CLOUDFLARE

THREAT REPORT

DDoS Threat Landscape Report

DDoS Trends from Q4 2022

Content

Executive Summary

Welcome to Cloudflare's quarterly distributed denial-of-service (DDoS) report for the fourth and final quarter of 2022. This report uncovers insights and trends about the DDoS threat landscape observed across Cloudflare's global network from October to December of 2022.

As the year drew to a close and billions around the world celebrated holidays, DDoS attacks persisted. We observed these attacks increase in size, frequency, and sophistication while attempting to disrupt our way of life – heavily targeting industries such as Aviation and Aerospace, Gaming/Gambling, Financial Services, and Education Management.

Cloudflare's automated DDoS defenses mitigated millions of attacks in Q4 alone. During the last week of November, we automatically detected and mitigated a 1 terabit per second (Tbps) DDoS attack targeted at a Korean-based hosting provider.

We've taken all of those attempted attacks, aggregated, analyzed, and prepared the bottom lines to help you better understand 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 to better prepare for current and emerging DDoS threats.

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

Report Highlights

Global DDoS attack trends

Despite a year-long decline, the amount of HTTP DDoS attack traffic still increased by 79% year-over-year (YoY) in Q4 2022. While most of these attacks were small, our network consistently observed terabit-strong DDoS attacks in the hundreds of millions of packets per second. We also saw HTTP DDoS attacks peaking in the tens of millions of requests per second, launched by sophisticated botnets.

Here are some of the other trends that emerged:

Volumetric attacks surged

- The number of attacks exceeding rates of 100 gigabits per second (Gbps) grew by 67% quarter-over-quarter (QoQ)

Ransom DDoS threats persisted

- Over 16% of respondents reported receiving a threat or ransom demand as part of a DDoS attack

Attack durations increased

- Attacks lasting 1-3 hours increased by 349% QoQ, while attacks lasting over three hours increased by 87% QoQ

Industries most targeted by DDoS attacks

- Aviation/Aerospace was the most-targeted industry for application-layer DDoS attacks, with attacks making up 35% of all web traffic to those Internet properties
- Education Management was the most-targeted industry for network-layer DDoS attacks, with attacks making up 92% of all web traffic
- Other highly-targeted industries for network-layer attacks included Information Technology & Services (74%), Public Relations and Communications (73%) and Finance (31%)

Source and targets of DDoS attacks

- Network-layer attack traffic originated from Botswana (52% of all recorded traffic), Azerbaijan (~40%), Paraguay (~40%), and Palestine (~40%)
- Network-layer attacks were directed toward China (93% of network-layer traffic), Lithuania (over 86%), and Finland (80%)
- Application-layer attacks were directed toward Georgia (42% of all traffic), Belize (28%), San Marino (almost 20%), and Libya (almost 20%)

Please 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.*

Sign up for the DDoS trends webinar to learn more about these emerging threats and how to defend against them.

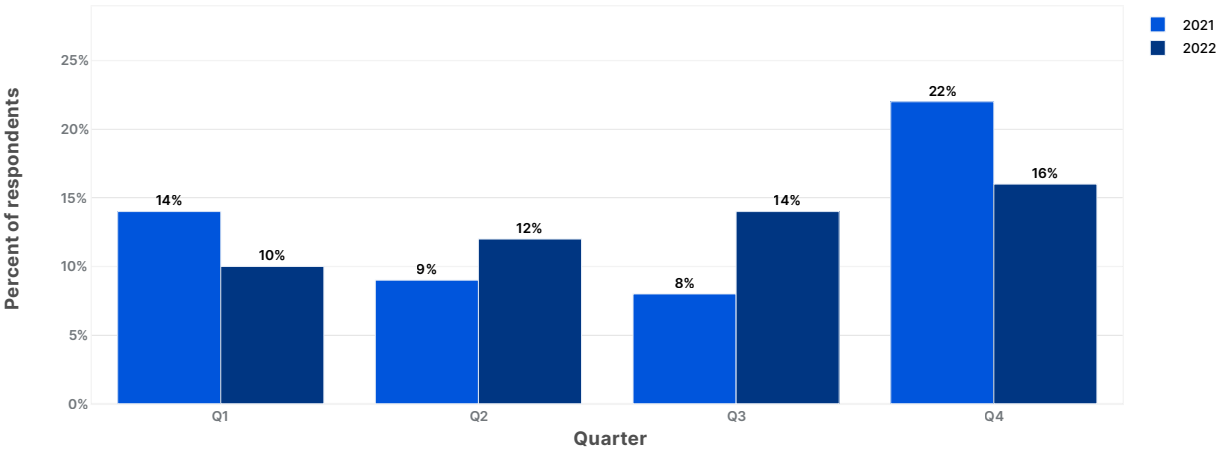
Ransom DDoS attacks

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, an attacker floods their victims' web properties with enough malicious traffic to disrupt their Internet services. Then, they demand a ransom payment — usually in the form of Bitcoin — to stop the attack. In some cases, the attacker sends a ransom note before carrying out the DDoS attack, relying on the threat of an attack to collect fraudulent payment from targeted organizations or individuals.

In Q4, 16% of surveyed Cloudflare customers 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.

Distribution of ransom DDoS attacks: 2021 and 2022 by quarter

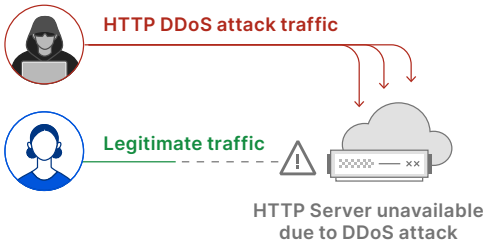


How ransom DDoS attack reports are calculated:

Cloudflare's systems constantly analyze traffic and automatically mitigate DDoS attacks as soon as they are detected. For the past two years, we have sent automated surveys to each targeted customer to help us better understand the nature of these attacks and the success of Cloudflare's mitigation services, averaging roughly 187 responses per quarter. One of the questions in the survey asks respondents whether they received a threat or a ransom note during the attack. These responses are used to calculate the percentage of reported ransom DDoS attacks.

Application-layer DDoS attacks landscape

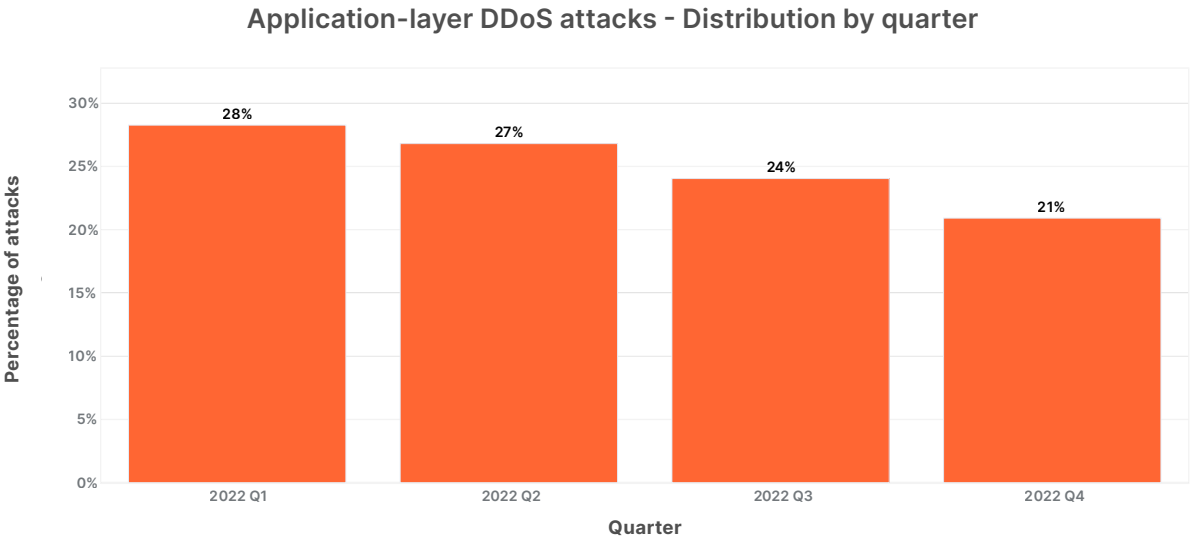
Application-layer DDoS attacks, specifically HTTP/S DDoS attacks, are cyber attacks that disrupt web servers by bombarding them with more requests than they can process. This often causes the server to drop legitimate user requests, resulting in degraded performance or outages.



A diagram of an application-layer DDoS attack denying service to legitimate users

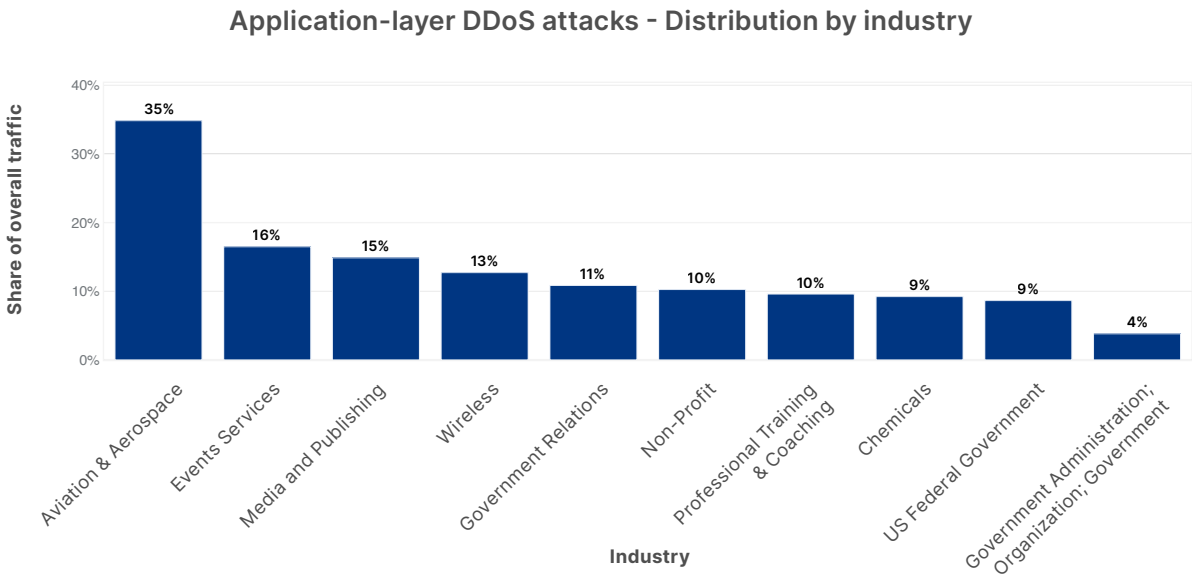
Application-layer DDoS attack trends

As seen in the graph below, HTTP DDoS attacks decreased over each quarter of 2022, but still represented a 79% increase YoY compared to Q4 2021.

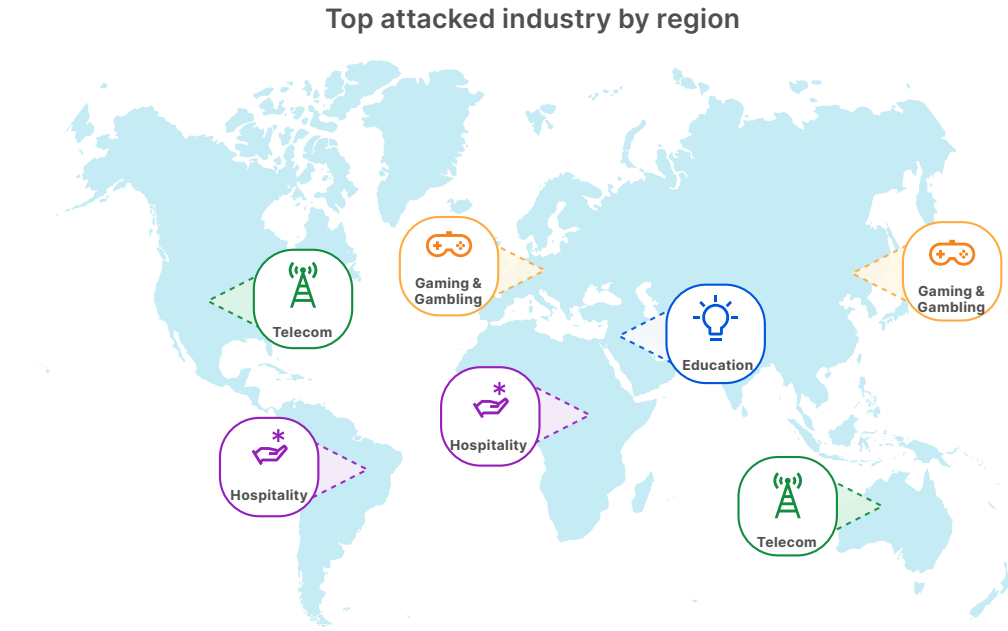


Target industries of application-layer DDoS attacks

As holiday travel spiked toward the end of the year, Aviation and Aerospace emerged as the most attacked industry, with HTTP DDoS attacks making up ~35% of all web traffic to those Internet properties. The second-most targeted industry was Events Services, with HTTP DDoS attacks constituting over 16% of its traffic. Following were Media and Publishing, Wireless, Government Relations, and Nonprofits. To learn more about how Cloudflare protects nonprofit and human rights organizations, read our recent Impact Report.



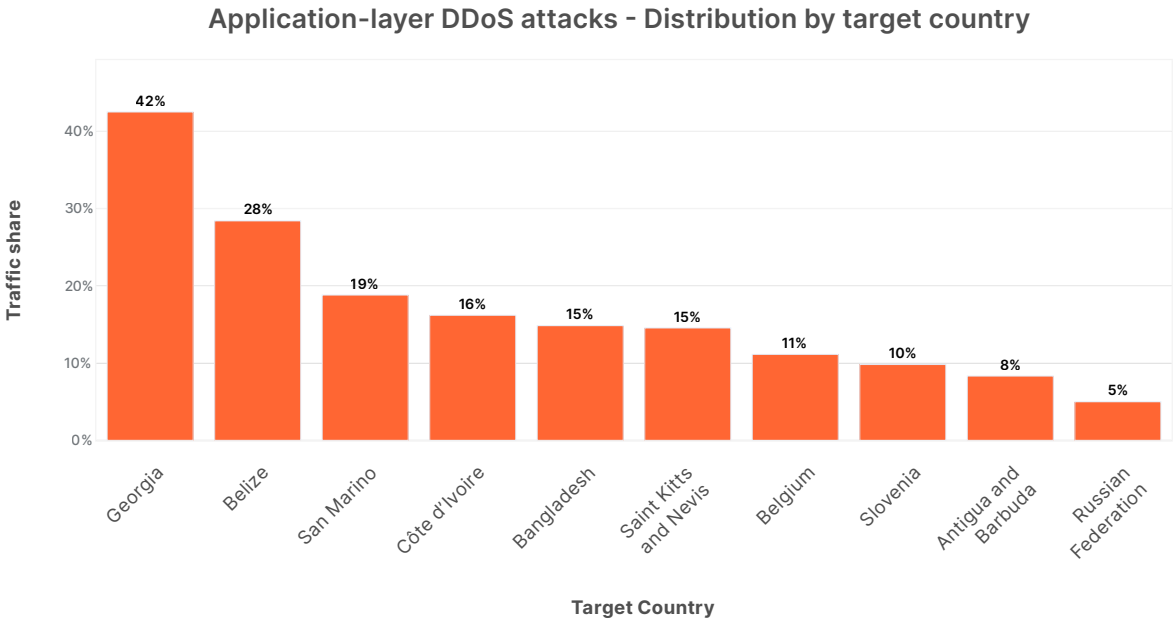
Breaking down the attacks by region, the Telecommunications industry was the most targeted in North America and Oceania.* In South America and Africa, the Hospitality industry was the most targeted. In Europe and Asia, Gaming & Gambling industries were the most targeted. And in the Middle East, the Education industry saw the most attacks.



Excluding generic industry buckets like Internet and Software Services

Target countries of application-layer DDoS attacks

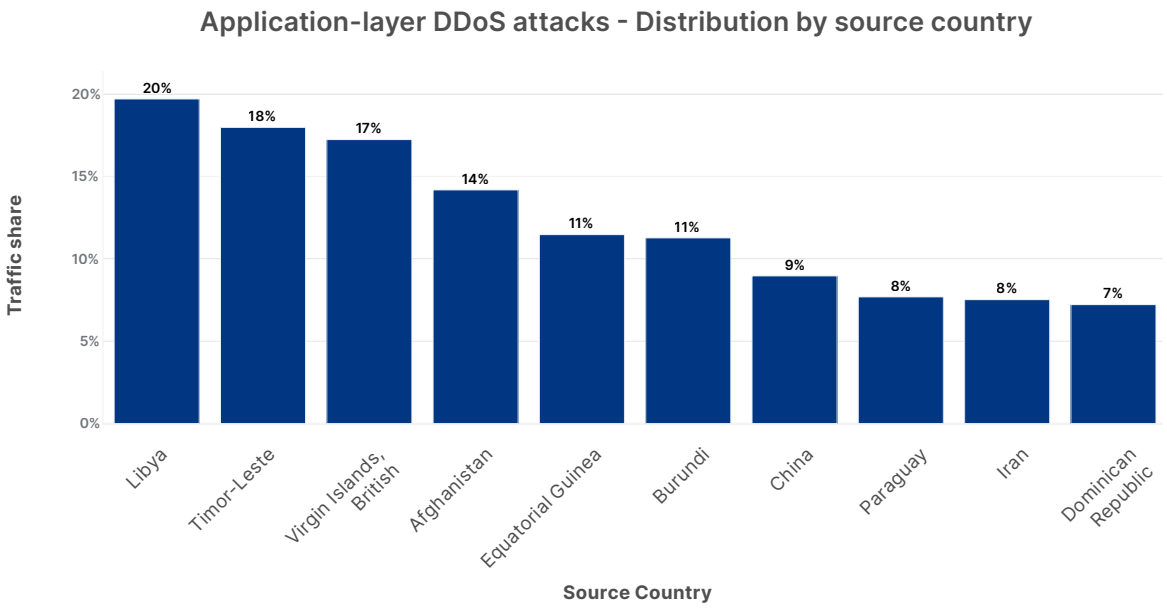
Grouping attacks by customer billing addresses helps us understand which countries are more frequently attacked. In Q4, DDoS attack traffic made up 42%+ of all traffic to Georgian-based HTTP applications. In second place, DDoS attacks represented almost a third of all traffic to Belize-based customers, followed by San Marino, with just below 20%.



Source of application-layer DDoS attacks

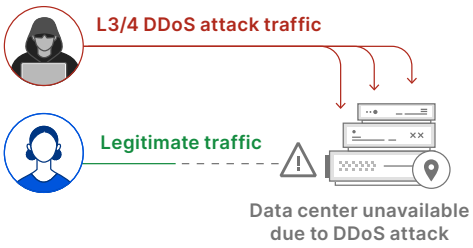
As part of our attack trend analysis, we observe the countries that send and receive the highest volume of attack traffic. However, it is worth noting that DDoS attacks are often launched remotely in an attempt to disguise the true location of the attacker. Top source countries are more often indicators that there are botnet nodes operating from within that country, in the form of compromised servers or IoT devices.

In Q4, HTTP DDoS attacks made up almost 20% of all HTTP traffic from Libya. Other top countries included Timor-Leste (18%), the British Virgin Islands (17%), and Afghanistan (14%).



Network-layer DDoS attacks

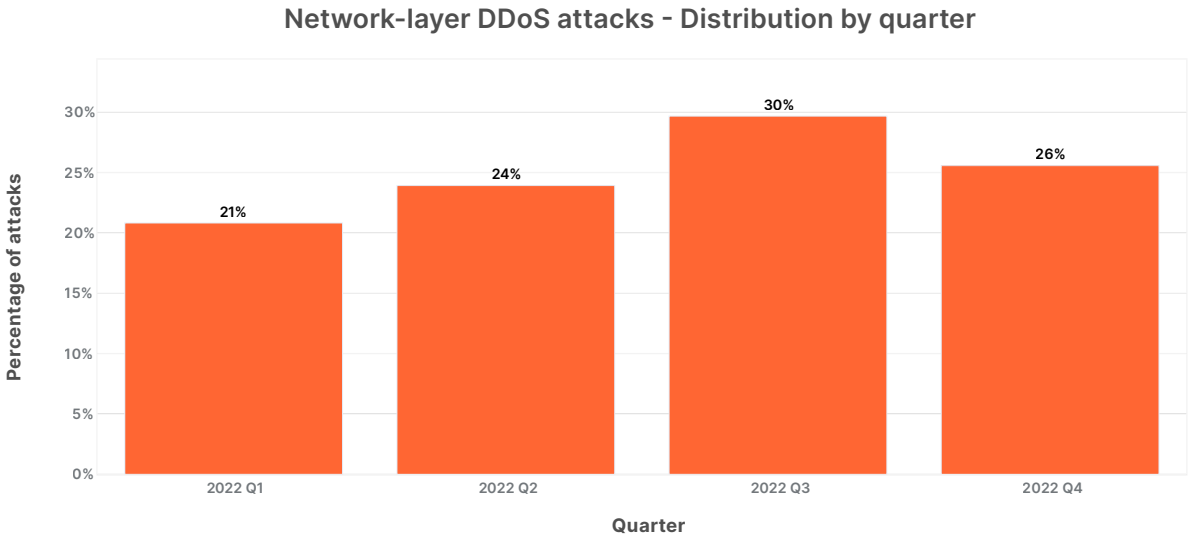
As the name suggests, network-layer DDoS attacks overwhelm network infrastructure. While application-layer DDoS attacks (also referred to as bit-intensive attacks) attempt to clog up the Internet connection to cause a denial-of-service event, network-layer attacks (or packet-intensive attacks) attempt to take down in-line devices, including routers, servers, and the Internet link itself. If an attack sends more packets than servers or other in-line appliances can handle, they may not be able to process legitimate user traffic, which may result in degraded performance or a crash.



A diagram of an network-layer DDoS attack denying service to legitimate users

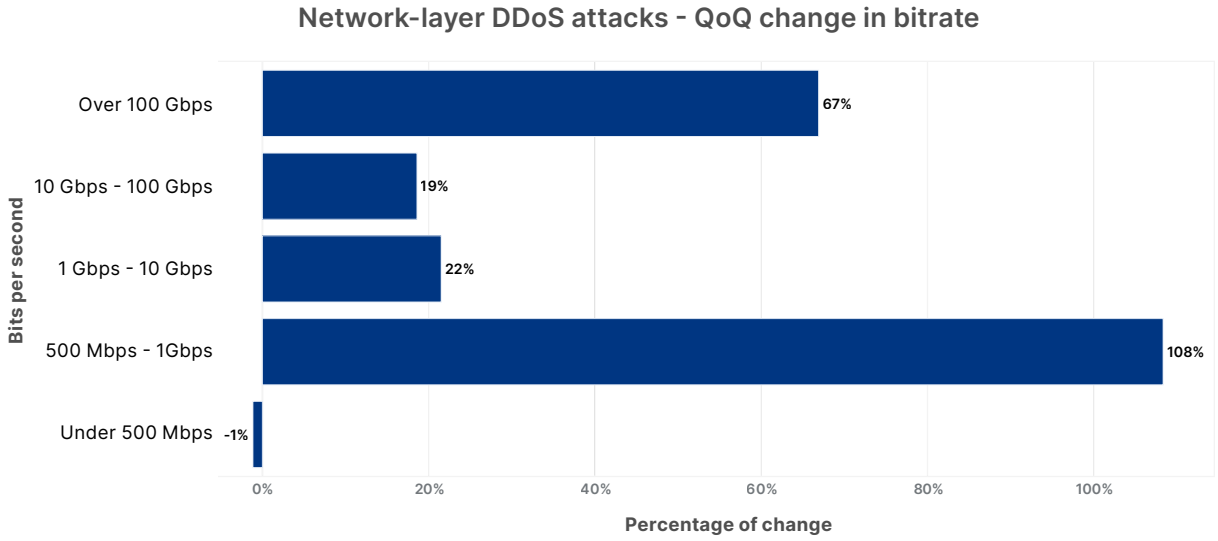
Network-layer DDoS attack trends

After a year of steady increases in network-layer DDoS attacks, the volume of attacks decreased by 14% QoQ and 13% YoY in Q4 2022. Although we do not have any definitive data on the reasons for this decline, we have seen a recent uptick in headlines claiming takedowns of DDoS-for-hire operations. These spikes may also be indicative of organizations proactively implementing DDoS mitigation systems to protect their networks.

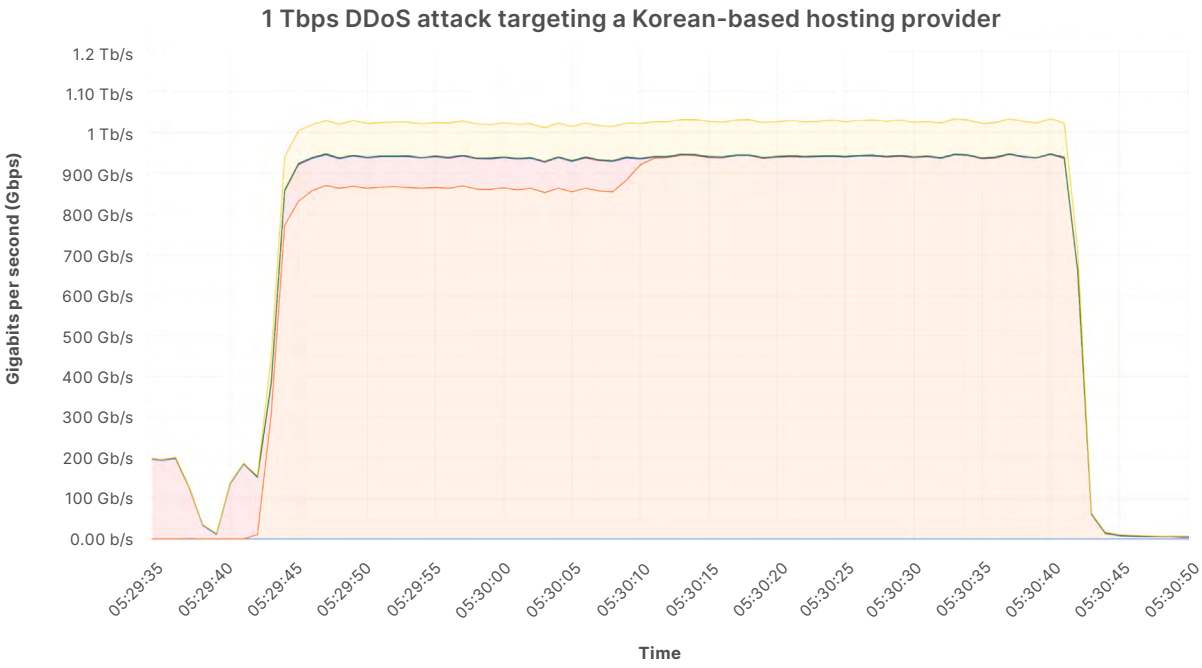


Network-layer DDoS attack rates

While the vast majority of network-layer 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.

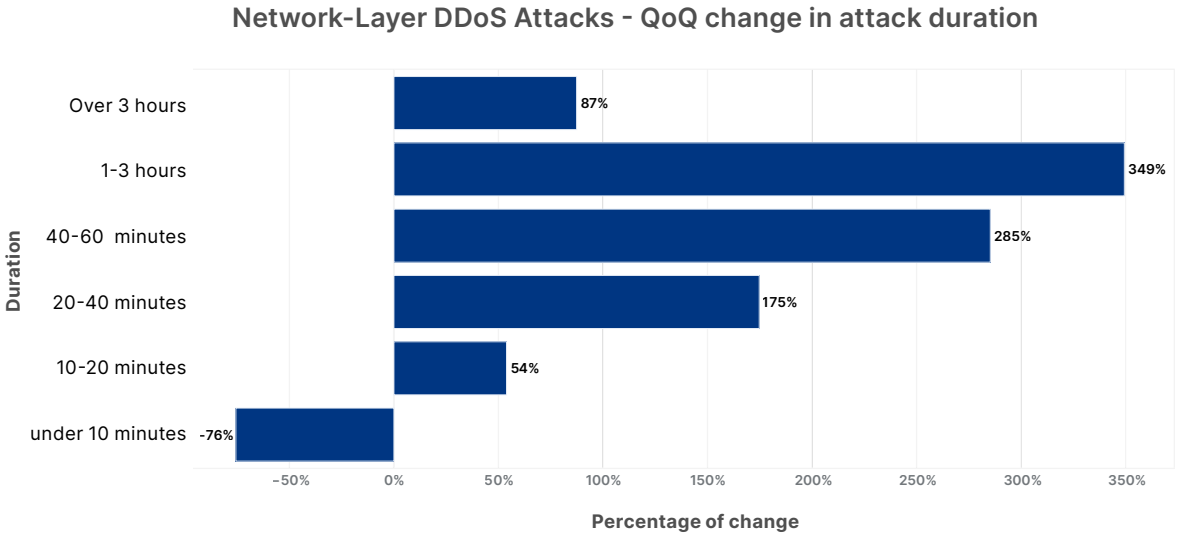


During the last week of November, we observed a 1 Tbps DDoS attack targeting a Korean-based hosting provider. The attack — an ACK flood — lasted roughly one minute, and was automatically detected and mitigated with the help of Cloudflare's L3 DDoS protection service, Magic Transit.



Network-layer DDoS attack duration

In Q4, the amount of attacks under 10 minutes decreased by 76% QoQ, while longer attacks increased in frequency. Most notably, attacks lasting 1-3 hours spiked by 349% QoQ and the attacks of three or more hours increased by 87% QoQ.



Network-layer DDoS attack vectors

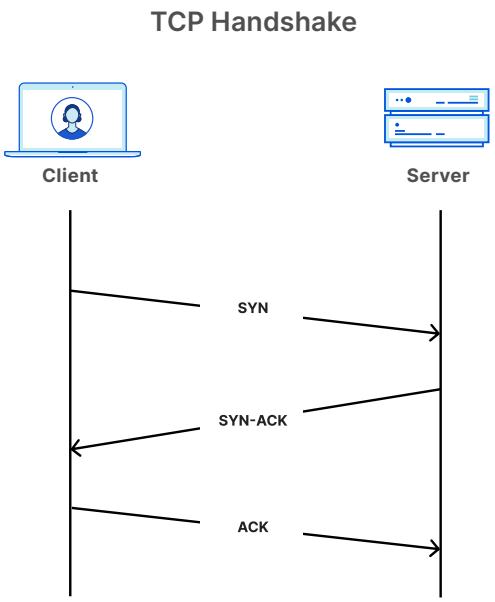
In Q4, the primary attack vector (or method) we observed was SYN floods, which made up almost half of all network-layer DDoS attacks mitigated by Cloudflare.

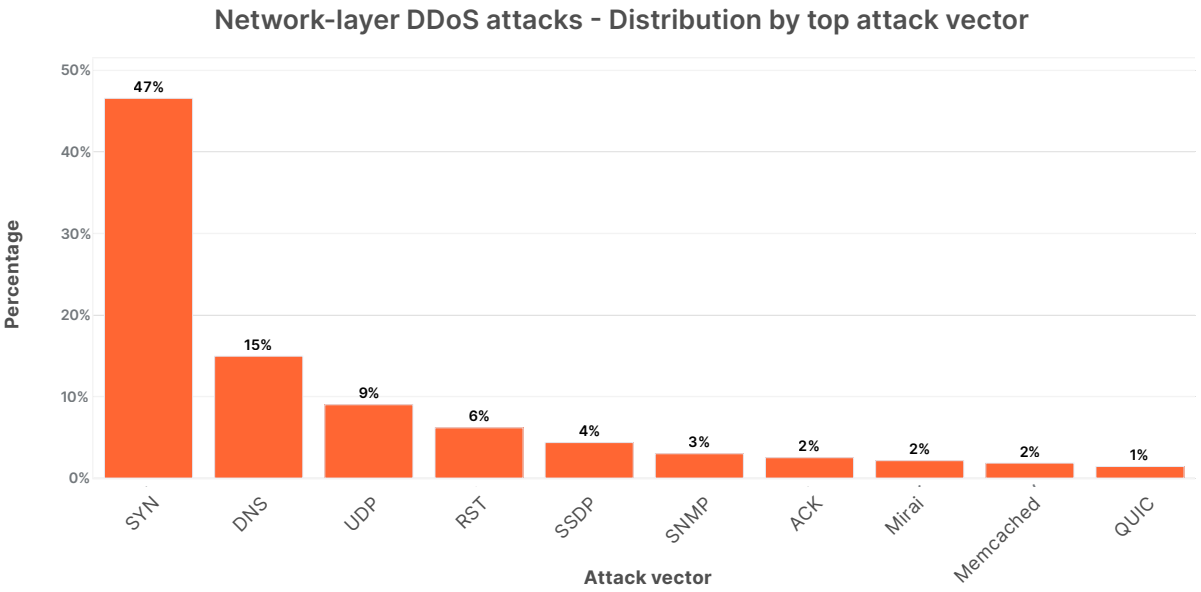
SYN floods are a type of DDoS attack that overwhelms server ports with SYN packets. SYN floods do this by taking advantage of the statefulness of the three-way TCP handshake — which is the primary method of establishing a connection between a server and a client.

For every connection in a TCP handshake, a certain amount of memory is allocated. In a SYN flood attack, 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. The spoofed IP addresses ignore the packets, while the server continues to wait for the ACK packets to complete the handshake. After a while, the server times out and releases those resources.

This attack method swiftly drains the server's resources, rendering it unable to handle legitimate user connections or crash altogether.

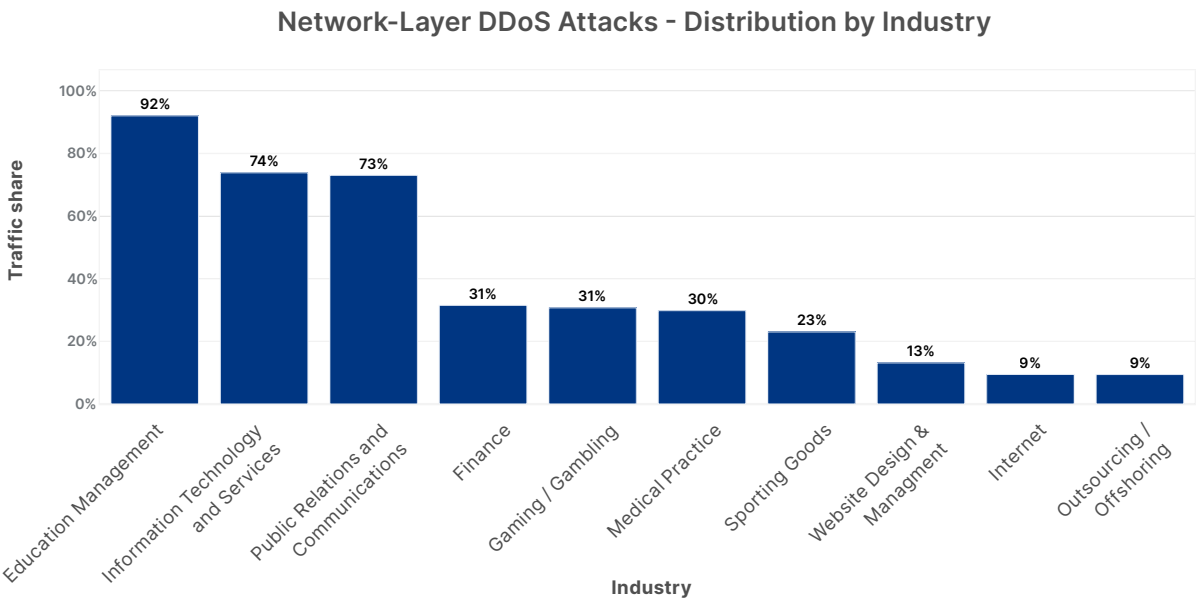
After SYN floods, DNS floods and amplification attacks accounted for ~15% of all network-layer DDoS attacks, while UDP-based DDoS attacks and floods made up another 9%.





Target industries of network-layer DDoS attacks

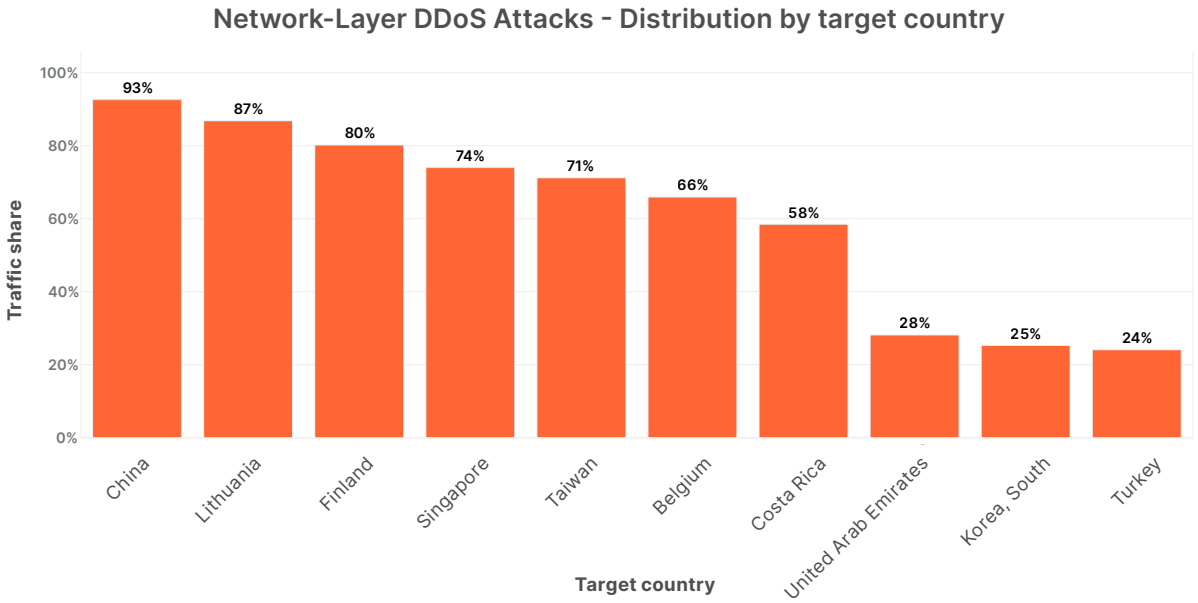
In Q4, the Education Management industry saw the highest percentage of network-layer DDoS attack traffic, at 92%. The Information Technology and Services also saw a significant amount of network-layer DDoS traffic, at 74%, and the Public Relations and Communications industry ranked third at 73%.



Target countries of network-layer DDoS attacks

Grouping attacks by our customers' billing country allows us to track which countries are subject to the highest volume of attacks. In Q4, network DDoS attack traffic made up a staggering 93% of all web traffic to China-based web properties.

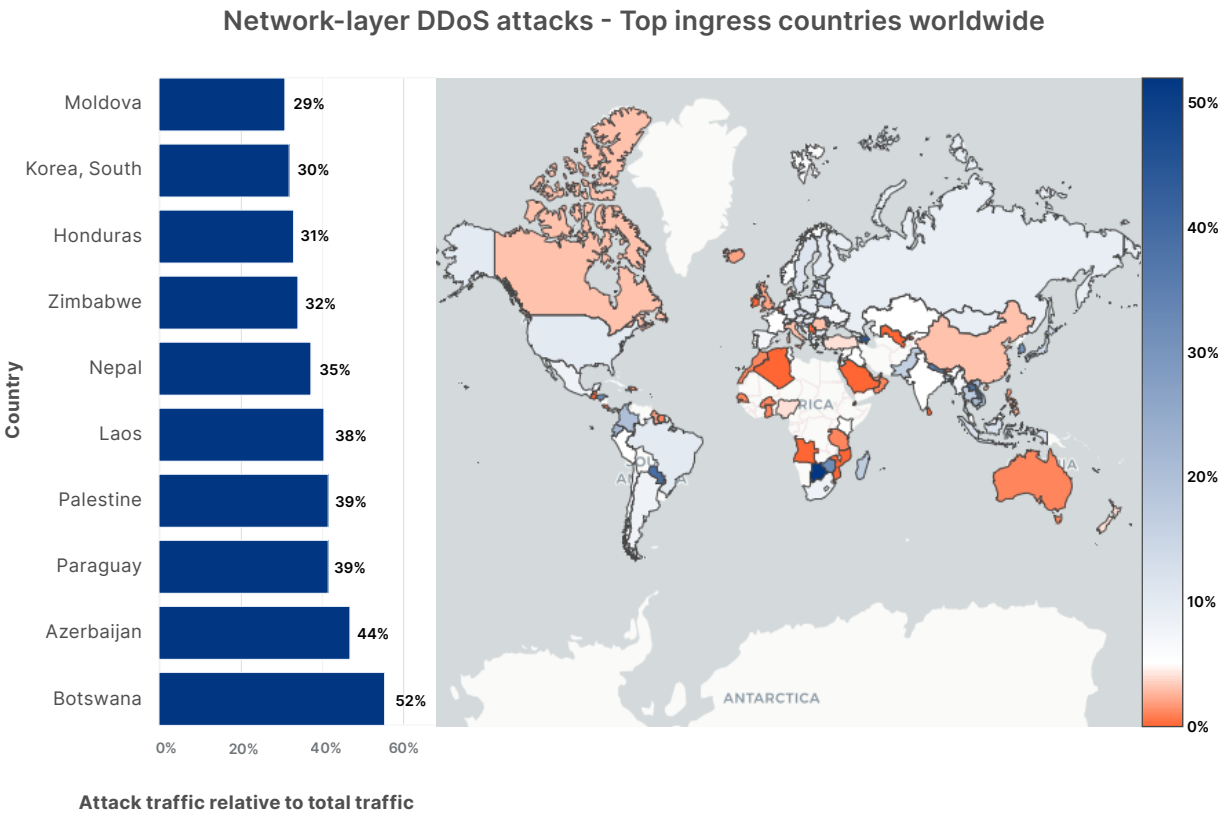
Other countries that were highly targeted by network-layer attacks included Lithuania (87%), Finland (80%), Singapore (74%), and Taiwan (71%).



Source of network-layer DDoS attacks

At the application layer, we observed IP addresses to better understand where attack traffic was originating from. We used this method because at that layer, IP addresses cannot be spoofed. However, in the network layer, source IP addresses can be spoofed. In order to identify where network-layer attacks start, then, we use the location of our data centers to see where the attack packets were ingested.

In Q4, attack traffic accounted for over 52% of the web traffic we ingested in our Botswana-based data center. Other top countries in this category included Azerbaijan (43%), Paraguay (39%), Palestine (39%), Laos (38%), and Nepal (35%).



Note: *Internet service providers may sometimes route traffic differently and can skew results. For example, traffic from China may be hauled through California due to various operational considerations.*

Emerging DDoS treats

In Q4, three DDoS attacks saw a significant spike QoQ: Memcached attacks, SNMP attacks, and VxWorks attacks.

Memcached-based DDoS attacks increased by 1,338% since Q3 2022. Memcached is a database caching system that speeds up websites and networks, but its servers can be abused to launch amplification/reflection DDoS attacks.

These attacks work by requesting content from the caching system and spoofing the victim's IP address as the source IP in the UDP packets. As a result, the victim is flooded with Memcached responses, which can be amplified by a factor of up to 51,200x.

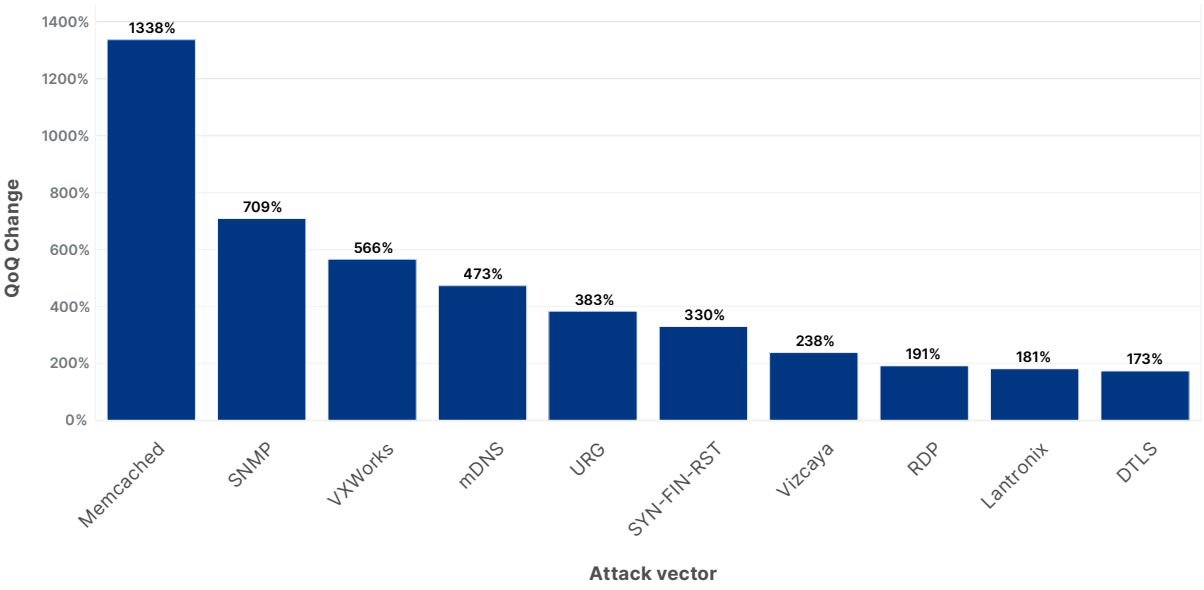
SNMP-based DDoS attacks also jumped considerably, with a 709% spike QoQ. Simple Network Management Protocol (SNMP) is a UDP-based protocol that is often used to discover and manage network devices such as printers, switches, routers, and firewalls that use UDP port 161.

In an SNMP reflection attack, the attacker sends out numerous SNMP queries while spoofing the source IP address in the packet. This allows them to target devices on the network, resulting in a volumetric DDoS attack as the devices attempt to respond to these fraudulent queries.

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 IoT devices. It also is used in networking and security devices like switches, routers, and firewalls.

By default, VxWorks includes an automatically-enabled debug service that can be exploited for DDoS amplification attacks. This exploit (CVE-2010-2965) was exposed as early as 2010 and still presents a persistent threat to targeted devices.

Network-layer DDoS attacks - Distribution by top emerging threats



Conclusion

As 2022 drew to a close, 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 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 Memcashed-based DDoS attacks continuing to increase in both frequency and severity.

Defending against DDoS attacks is critical for organizations of all sizes. While attacks are initiated by humans, they are executed by bots, which are nearly impossible to manually mitigate at scale. Attack detection and mitigation must be automated as much as possible, because relying solely on humans puts defenders at a disadvantage. The breadth of Cloudflare's global network allows us to observe malicious traffic patterns, track emerging threats, and automatically mitigate attacks on behalf of 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. 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.

Cloudflare's mission is to help build a better Internet. And a better Internet is one that is more secure, faster, and reliable for everyone.

Sign up for the DDoS trends webinar to learn more about these emerging DDoS threats and how to defend against them.

Changes to the report methodologies

Since our first DDoS trends report in 2020, we have always used percentages to represent attack traffic (i.e. the percentage of attack traffic out of all web traffic, including legitimate user traffic). We did this to standardize our data, avoid data biases, and be more flexible when incorporating new mitigation system data into our reports.

In this report, we have adjusted our calculations for those percentages in the following categories:

- Target industries of application-layer DDoS attacks
- Target countries of application-layer DDoS attacks
- Source of application-layer DDoS attacks
- Target industries of network-layer DDoS attacks
- Target countries of network-layer DDoS attacks

Previously, we 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 the target industries and target countries categories, we divided the amount of attack IP packets to a given dimension by the total attack packets to all dimensions.

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

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 standardize our calculation methods throughout the report and improve our data accuracy so it better represents the attack landscape.

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

For example, when using our previous calculations, the top industry targeted by application-layer DDoS attacks was the Gaming/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 method, the Aviation/Aerospace industry came in 12th place, at 0.0065%.

After adjusting our calculations, the Aviation/Aerospace industry ranked first as the most attacked industry, with attacks accounting for 35% of all traffic (attack and non-attack) towards that industry alone. By those same calculations, the Gaming/Gambling industry came in 14th place, at 2.4%.

No other changes were made to the calculations in this report. The Source of network-layer DDoS attacks metrics have used our updated calculation method since our initial report in 2020. 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.

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

REV:BDES-4180.2023JAN20