GCORE

Gcore Radar

DDoS Attack Trends

Q3–Q4 2024

January 2025 | gcore.com

Contents

About Gcore Radar

Monitoring DDoS trends is essential for anticipating emerging threats and enhancing defense strategies. Gcore's twice-annual Radar report analyzes DDoS attack data observed across our global network, spanning six continents and over 180 PoPs, to uncover key insights from the past six months.

This report examines attack data from Q3 and Q4 of 2024, identifying the industries most targeted, the prevailing types of DDoS attacks, and the evolving attack patterns during this period. Our comparisons to previous periods reveal clear trends in the ever-intensifying threat landscape.

Q3-Q4 2024 DDoS attack trends and key insights

Significant increase in attacks

The total number of DDoS attacks increased by 17% compared to Q1-Q2 2024.

Surge in attack size

The largest attack peaked at 2 Tbps in Q3-Q4 2024, an 18% increase from Q1-Q2 2024.

Industry-specific trends

Financial services saw the most significant rise in attacks with a 117% increase, while gaming remained the most-targeted industry despite a 31% decrease in the share of attacks compared to Q1-Q2 2024.

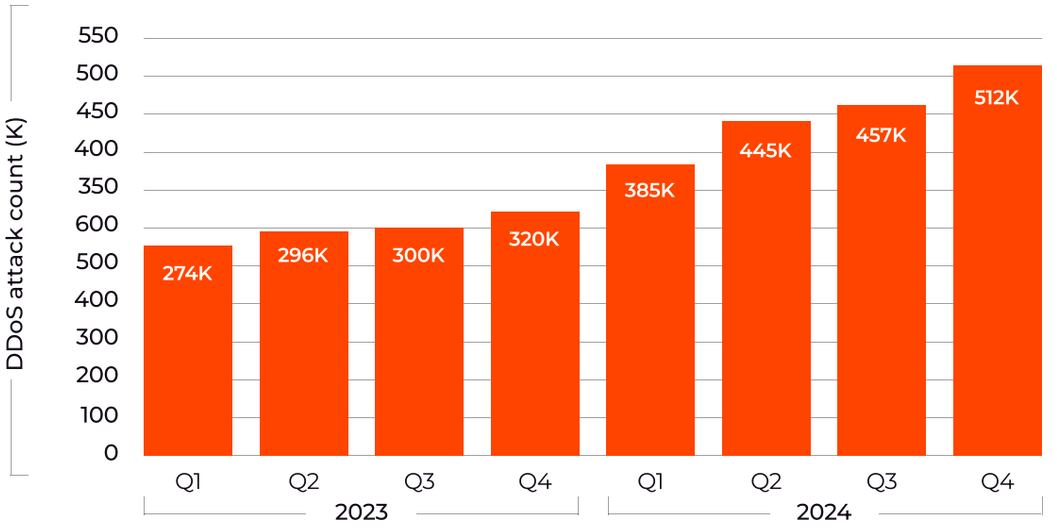
These findings underscore the need for advanced, adaptive DDoS protection strategies to counter evolving attack patterns and shifting targets.

Now, let's explore these trends and insights in more detail, starting with the total number of attacks recorded in Q3-Q4 2024.

The number of DDoS attacks continues to grow

The chart below shows a consistent increase in DDoS attacks over time, and Q3-Q4 2024 is no different. While increases appear steady quarter-on-quarter, with attacks increasing by 17% from Q1-Q2 2024, we see a sharper increase of 56% when compared to Q3-Q4 2023, highlighting the sustained momentum in attack volume.

DDoS attack count 2023-2024



Why are DDoS attacks increasing?

There are many reasons for the overall rise in DDoS attacks.

- **Growing availability of tools:** Easy access to attack tools and resources allows threat actors to evolve their tactics and exploit new opportunities in the expanding digital landscape.
- **Proliferation of IoT devices:** Poorly secured IoT devices have made it easier for attackers to build large botnets, increasing the scale and impact of attacks.
- **Geopolitical tensions and economic rivalries:** These factors are driving targeted attacks on critical infrastructure and organizations, increasing their frequency and intensity.
- **Advanced techniques:** The development of sophisticated methods, such as multi-vector and application-layer attacks, makes DDoS attacks more difficult to detect and mitigate.

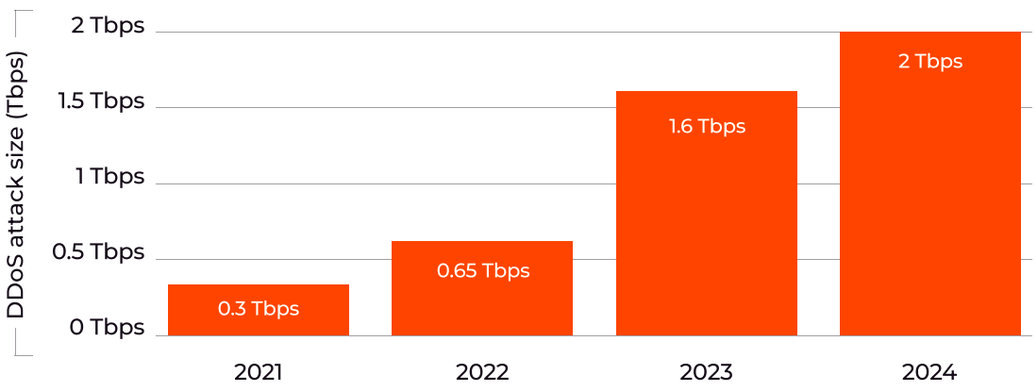
Together, these factors have made DDoS attacks more frequent, complex, and damaging than ever before.

New heights in DDoS attack size

In Q3-Q4 2024, Gcore observed a surge in DDoS attack size, with the largest attack reaching 2 Tbps, targeting a leading global gaming company. While the attack was quickly and successfully mitigated, it signals a concerning rise in attackers' attempts to overwhelm networks, applications, and digital services.

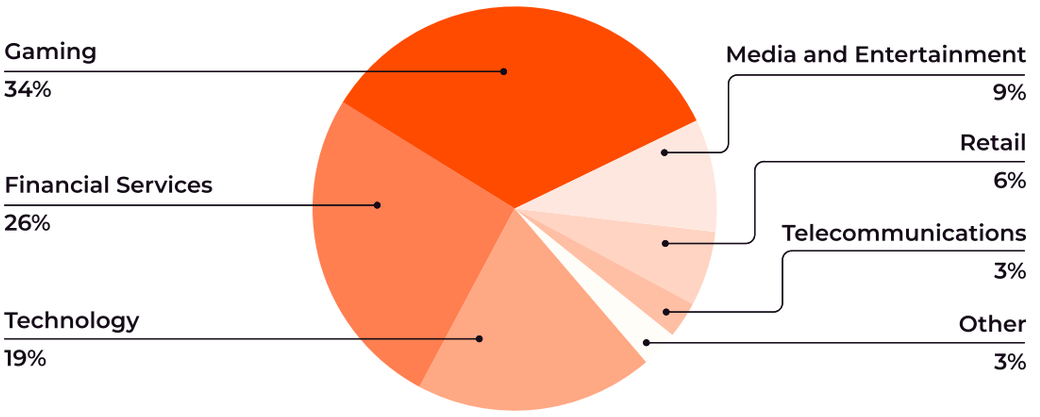
In our previous report, the largest recorded attack peaked at 1.7 Tbps. While a 0.3 Tbps increase may seem incremental, it represents a substantial jump in destructive potential. Terabit-level attacks can cripple even the most resilient systems, resulting in complete service outages, disruption of critical applications, and severe financial and reputational damage for the organizations targeted.

Peak DDoS attack size 2021-2024



The most attacked industries

DDoS attack distribution by industry Q3-Q4 2024



Gaming

Gaming remained the most-attacked industry, although it saw 31% fewer attacks than in Q1-Q2 2024. While this decline is notable, gaming continues to face a high volume of attacks, underscoring its ongoing vulnerability. This shift could be attributed to various factors. Gaming companies could be strengthening their DDoS protection in response to elevated risks, making successful attacks more challenging. Additionally, attackers might be shifting focus towards other high-value sectors, such as financial services, which saw a significant increase in attacks.

The gaming industry continues to be the most targeted by DDoS attacks, accounting for 34% of all attacks. Although this is a notable drop from 49% in Q3–Q4 2023, gaming continues to face the highest volume of DDoS attacks. Here is why:

- **Competitive advantage:** The highly competitive nature of online gaming can drive players, groups, or competitors to launch DDoS attacks against opponents to gain an advantage in tournaments or matches.
- **Revenue impact of downtime:** 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.

Financial services

Financial services experienced the most significant increase in DDoS attacks in Q3-Q4 2024. As a highly lucrative target that is heavily regulated and has a low tolerance for disruption and downtime, it is unsurprising that attackers have turned their focus to financial services, and the volume of attacks has increased.

In Q3-Q4 2024, financial services experienced a significant increase, accounting for 26% of all DDoS attacks, up from 12% in the previous period. Financial services is a prime target for cybercriminals, driven by two key factors:

- **Criticality of services:** Financial institutions, including banks, provide critical services such as online banking and payment systems. Any disruption to these services causes severe customer dissatisfaction, damage to reputation, and potential regulatory fines.
- **Extortion opportunities:** Due to the vital nature of financial services, downtime can have significant financial and reputational consequences. This makes financial organizations particularly susceptible to ransom DDoS attacks, where systems are flooded with traffic, rendering them inaccessible unless a ransom is paid. Given the urgency to restore services and avoid penalties, financial institutions are often willing to pay for the ransom, increasing their vulnerability to these types of attacks.

Technology

The technology industry has seen a consistent increase in its share of total DDoS attacks, from 7% in Q3–Q4 2023 to 15% in Q1–Q2 2024, and reaching 19% in Q3-Q4 2024. While the recent increase is incremental and less pronounced than in previous periods, the sector continues to experience a growing share of attacks.

Technology service providers are critical in supporting essential business infrastructure, including servers, storage systems, and networking solutions. Here's why they're a popular target for attacks:

- **High disruption potential:** Any disruption to technology services can have far-reaching consequences, affecting countless organizations that rely on their availability and performance. As a result, technology providers have become prime targets for cyber attackers seeking widespread operational disruption.
- **Extensive compute power:** Technology platforms are frequently targeted for their vast computational power, which attackers can exploit to intensify DDoS attacks or support other malicious operations. The extensive resources available within these environments make them an appealing target for cybercriminals looking to scale their attacks or conceal harmful activities.

How did other industries compare to previous periods?

Other industries experienced relatively minor fluctuations in their share of DDoS attacks during Q3-Q4 2024.

- **Media and entertainment:** This sector saw a considerable increase, with its share of attacks rising by 80%, reaching 9%.
- **Telecommunications:** Attacks on this sector significantly reduced, dropping from 10% to 3%.
- **Retail:** The share of attacks on retail reduced slightly, falling from 7% to 6%.

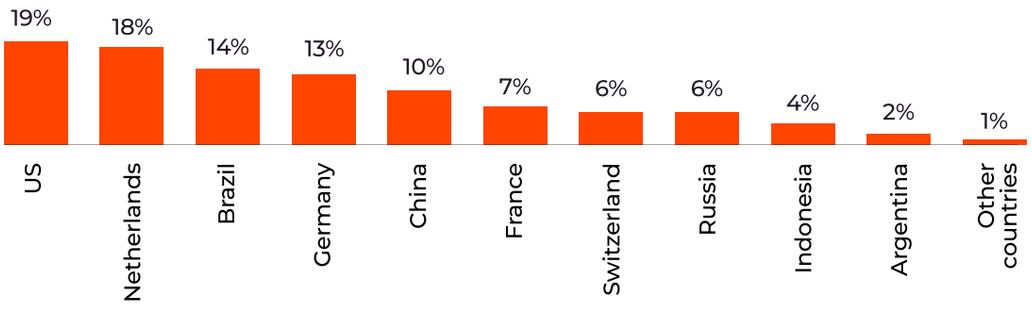
Geographical distribution of DDoS attacks

With an extensive presence across six continents, Gcore can provide precise geographical insights into the origins of all DDoS attack types.

Network-layer attacks

Since source IP addresses can be easily spoofed at the network layer, we focus on identifying the geographic locations of the data centers where malicious traffic is detected.

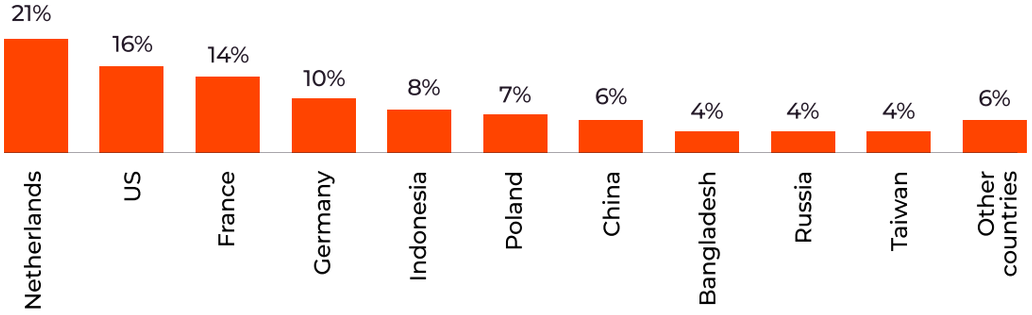
Network-layer DDoS attack distribution by source country
Q3-Q4 2024



Application-layer attacks

At the application layer, attackers' IP addresses offer a reliable way to determine their country of origin, as IP addresses cannot be faked or modified.

Application-layer DDoS attack distribution by source country
Q3-Q4 2024



Notable attack origins

The geographical distribution of DDoS attacks reveals notable trends across network- and application-layer sources.

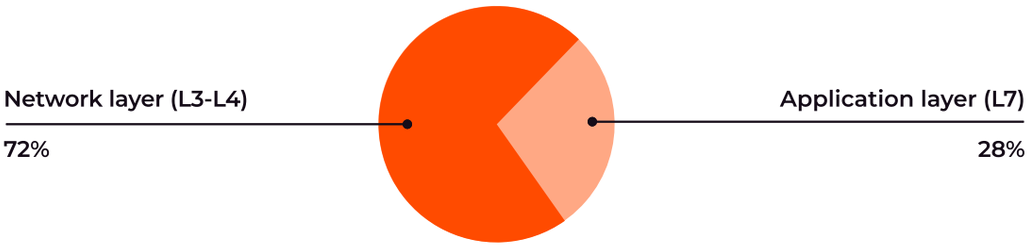
- **Netherlands:** Emerges as a key origin, leading application-layer attacks (21%) and ranking second for network-layer attacks (18%), highlighting its robust infrastructure being exploited by attackers.
- **United States:** The US consistently ranks high across both layers, reflecting its vast internet infrastructure and resources being leveraged for malicious activity.
- **Brazil:** Prominent in network-layer attacks (14%), Brazil's growing digital economy and expanding connectivity make it an emerging source of significant attack activity.
- **China and Indonesia:** Both countries contribute heavily to attacks across layers. Indonesia, in particular, shows growth in application-layer attacks (8%), signaling a rising trend in malicious activity from Southeast Asia.

These insights suggest that attackers are selecting regions with dense infrastructure and high connectivity, making proactive defenses in these areas increasingly critical.

Distribution of DDoS attack types

The distribution of DDoS attacks across the network and application layers during Q3-Q4 2024 highlights a greater prevalence of network-layer attacks.

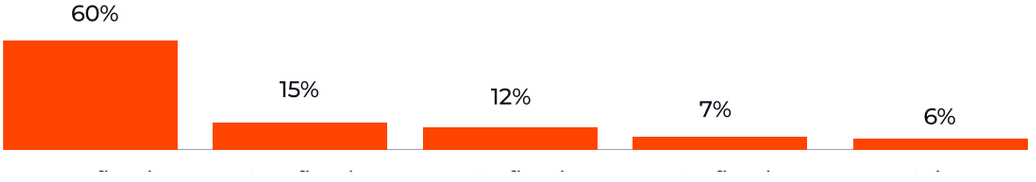
DDoS attack distribution by layer Q3-Q4 2024



Network-layer attack vectors

UDP flood attacks continue to dominate, comprising 60% of network-layer DDoS attacks, similar to the 61% observed in the previous period. SYN and TCP flood attacks also remain a popular choice, accounting for 15% and 12% of the total attacks, respectively. These attack vectors persist due to their simplicity, effectiveness, and the ability to overwhelm targeted networks with high traffic volumes, making them a staple method for many cybercriminals.

Network-layer DDoS attack distribution by vector
Q3-Q4 2024



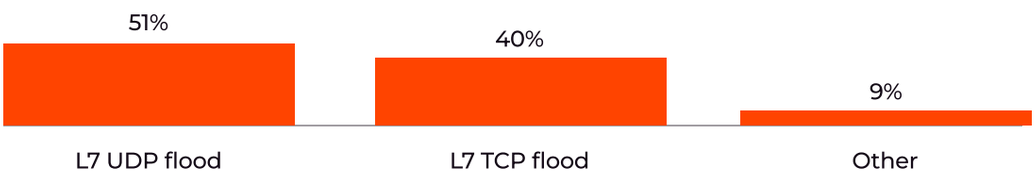
ACK flood ranks among top attack vectors

ACK flood attacks are emerging as a prominent attack vector accounting for 7% of network-layer DDoS attacks. They represent a growing challenge due to their deceptive nature. These attacks exploit the victim's system by overwhelming it with ACK packets, each requiring a resource-intensive response. Unlike other attack types, ACK flood attacks closely mimic legitimate traffic, complicating detection and filtering efforts. Their simplicity—easily executed using botnets or spoofed IPs—makes them increasingly attractive to attackers aiming to bypass conventional defenses while maximizing resource exhaustion. The rise of ACK flood attacks highlights the evolving sophistication of network-layer threats.

Application-layer attack vectors

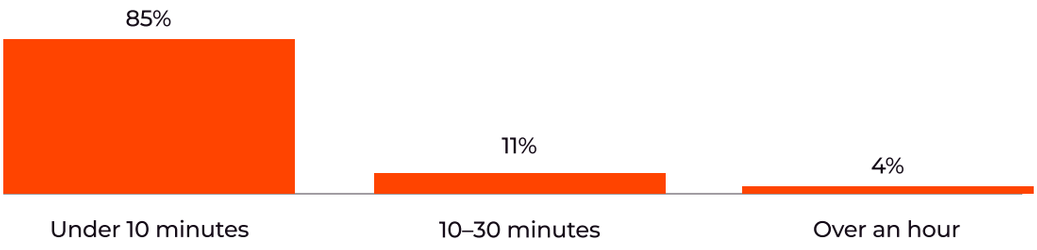
L7 UDP flood attacks accounted for 45% of all application-layer attacks in Q3-Q4 2024, while L7 TCP flood attacks increased to 37%, reflecting attackers' growing use of adaptive, high-impact methods to overwhelm application resources and evade traditional mitigation strategies.

Application-layer DDoS attack distribution by vector
Q3-Q4 2024

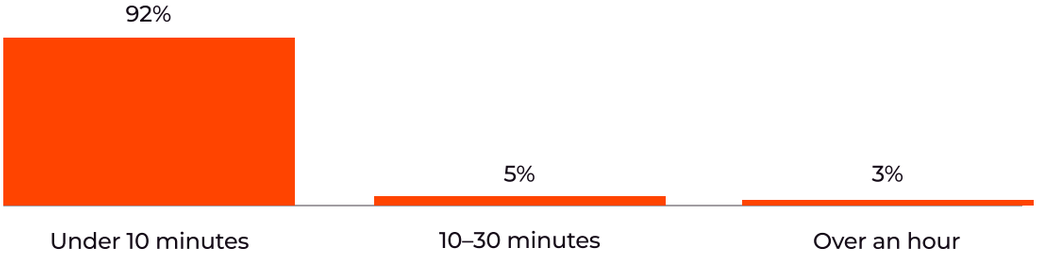


Trends in DDoS attack duration

Network-layer DDoS attack distribution by duration
Q3-Q4 2024



Application-layer DDoS attack distribution by duration
Q3-Q4 2024

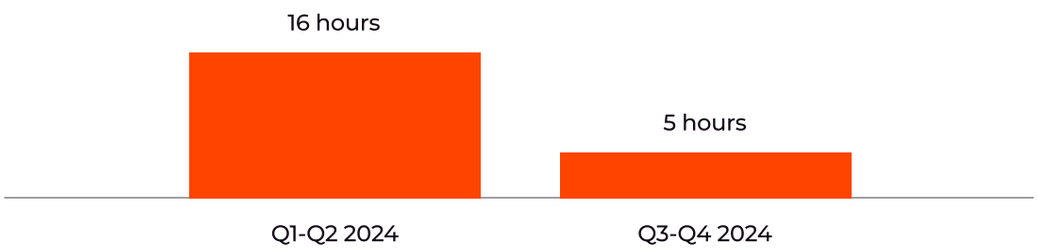


The shift toward shorter DDoS attack durations

The maximum DDoS attack duration recorded during Q3–Q4 2024 was five hours, a sharp drop from the previous period, where the longest attack lasted 16 hours.

This significant reduction in attack duration highlights a shift towards burst attacks. These attacks are shorter but more intense, occurring in rapid, concentrated intervals that can easily blend in with normal traffic spikes. By using realistic-looking requests (e.g., HTTP GET requests) with spoofed IP addresses, attackers can disguise their actions, making it harder for systems to differentiate between legitimate users and malicious activity. This delay in detection gives attackers enough time to disrupt services before defenses kick in.

Maximum DDoS attack duration 2024



Why are DDoS attacks getting shorter?

The vast majority of both network-layer and application-layer attacks continue to last under 10 minutes—and attack durations are increasingly measured in minutes rather than hours—but this doesn't mean they are any less disruptive. The trend of shorter DDoS attack durations can be attributed to evolving attacker tactics and advancements in cybersecurity measures. Several key factors contribute to this shift:

- **The effectiveness of short, high-impact attacks:** Burst attacks—brief but highly intense attacks—enable attackers to cause significant disruption in a short amount of time. Even a few minutes of downtime for critical services can lead to severe business consequences, including financial losses and reputational damage. These rapid attacks are challenging for some security solutions to detect and mitigate in real time, as they often do not conform to traditional patterns of sustained attacks. This means that by the time the attack is detected, significant damage may already be done.
- **Rise of multi-stage attack strategies:** Cybercriminals are increasingly using short DDoS attacks as a distraction tactic, diverting the attention of IT teams while carrying out their primary objective: system infiltration or data theft. A brief DDoS attack can serve as a smokescreen to conceal the initial deployment of ransomware or other malicious activities.
- **Masking malicious traffic:** Short-lived attacks, characterized by irregular traffic bursts, closely mimic legitimate user activity, making them harder to detect and mitigate swiftly. This complexity allows attackers to bypass conventional detection mechanisms and prolong their malicious efforts.

As a result of these factors, short-duration DDoS attacks have become a precise, efficient, and cost-effective method for today's threat actors.

Key takeaways from an evolving threat landscape

The DDoS threat landscape continues to evolve in terms of volume, complexity, and target precision.

1. **Attacks on financial services have increased.** This industry has seen a notable increase in DDoS attacks. While financial services are a prime target, all sectors must remain vigilant about evolving threats, particularly gaming and technology.
2. **Short, powerful attacks remain popular.** Short but intense attacks can cause significant damage in minimal time and evade traditional detection mechanisms.
3. **Beware of attacks that mask legitimate traffic.** Burst attacks, which mimic irregular traffic patterns, complicate detection and mitigation efforts.

As attack trends evolve to better infiltrate and disrupt critical systems and infrastructure, organizations must prioritize proactive defense strategies to effectively mitigate attacks.

DDoS Protection

Staying ahead of DDoS threats requires a clear understanding of the evolving tactics and strategies employed by cyber attackers. Gcore has a proven track record of repelling even the most powerful and sustained attacks. With a filtering capacity exceeding 200 Tbps and coverage across six continents with 180+ PoPs, Gcore DDoS Protection provides robust protection against evolving threats, regardless of size or sophistication.

Discover Gcore DDoS Protection

About Gcore

Gcore is a global edge AI, cloud, network, and security solutions provider. Headquartered in Luxembourg, with a team of 600 operating from ten offices worldwide, Gcore provides solutions to global leaders in numerous industries. Gcore manages its global IT infrastructure across six continents, with one of the best network performances in Europe, Africa, and LATAM due to the average response time of 30 ms worldwide. Gcore's network consists of 180 points of presence worldwide in reliable Tier IV and Tier III data centers, with a total network capacity exceeding 200 Tbps.

Learn more at **gcore.com**

GCORE