is by measuring the volume of traffic it delivers — in other words, the bit rate (specifically, terabits per second or gigabits per second). Attacks with high bit rates attempt to cause a denial-of-service event by clogging the Internet link.

Another way of measuring these attacks is by tracking the number of packets it delivers — also known as the packet rate (specifically, millions of packets per second). Attacks with high packet rates attempt to overwhelm the servers, routers, or other inline hardware appliances. These devices dedicate a certain amount of memory and computation power to process each packet, so by bombarding it with many packets, the appliance may be left with no further processing resources. In such a case, packets are "dropped," meaning the appliance is unable to process them. For users, this results in service disruptions and denial-of-service events.

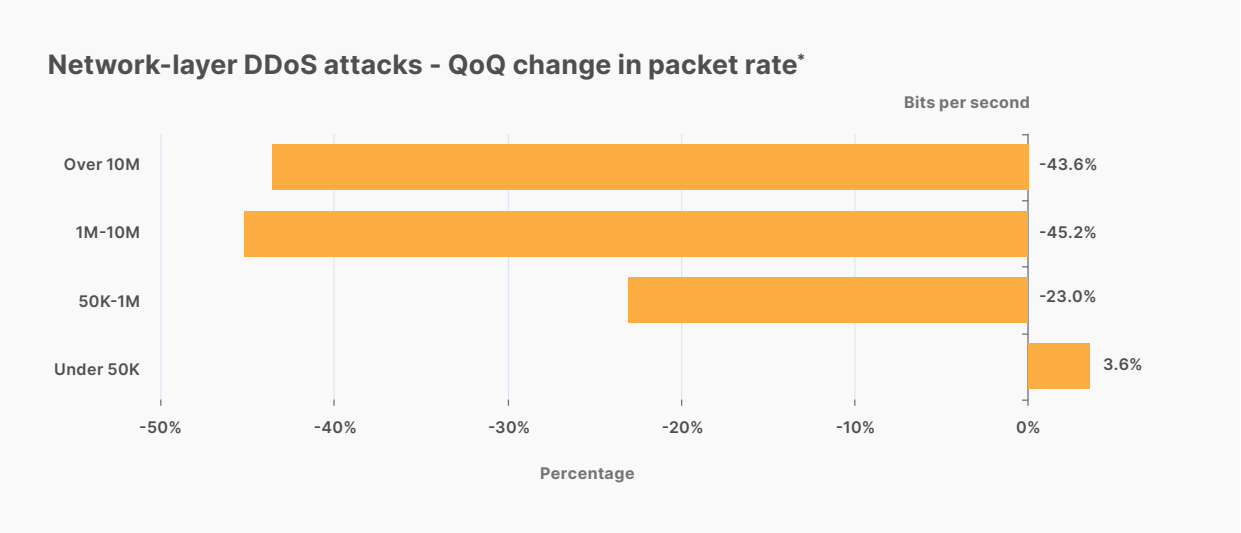
*Source: https://radar.cloudflare.com/notebooks/ddos-2022-q2

Distribution by packet rate

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



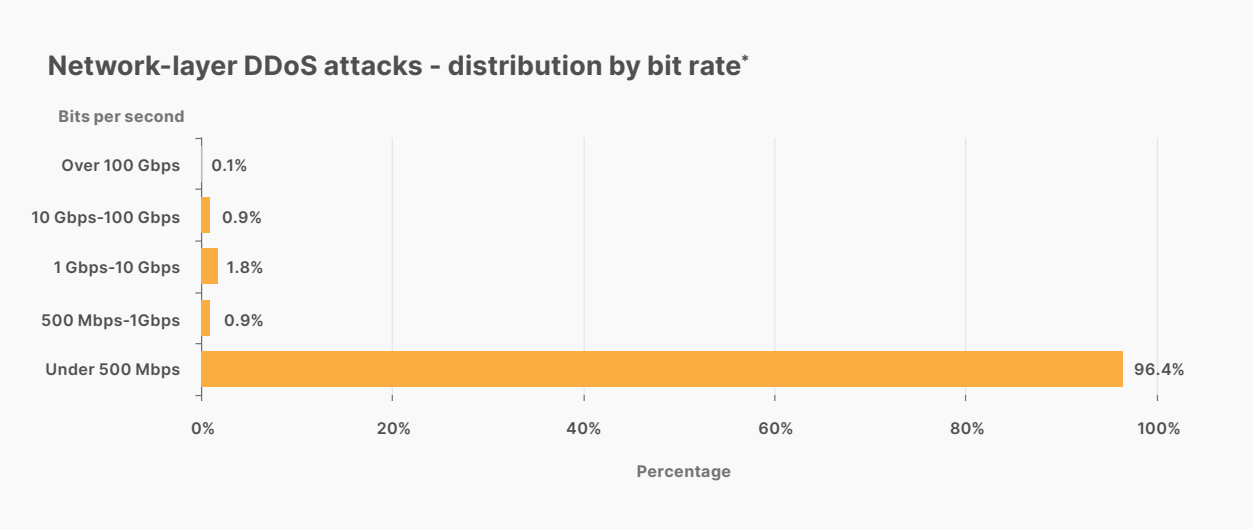
When we look at the changes in the attack sizes, we can see that packet-intensive attacks above 50 kpps decreased in Q2, resulting in an increase of 4% in small attacks.



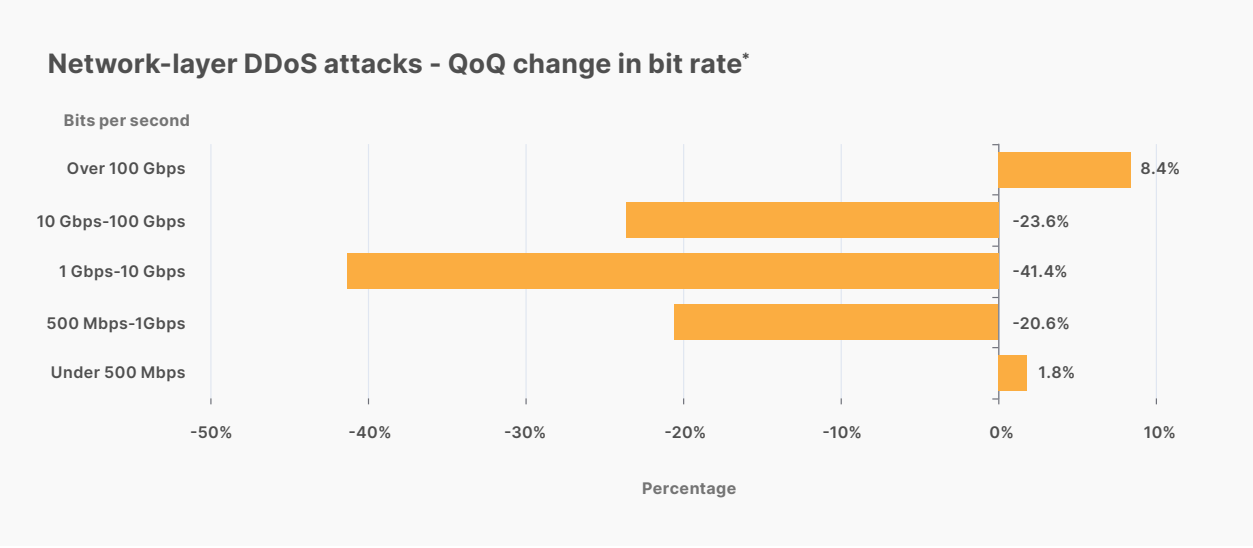
*Source: https://radar.cloudflare.com/notebooks/ddos-2022-q2

Distribution by bitrate

In the second quarter, most of the network-layer DDoS attacks remained below 500 Mbps. This is still small in comparison to the scale of Cloudflare's network, but can quickly shut down unprotected Internet properties with less capacity or, at the very least, cause congestion for a standard gigabit Ethernet connection.



Interestingly, large attacks between 500 Mbps and 100 Gbps decreased by 20-40% QoQ, but volumetric attacks above 100 Gbps increased by 8%.



*Source: https://radar.cloudflare.com/notebooks/ddos-2022-q2

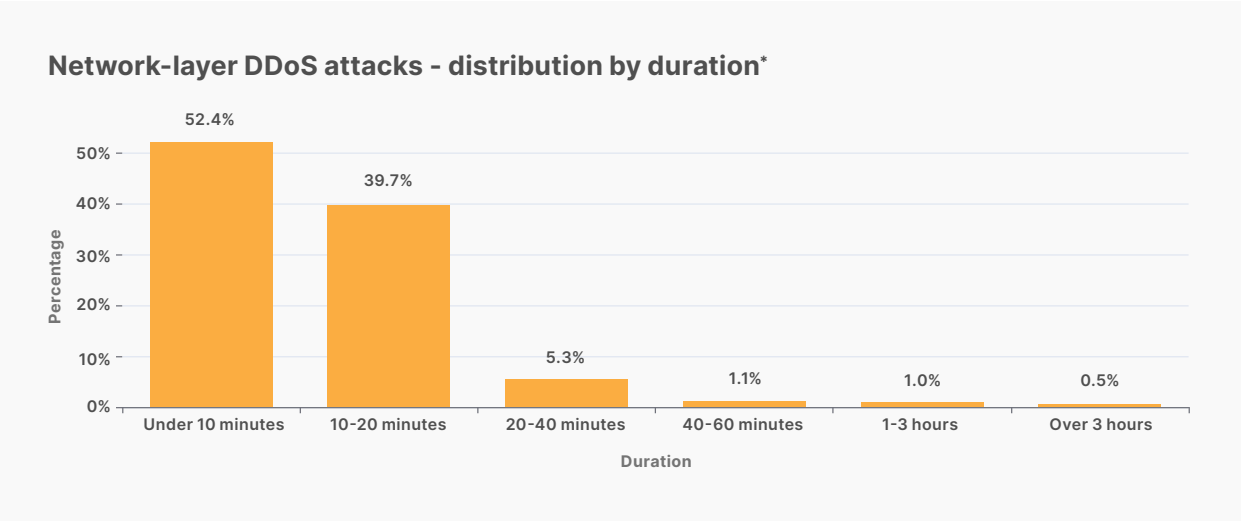
Network-layer DDoS attacks by duration

In Q2, attacks lasting over three hours increased by 9%.

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

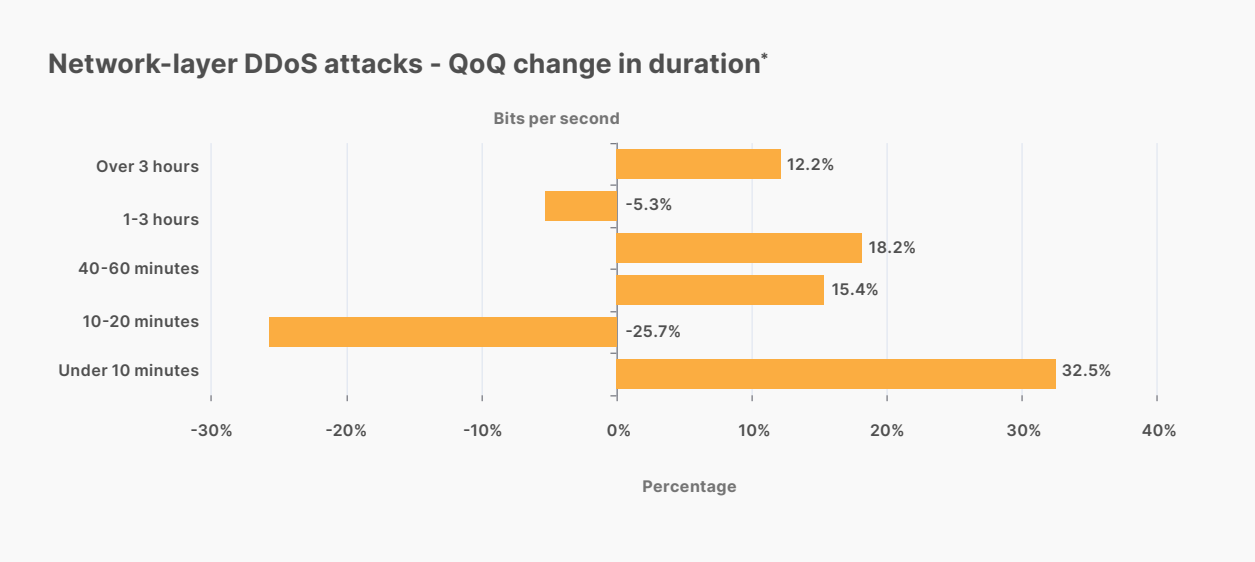
In Q2, 52% of network-layer DDoS attacks lasted less than 10 minutes. Another 40% lasted 10-20 minutes. The remaining 8% of attacks ranged from 20 minutes to over three hours.

An important note: Even if an attack lasts only a few minutes, a successful attack could have repercussions that last well beyond the initial attack duration. IT personnel responding to a successful DDoS attack may spend hours — even days — restoring their services. Disruptions of that magnitude will rarely go unnoticed by end users. Often, successful DDoS attacks result in a significant loss of revenue and may lead to customer attrition.



While most of the attacks recorded in Q2 were short-lived, we saw an increase of over 15% in attacks ranging between 20-60 minutes, and a 12% increase in attacks lasting more than three hours.

*Source: https://radar.cloudflare.com/notebooks/ddos-2022-q2



Short attacks can easily go undetected, especially burst attacks. Burst attacks can bombard a target with a significant number of packets, bytes, or requests in a matter of seconds. When this happens, DDoS protection services that rely on manual mitigation have almost no chance at mitigating the attack in a timely manner. 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 redirects traffic to a DDoS provider only when an attack has already been detected, is also insufficient. In most cases, the attack will already be over before the traffic routes to the on-demand DDoS provider.

For these reasons, we recommend that companies use automated, always-on DDoS protection services that analyze traffic and apply real-time fingerprinting fast enough to block short-lived attacks.

*Source: https://radar.cloudflare.com/notebooks/ddos-2022-q2

Conclusion

The second quarter of 2022 saw a continuation of DDoS attacks across a wide range of organizations.

As the war in Ukraine continued, DDoS attacks attempted to stop the spread of information by targeting Ukrainian broadcast media and communications-related organizations. On the opposite side of the war, banking and financial services became the most attacked industry in Russia.

Outside of the Russia-Ukraine conflict, a new wave of ransom DDoS attacks peaked at the highest levels of the year so far. Application-layer DDoS attacks increased year-over-year, with most attacks targeting the United States and the aviation and aerospace industry. Network-layer DDoS attacks also increased year-over-year, with a notable increase in larger attacks (100 Gbps) and attacks lasting more than three hours. For network-layer attacks, the top targeted industry was telecommunications and the most targeted country was the United States.

It is clear that DDoS attacks are increasing in scale, sophistication, and duration. Just as organizations around the world have benefited from easier, cheaper and faster compute, storage, and networking capabilities — so have attackers. We continue to see record-breaking attacks each quarter, including a 26 million request per second HTTPS DDoS attack that Cloudflare stopped recently.

As part of the Cloudflare mission, we've been providing unmetered and unlimited DDoS protection for free to all of our application services customers since 2017. Over the years, it has become increasingly easier for attackers to launch DDoS attacks. We want to help ensure that it is even easier and cost-effective for organizations of all sizes to protect themselves against DDoS attacks of all kinds.

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

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

REV:BDES-3514.2022JUL18