GCORE

WHITE PAPER

# Gcore Radar

# DDoS Attack Trends

Q1–Q2 2024

August 2024 | gcore.com

# DDoS Attack Trends for Q1–Q2 2024

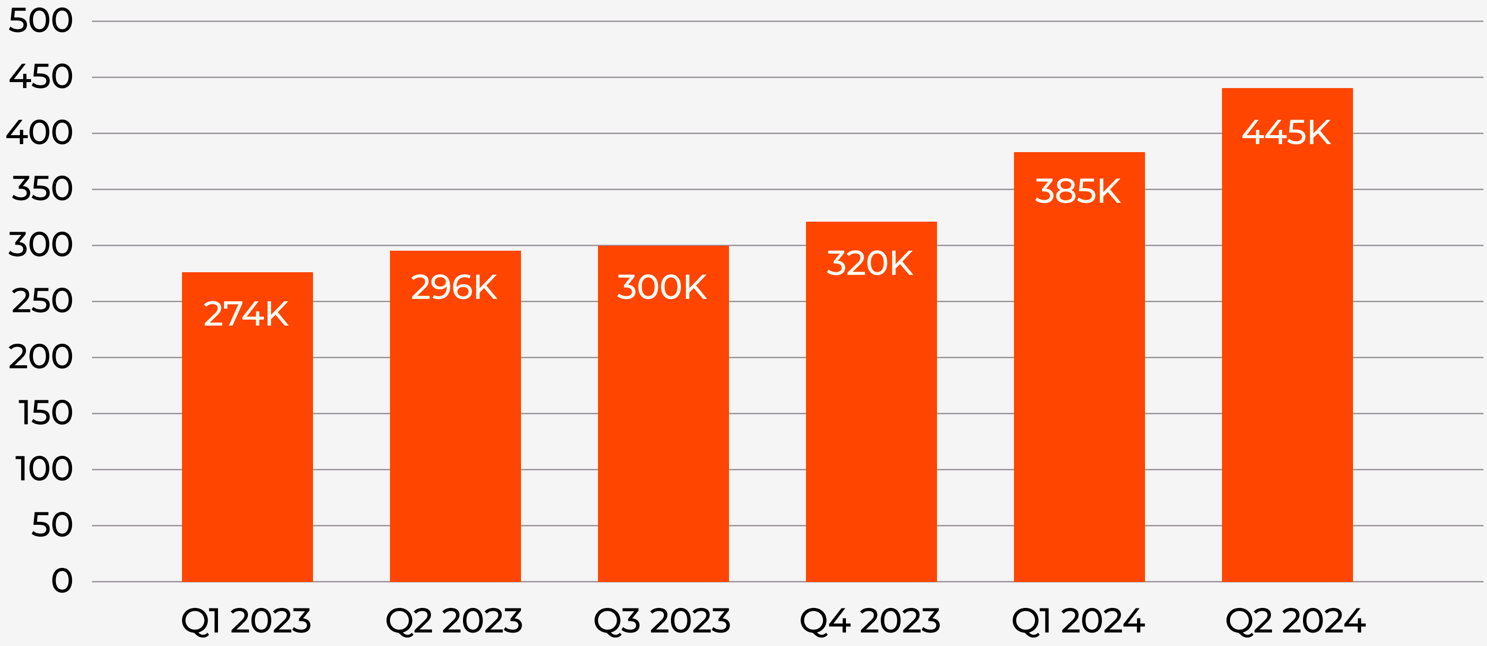
Continuously reviewing evolving DDoS trends is crucial for staying ahead of emerging threats and adapting defense strategies accordingly. The twice-yearly Gcore Radar report reviews DDoS attack data for the previous six months, scrutinizing attack statistics to visualize how attacker behavior and the evolving threat landscape has changed, as observed on Gcore's network.

In this report, we share breakdowns for which industries were most targeted and the types of DDoS attacks that were most common. We compare the first half of 2024 to previous data to identify trends and directions in attack patterns.

Let's start with some standout findings for Q1–Q2 2024.

# Key takeaways

## The number of attacks is growing



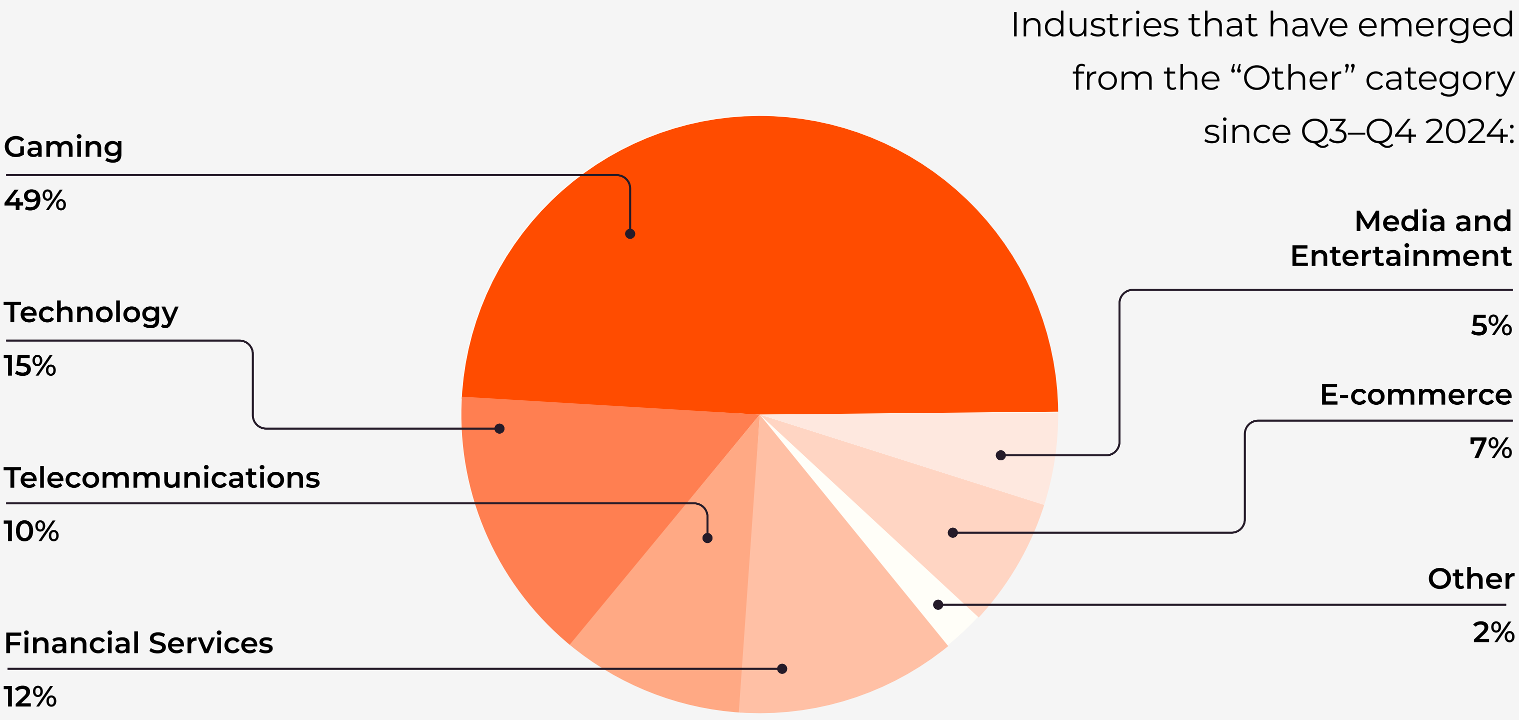
The number of DDoS attacks has increased by 46% compared to the same period 12 months ago (Q1–Q2 2023). Compared to data for the previous six months (Q3–Q4 2023), it has increased by 34%.

## DDoS peak attack power continues to surge

Alarmingly, last year saw a significant rise in peak attack power, shifting the measurement from gigabits per second (Gbps) to terabits per second (Tbps), starting in H2 2023. In the first half of 2024, the most potent attack reached 1.7 Tbps, surpassing the H2 2023 peak of 1.6 Tbps. Even a 0.1 Tbps increase represents a substantial escalation in attackers' ability to overwhelm networks, applications, and digital services. Terabit-level attacks are powerful enough to cripple the most robust infrastructures, leading to complete service outages, disrupt critical applications, and lead to significant financial and reputational damage.

# Which were the most-attacked industries?

## Top attacked industries



## Gaming is still attacked the most

The gaming industry continues to be the most targeted by DDoS attacks, with the share increasing to 49%, up from 46% in Q3–Q4 2023. The competitive nature of online gaming can lead to players, groups, or competitors launching DDoS attacks against opponents to gain an advantage in tournaments or matches. Many games rely on continuous player engagement for monetization through in-game purchases or subscriptions. Downtime directly impacts revenue, making the industry a lucrative target for DDoS attacks.

## The technology industry saw an increase in attacks

Interestingly, an industry that saw a significant increase compared to the previous period was technology. In Q3–Q4 2023, the technology industry was the target for 7% of attacks; in Q1-Q2 2024, this number more than doubled to 15%. Technology providers host critical infrastructure for businesses, including servers, storage, and networking resources. Disrupting these services can significantly impact the numerous organizations relying on them. This makes technology providers an increasingly attractive target for attackers seeking to cause widespread disruption.

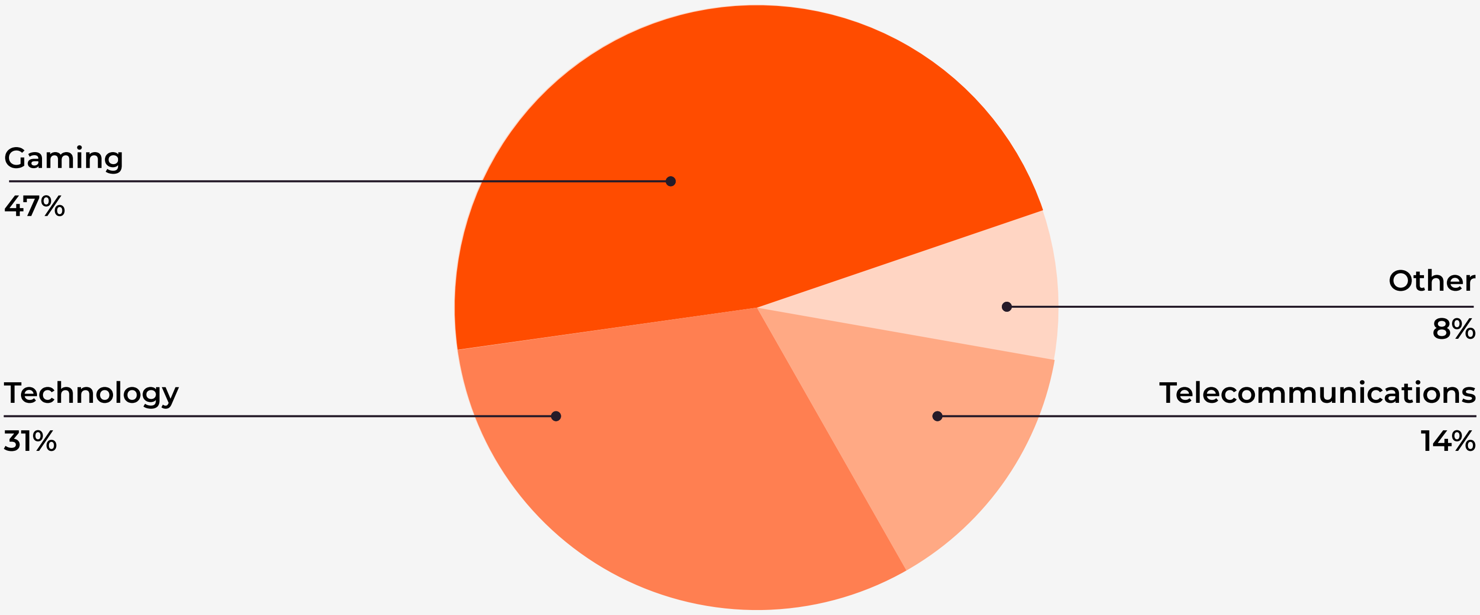
Another reason for the prevalence of attacks on technology platforms is that these environments typically have substantial computational resources, making them attractive for DDoS attacks that leverage these resources to amplify attacks or host malicious activities.

Other industries that were significantly targeted were financial services (12%), telecommunications (10%), and e-commerce (7%). This is unsurprising, given the financial gains from a successful attack on these sectors.

## Network-layer attacks

With a share of 47% of all network-layer DDoS attack bytes, the gaming industry was the most targeted by network-layer DDoS attacks. The combination of high traffic volumes, real-time requirements, competitive dynamics, and significant financial and reputational stakes makes the gaming industry a prime target for network-layer DDoS attacks. As attackers continue to favor this sector, DDoS detection, mitigation, and protection should be a top priority for the gaming industry to avoid disruption, downtime, and revenue loss.

### Top three industries targeted by network-layer attacks (L3-4)



Technology came in second at 31% and telecommunications in third (14%) at the L3–4 layers. Technology platforms support critical business functions and services for many organizations. Disrupting a technology provider can have a cascading effect, impacting multiple businesses and services simultaneously. It can result in significant economic losses for both the provider and its customers. This financial impact can be a motivation for attackers, whether for ransom or competitive sabotage.

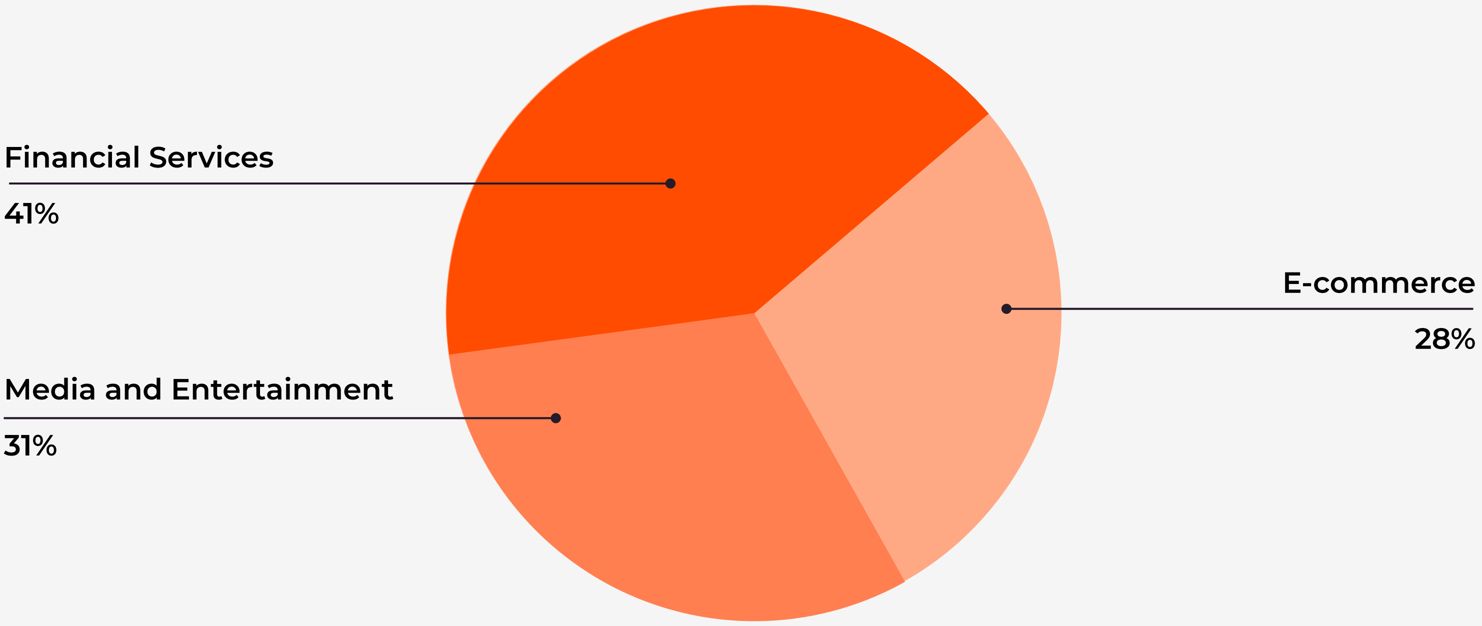
Telecommunications companies provide the backbone of internet connectivity and communication. Disrupting these services can have widespread implications, affecting not just individual users but entire businesses and government functions. These providers serve a wide range of customers, including individual consumers, businesses, and critical infrastructure sectors like financial services and healthcare, and this diversity makes them targets for different types of attackers with various motives.

## Application-layer attacks

The financial services industry is highly targeted for DDoS attacks at the application layer due to their low tolerance for any disruption or downtime and the high potential gains from a successful attack:

- Financial institutions are required to comply with stringent regulations. Downtime or data breaches that follow DDoS attacks can lead to significant regulatory penalties.
- DDoS attacks at the application layer can distract IT staff while other malicious activities, like phishing, fraudulent transactions, or hacking, go unnoticed.

## Top three industries targeted by application-layer attacks (L7)



The combination of high stakes, sensitive transactions, regulatory requirements, and the critical need for maintaining customer trust makes the financial services industry particularly vulnerable and attractive to L7 DDoS attacks.

The next most targeted industry was e-commerce, suffering 28% of application-layer attacks. E-commerce is an attractive industry for DDoS attacks as its websites often handle large volumes of traffic and transactions, especially during peak shopping periods. Disrupting these services can cause significant financial loss and inconvenience.

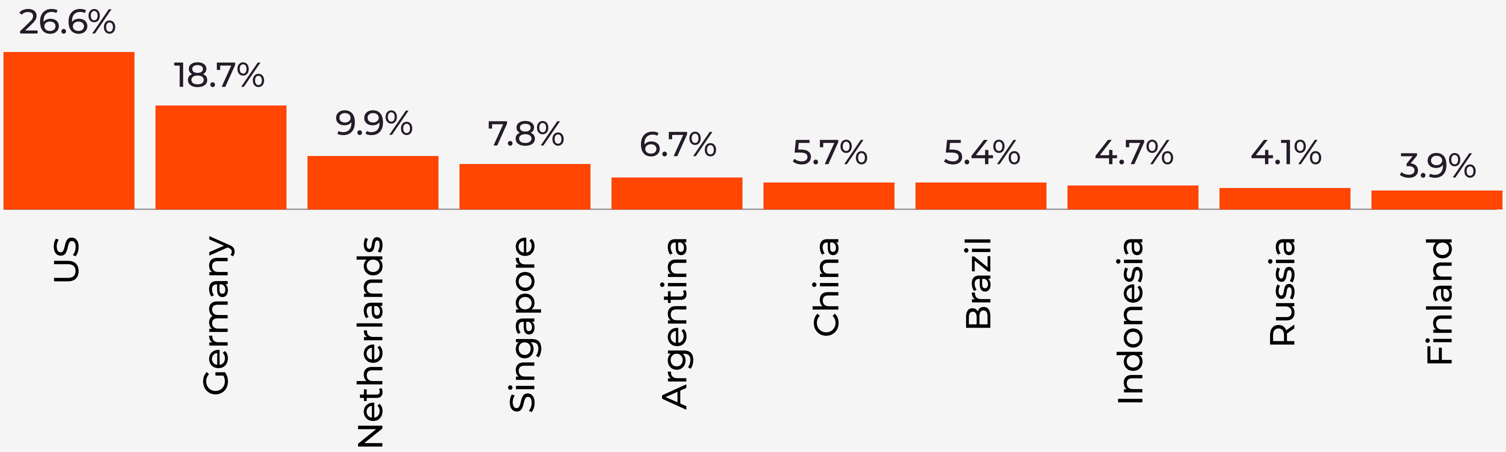
The media and entertainment industry ranked third most targeted at the application layer (L7), a concerning result for a competitive industry with a low tolerance for disruption and high customer expectations. Media and entertainment providers must prioritize their L7 protection strategy to deliver uninterrupted streaming and seamless content delivery.

# Where did most DDoS attacks originate?

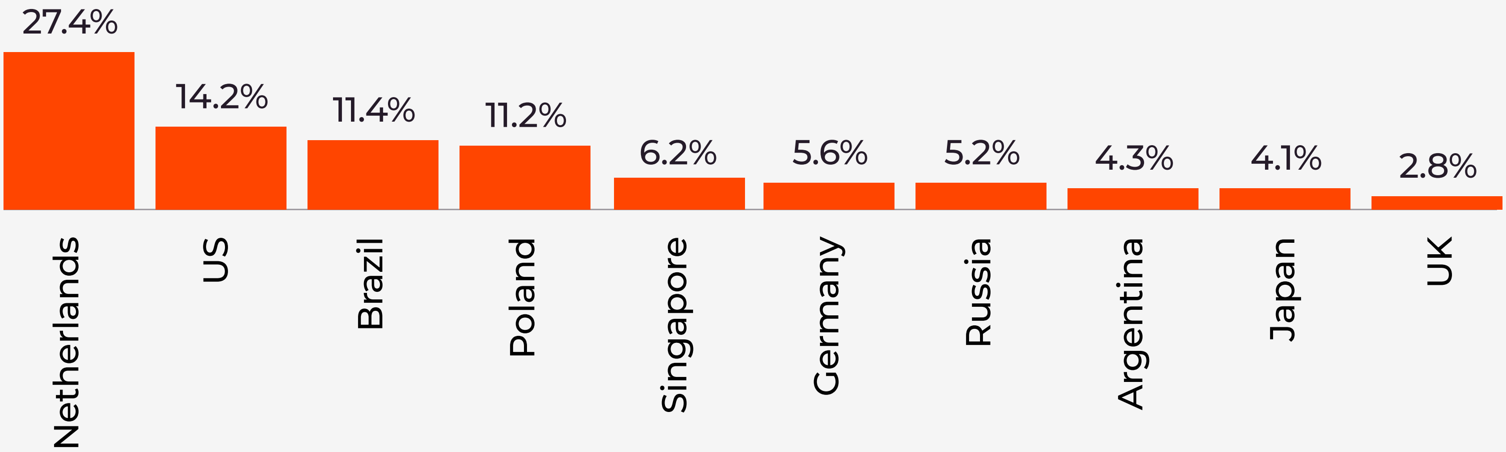
At the application layer, we use the attackers' IP addresses to determine their country of origin, as IP addresses cannot be altered or spoofed at this layer. In contrast, at the network layer, source IP addresses can be spoofed. Therefore, rather than relying on IP addresses to trace the source, we identify the locations of its data centers where the attack packets were received.

Due to our global coverage of six continents, we can report attack origins with geographical accuracy.

## Network-layer attacks: distribution by source country

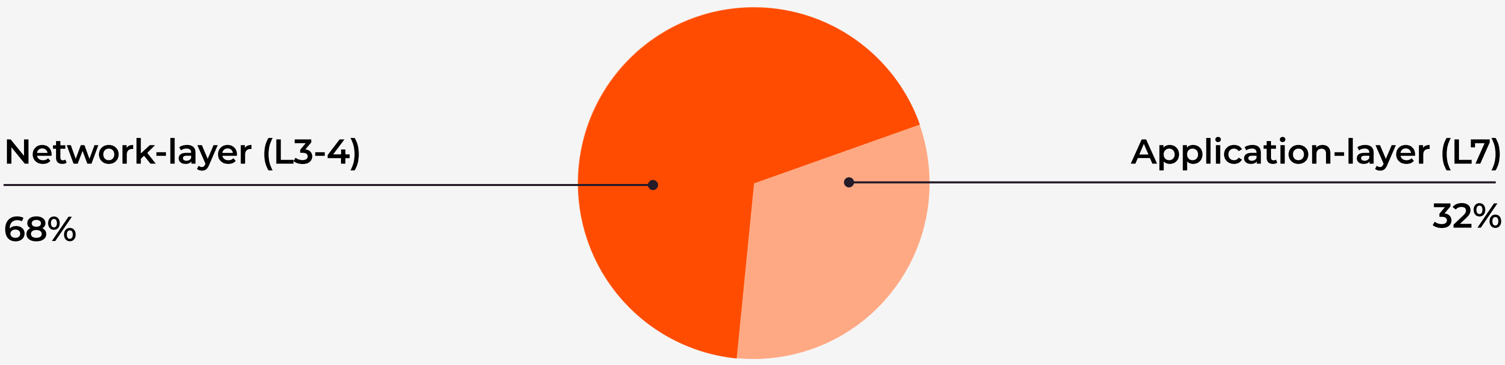


## Application-layer attacks: distribution by source country



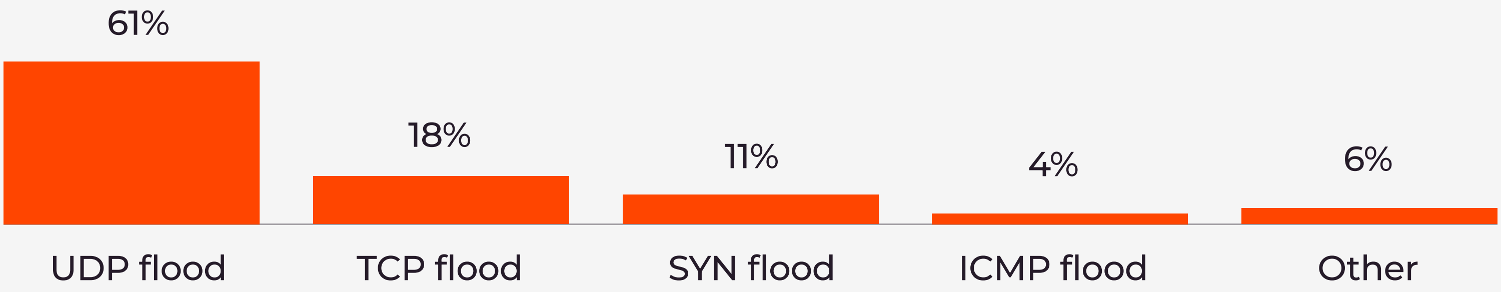
# Distribution of DDoS attack types

## Distribution of DDoS attack types

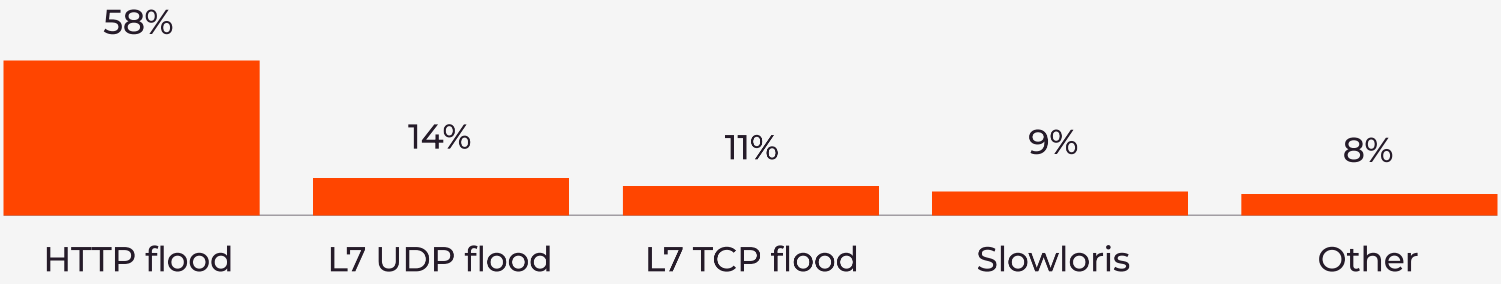


UDP floods continue to dominate at the L3–4 layers, constituting 61% of DDoS attacks. TCP and SYN flood attacks also remain popular, accounting for 18% and 11% of the total, respectively.

## Network-layer attack vectors (L3–4)

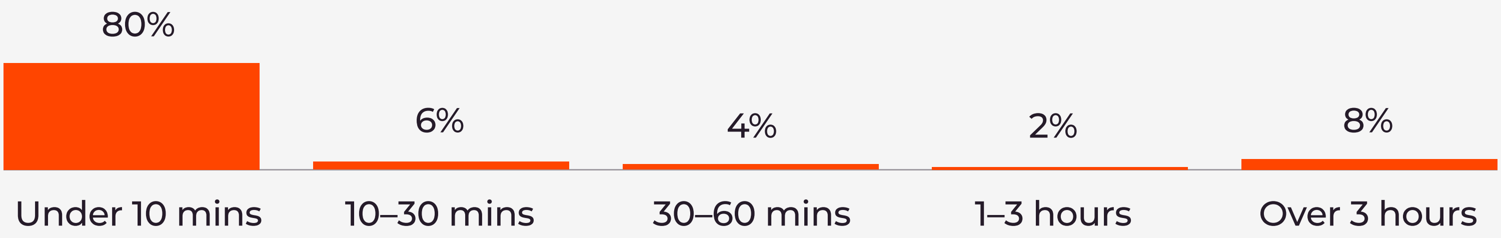


## Application-layer attack vectors (L7)

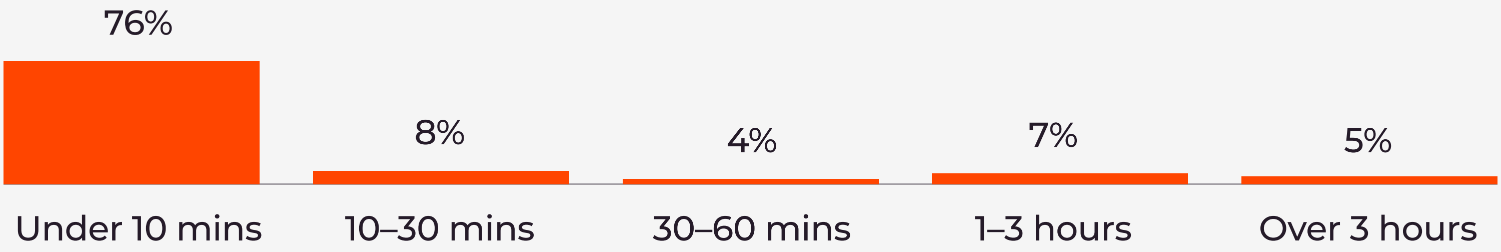


# The trend of short, powerful attacks remains

## Network-layer attack duration



## Application-layer attack duration



## Attack duration analysis

The maximum attack duration recorded during Q1–Q2 2024 was 16 hours, but as you can see, attacks are much shorter on average. Most attacks last under 10 minutes—and the durations are predominantly measured in minutes—but this doesn't mean that they are any less disruptive.

Attacks of any duration are detrimental to the user experience and brand reputation, and even short attacks can still be extremely costly.

# DDoS attacks are a universal threat, but they are becoming more personalized

The issue of DDoS attacks persists as a critical worldwide concern, calling for global collaboration and the exchange of intelligence to act swiftly and minimize the impact of these kinds of attacks.

The variability in the duration of attacks indicates that the perpetrators are adopting more sophisticated tactics, customizing their methods to align with the vulnerabilities and priorities of their targets. In the gaming industry, for instance, attacks are generally short-lived and less powerful but occur with greater frequency. This tactic aims to continually disturb a particular server, thereby degrading the gaming experience in hopes of compelling players to migrate to rival games. In contrast, for the financial services and telecommunications sectors—where service disruptions have incredibly high stakes and revenue repercussions are more immediate—attacks tend to be more intense in volume and vary significantly in length.

The ongoing focus on the gaming, technology, financial services, and telecommunications industries underscores attackers' deliberate strategy of selecting targets where disruption can lead to considerable economic and operational consequences.

# Gcore can protect your business, no matter the attack type, size, region, or duration

One thing is clear and consistent across all industries and regions: The threat of DDoS attacks is showing no sign of slowing down. Both the attacks themselves and targeting strategies are increasing in complexity. Now is the time for organizations, regardless of industry or size, to be vigilant and invest in their protection and prevention strategy.

Staying ahead of DDoS threats requires a keen understanding of cyber attackers' changing patterns and strategies. Gcore DDoS Protection has a proven record of repelling even the most powerful and sustained attacks. With 150+ Tbps of filtering capacity, coverage across six continents, and a global network constantly learning from its millions of internet properties, Gcore protects you against the largest and most sophisticated attacks.

Discover Gcore DDoS Protection