qrator.net

QRATOR LABS

Q1, 2026 DDOS, BAD BOTS, AND BGP INCIDENTS STATISTICS AND OVERVIEW

Executive summary

The largest DDoS botnet we first detected in March 2025 has grown significantly over the past year, expanding from 1.33 million to 13.5 million infected devices. The majority of these devices are located in the United States, Brazil, and India.

In Q1 2026, we discovered the Aeternum C2 botnet, which uses the Polygon blockchain as its primary command-and-control infrastructure, making it highly resistant to traditional takedown methods.

The most intensive DDoS attack observed in Q1 2026 targeted an organization in the Betting segment. At its peak, it exceeded 2 Tbps and reached nearly 1 Bpps. Notably, the high-intensity phase lasted for more than 40 minutes, which is unusually long for attacks of this scale.

The share of multi-vector DDoS attacks in Q1 2026 increased compared to 2025, rising from 8.0% to 10.7% of all incidents. The share of attacks combining L3-L4 and L7 grew even more significantly, from 3.6% to 6.2% of all incidents.

The highest number of DDoS attacks in Q1 2026 targeted the FinTech (44.2%), Information and communication technology (19.3%), and Betting (10.0%) segments. Together, these three segments accounted for nearly three quarters of all attacks we recorded.

The most frequently targeted microsegments in Q1 2026 included Banks (22.8%), Payment systems (15.9%), Betting shops (10.0%), Hosting platforms (6.8%), and System integrators (6.4%).

In Q1 2026, the largest sources of L7 DDoS attacks were Brazil (12.1%), the United States (11.5%), and Russia (7.3%). At the same time, the share of the top five countries decreased from 56.5% to 42.0% compared to the previous year, indicating a more even distribution of attack sources across countries.

In Q1 2026, the average monthly number of blocked bad bot requests increased by 12% compared to 2025, reaching 2.5 billion.

The overall "bot index" in Q1 2026 stood at 1.97%, slightly below the average for the last nine months of 2025 (2.1%), but still notably high.

The longest bad bot attack in Q1 2026 targeted an organization in the E-commerce segment. It lasted for more than two weeks, during which over 178 million bot requests were blocked.

In Q1 2026, the number of unique ASes responsible for route leaks remained at the level of the previous year. Meanwhile, the number of ASes involved in BGP hijacks decreased by approximately 17% compared to Q1 2025.

The number of global BGP incidents in Q1 2026 was high — we recorded seven route leaks and one BGP hijack.

Prevalent DDoS attack vectors in Q1 2026

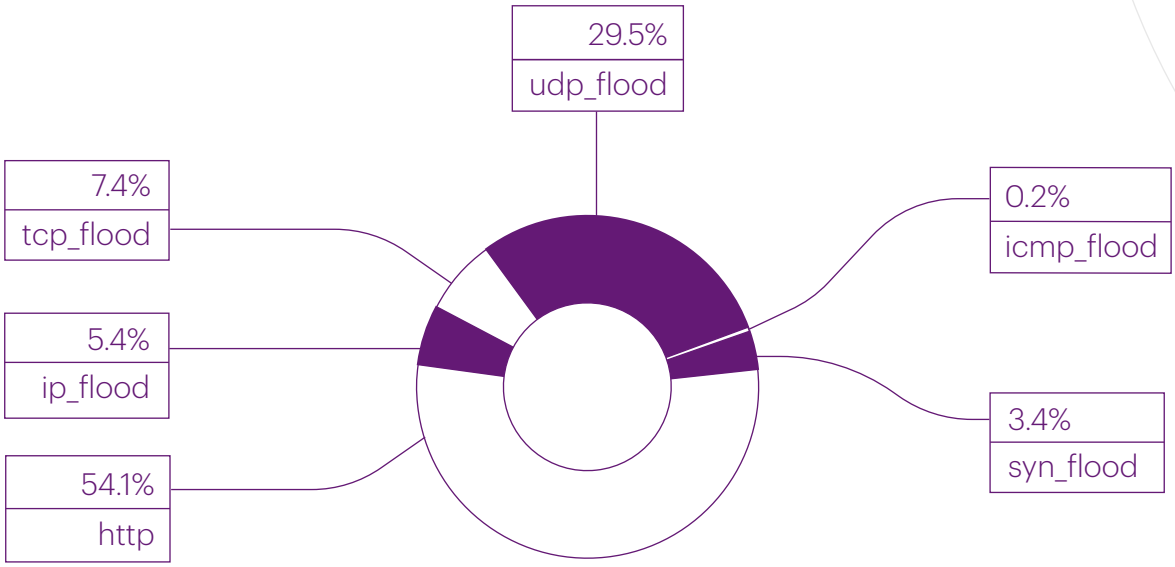
Starting from Q2 2025, we changed our methodology for analyzing DDoS attacks. Previously, we considered network- and transport-layer attacks (L3-L4 DDoS) and application-layer attacks (L7 DDoS) separately. We now use a unified approach based on incidents, which may consist of multiple attacks across different vectors.

We filter out L3-L4 DDoS attacks with an intensity below 1 Gbps, considering them background noise. For L7 DDoS attacks, we also apply threshold criteria: at least 100 blocked IP addresses and a rate of at least 1,000 requests per second. Multiple attack waves are grouped into a single incident if the time gap between them does not exceed one hour.

In Q1 2026, the majority of DDoS attacks were HTTP-based, that is, application-layer (L7) attacks. They accounted for 54.1% of all attacks we recorded, which is broadly in line with the level observed over the last nine months of the previous year (56.4%). UDP flood ranked second, with its share increasing significantly compared to the previous year (22.9% — 29.5%).

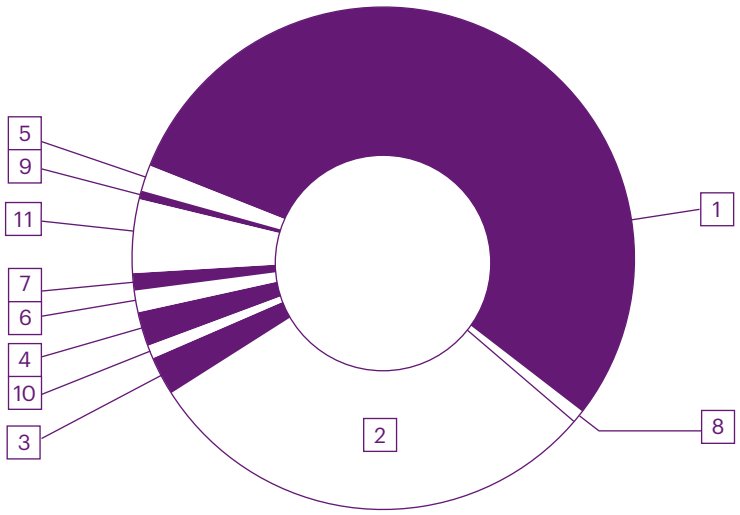
IP flood is becoming less favored by attackers (13.8% — 5.4%), which resulted in TCP moving into third place (4.2% — 7.4%). The relative share of SYN flood and ICMP flood attacks remained roughly at the same level as in the previous year.

Distribution of DDoS attacks by attack vector in Q1 2026



In Q1 2026, compared to the last nine months of 2025, the share of multi-vector attacks increased noticeably, rising from 8.0% to 10.7% of all recorded incidents. The share of multi-vector attacks combining L3-L4 DDoS and L7 DDoS also grew significantly, from 3.6% of all incidents in 2025 to 6.2% in Q1 2026.

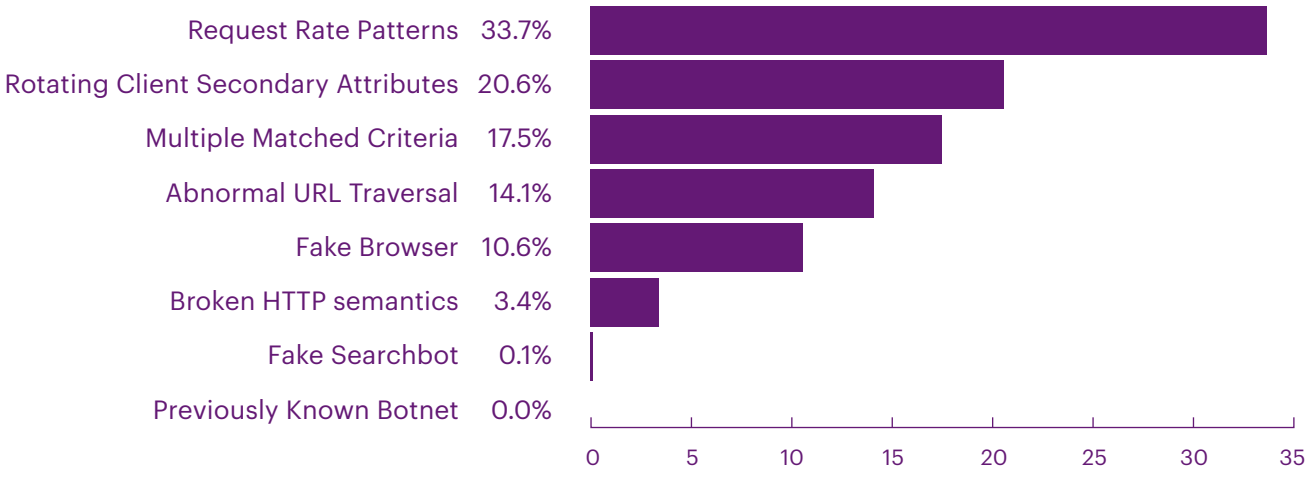
Multivector L3-L4 DDoS attacks in 2026



1	54.6	http			
2	29.8	udp_flood			
3	2.3	tcp_flood			
4	2.3	tcp_flood	http		
5	1.8	udp_flood	ip_flood		
6	1.2	ip_flood			
	%				

7	1.2	syn_flood			
8	0.8	http	udp_flood	ip_flood	
9	0.7	http	udp_flood	syn_flood	tcp_flood	ip_flood
10	0.6	http	udp_flood		
11	4.7	Others			
	%				

L7 DDoS attacks by type in Q1 2026

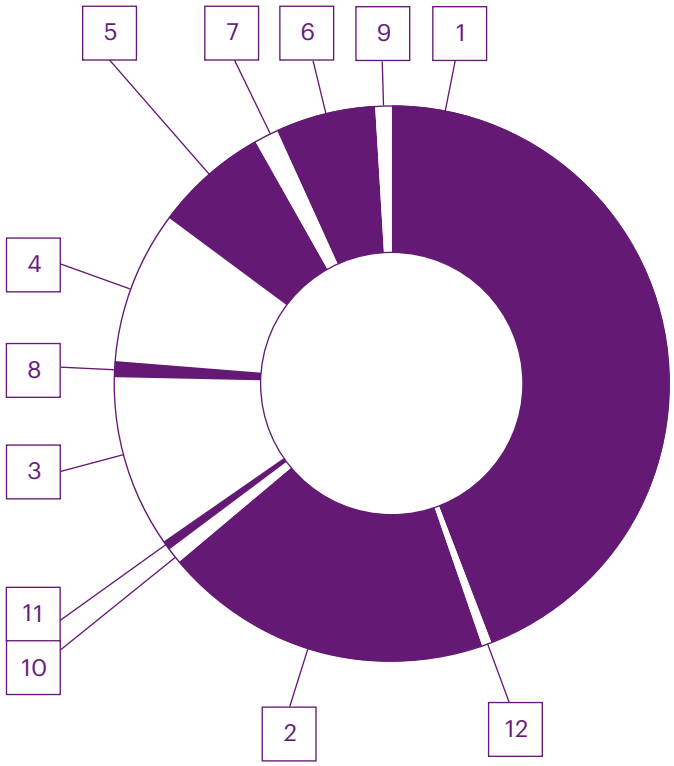


Distribution of DDoS attacks by industry in Q1 2026

The majority of DDoS attacks in Q1 2026 targeted organizations in the FinTech (44.2%), Information and communication technology (19.3%), and Betting (10.0%) segments. Together, these segments accounted for nearly three quarters of all recorded incidents.

The increased activity in the Betting segment is worth noting separately — along with a noticeably higher number of incidents compared to the previous year, it also saw both the most intensive and the longest DDoS attack of the quarter (discussed in more detail below).

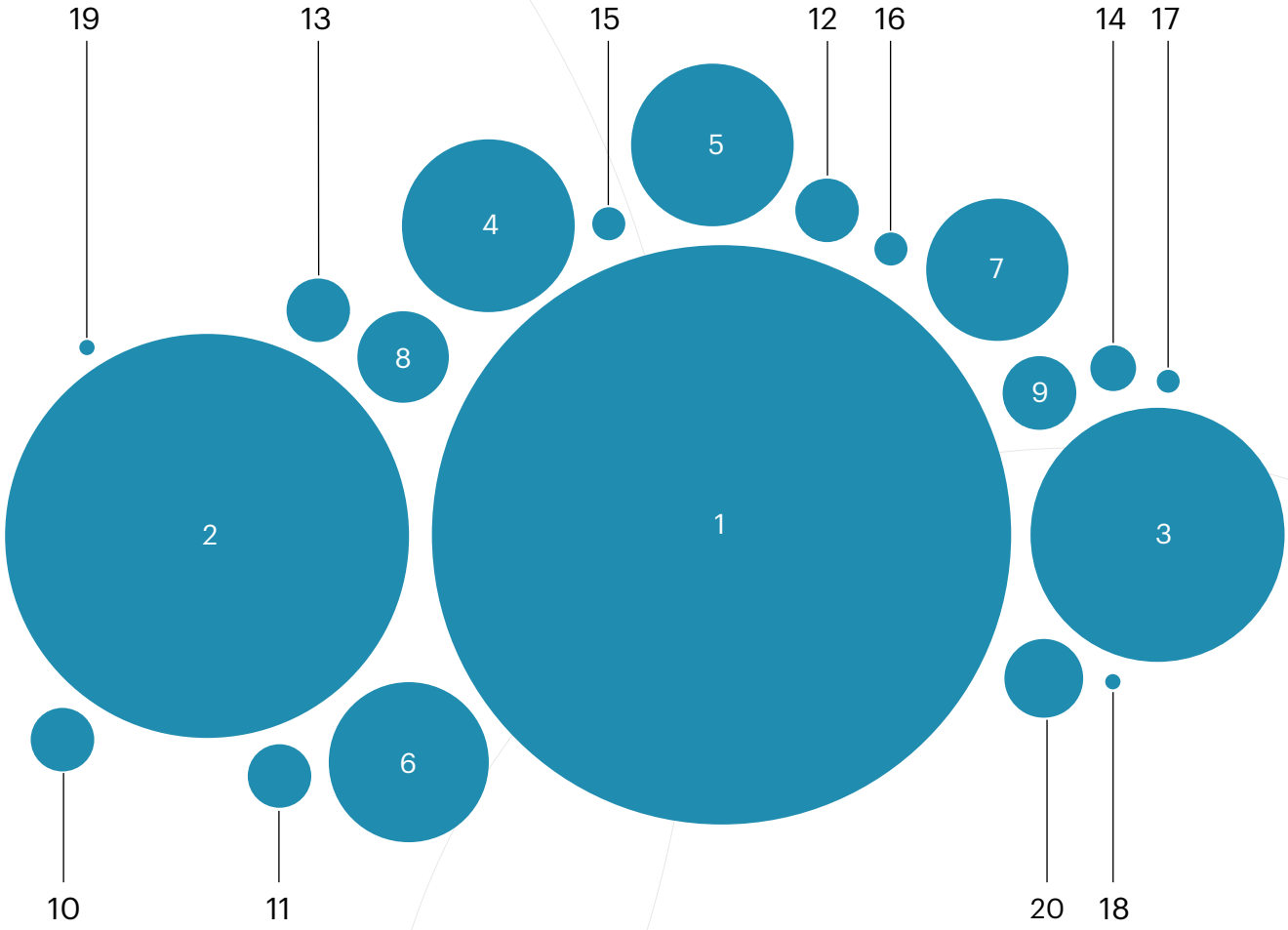
Macro-level segmentation of DDoS attacks in Q1 2026



1	**44.2%**	FinTech
2	**19.3%**	IT&Telecom
3	**10.0%**	Betting
4	**8.8%**	Media
5	**6.6%**	E-commerce
6	**5.9%**	EdTech
7	**1.4%**	Games
8	**0.9%**	Industrial
9	**0.9%**	Government
10	**0.9%**	Healthcare
11	**0.6%**	Transport&Logistics
12	**0.5%**	Ads&Entertainment

At a more granular level, DDoS attacks in Q1 2026 primarily targeted Banks (22.8%), Payment systems (15.9%), Betting shops (10.0%), Hosting platforms (6.8%), and System integrators (6.4%). Together, these five microsegments accounted for nearly two thirds (62.0%) of all attacks recorded in Q1 2026.

Micro-level segmentation of DDoS attacks in Q1 2026



1	22.8%	Banks	11	2.5%	Telecom operators
2	15.9%	Payment systems	12	2.5%	Social media
3	10.0%	Betting shops	13	2.5%	Food retail
4	6.8%	Hosting platforms	14	1.8%	Cryptocurrency exchanges
5	6.4%	System integrators	15	1.3%	Online retail
6	6.3%	Media, TV, radio, and bloggers	16	1.3%	Game platforms
7	5.6%	Digital education	17	0.9%	Oil&Gas
8	3.6%	Software services	18	0.6%	Airports
9	2.9%	Forex	19	0.6%	Medical laboratories
10	2.5%	Classified ads	20	3.1%	Other

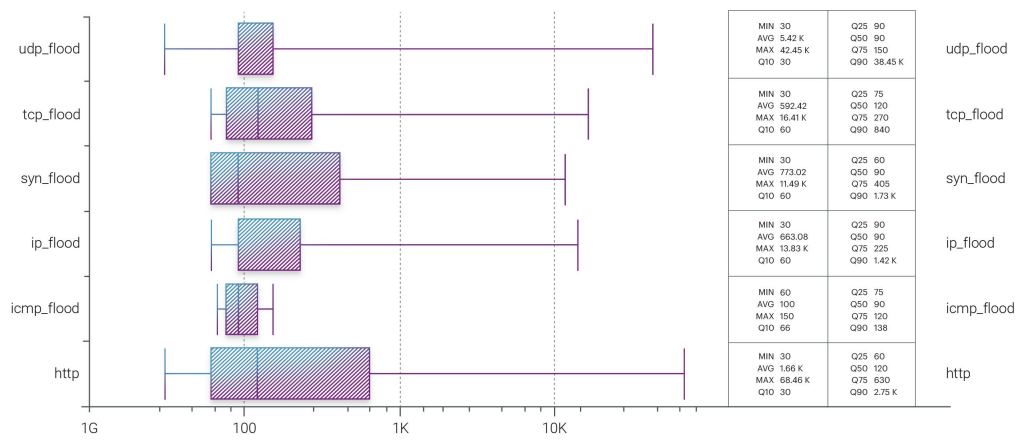
Duration of DDoS attacks in Q1 2026

The longest DDoS attacks in Q1 2026 targeted the following segments: Betting shops (19.0 h), Media, TV, radio, and bloggers (16.2 h), System integrators (11.8 h), and Software services (10.1 h). These durations are relatively short — for comparison, the longest attack recorded in 2025 lasted 119.2 hours.

Longest DDoS attacks in hours in Q1 2026

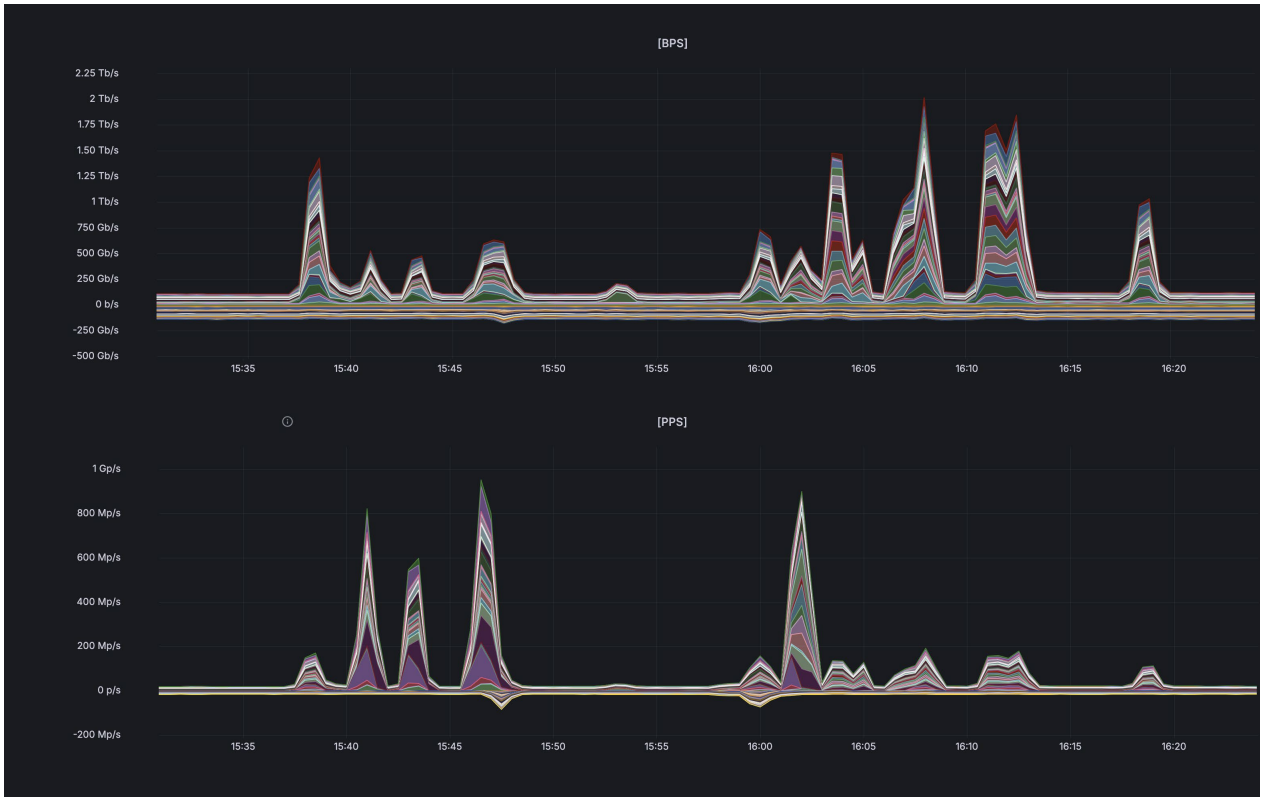
Despite these relatively modest maximum durations, the average attack duration in Q1 2026 increased slightly compared to 2025, from 2,268 to 3,221 seconds. The median duration remained unchanged at 120 seconds.

Duration of DDoS attacks in seconds by attack vector in Q1 2026



Intensity of L3-L4 DDoS attacks in Q1 2026

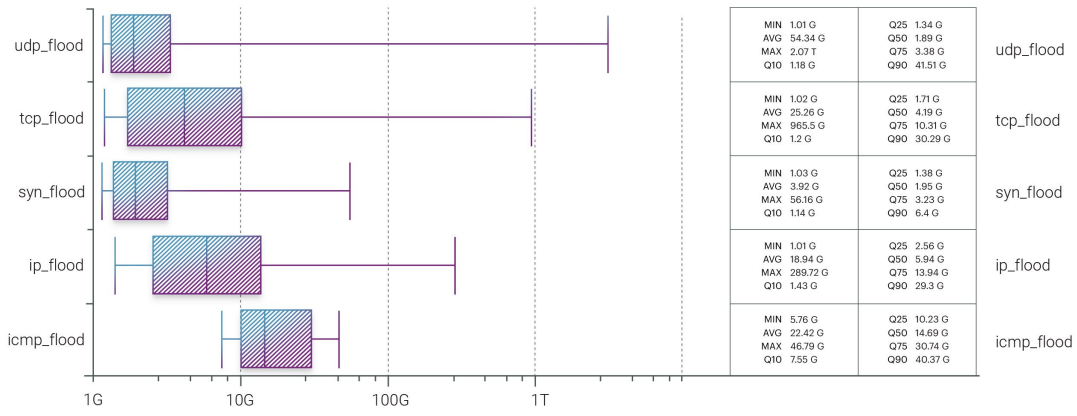
The most intensive attack of Q1 2026 occurred in mid-March and targeted an organization in the Betting segment. At its peak, the attack reached 2,065 Gbps, while the maximum packet rate was 953 Mpps, just short of 1 Bpps.



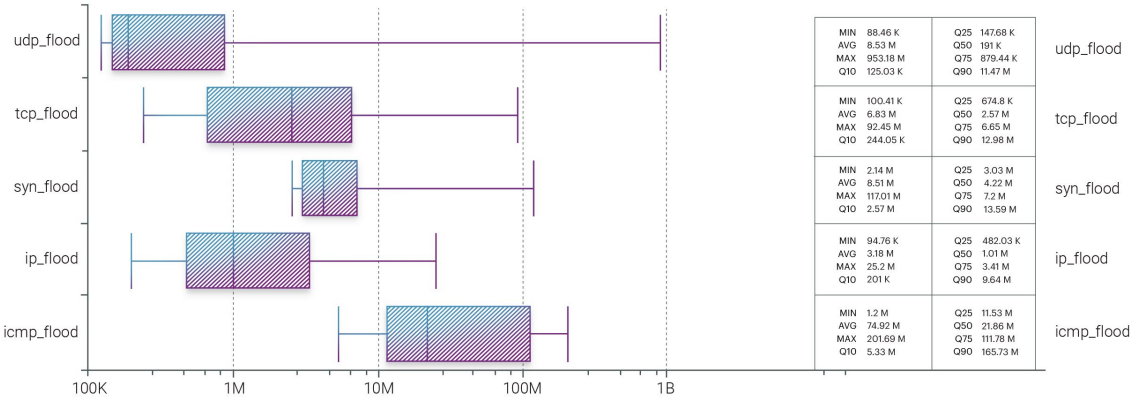
What is particularly unusual for an attack of this scale is that its peak phase lasted not just seconds, as is typically the case, but a full 40 minutes. During this period, we observed 11 spikes, four of which exceeded 1 Tbps. This suggests that the attackers were attempting to adapt their strategy and maintain sustained pressure on the infrastructure. Despite these efforts, the attack was successfully mitigated without any impact on service availability.

While attacks exceeding 1 Tbps were relatively rare in 2025, they are becoming increasingly common in 2026. In Q1 2025, we did not record a single attack above 1 Tbps, whereas in Q1 2026, there were already four such incidents.

L3-L4 DDoS attack volume in bits per second (bps) by attack vector in Q1 2026

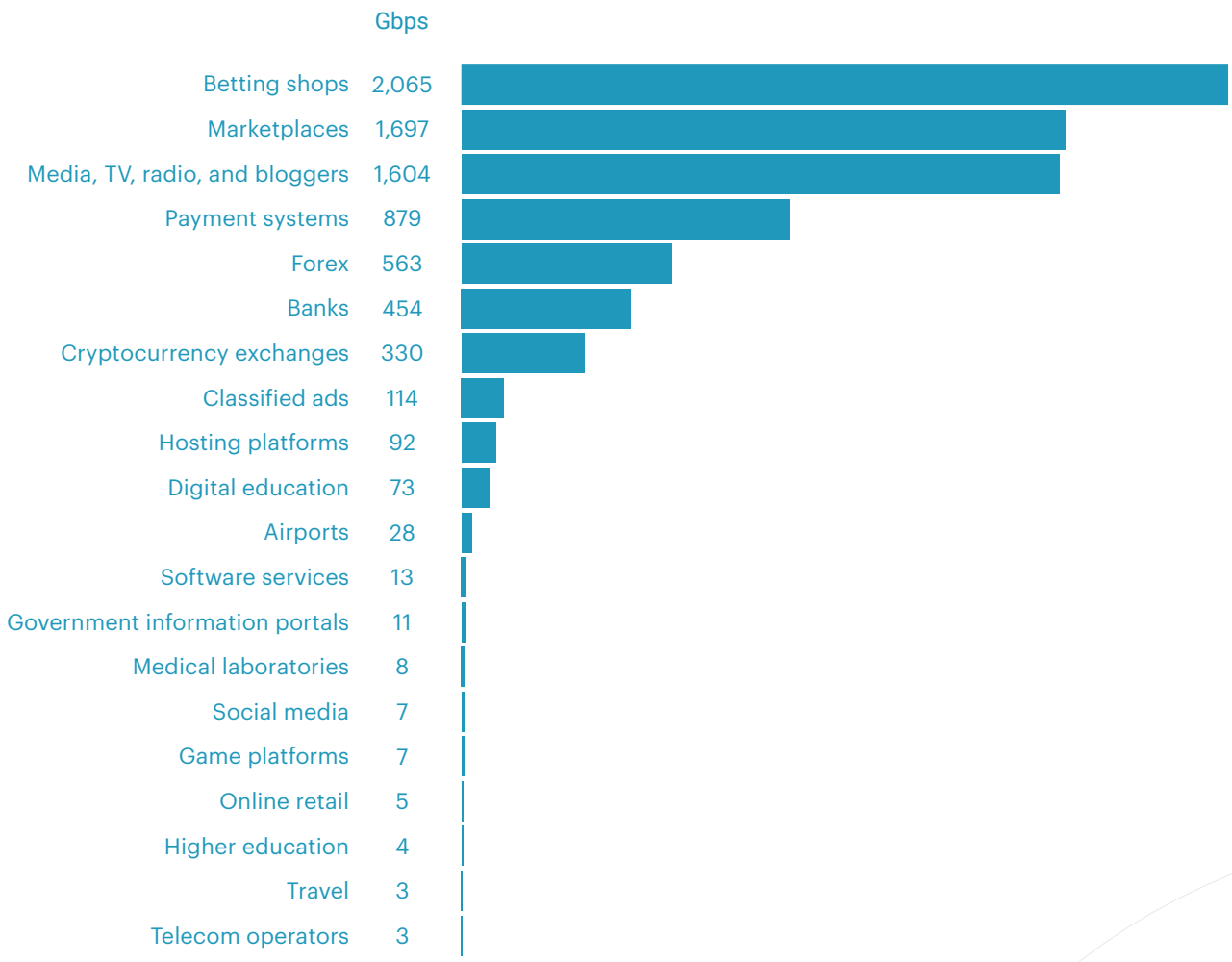


L3-L4 DDoS attack volume in packets per second (pps) by attack vector in Q1 2026



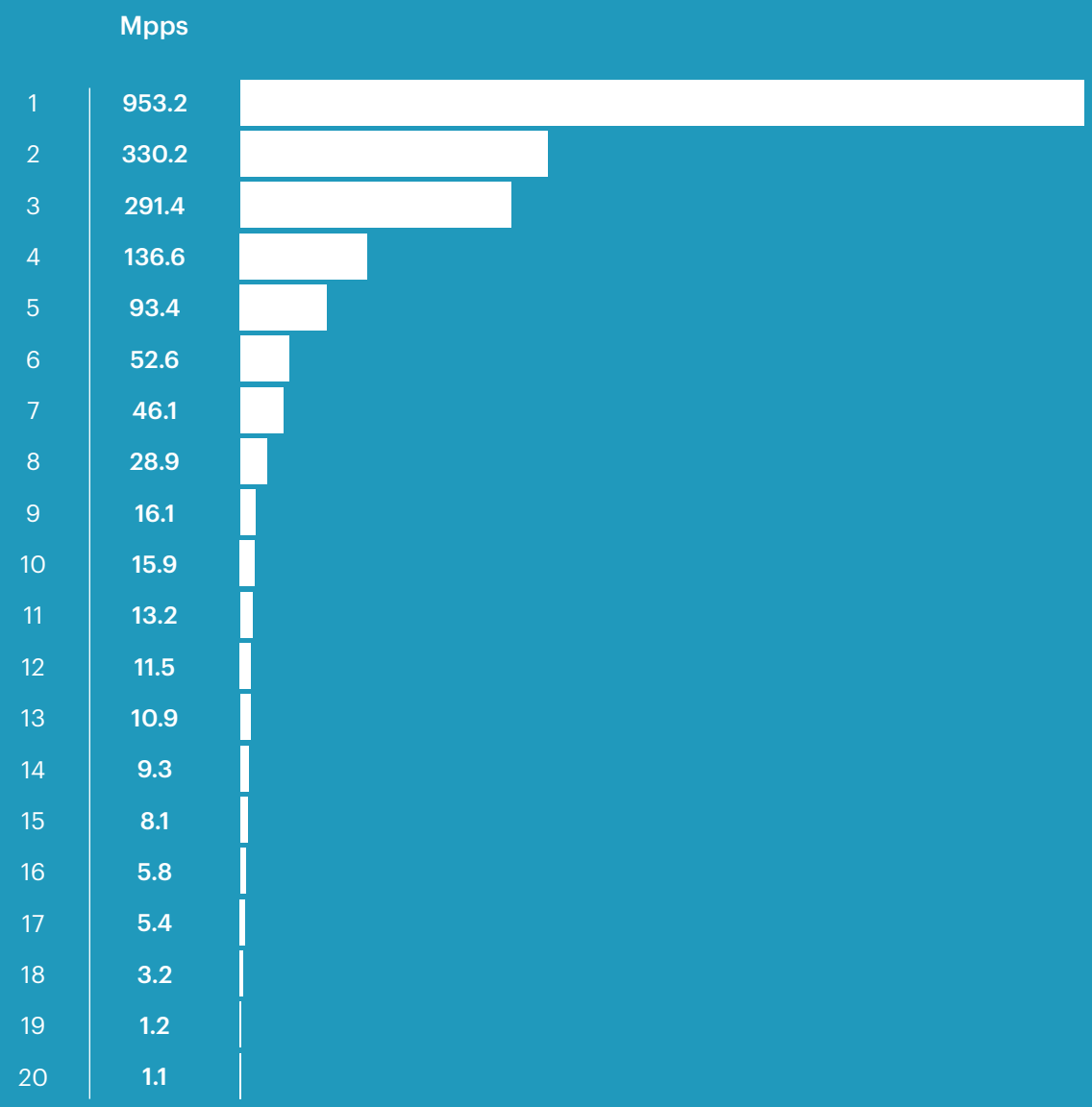
The top five microsegments targeted by the most intensive L3-L4 DDoS attacks in Q1 2026 were as follows: Betting shops (2,065 Gbps), Marketplaces (1,697 Gbps), Media, TV, radio, and bloggers (1,604 Gbps), Payment systems (879 Gbps), and Forex (563 Gbps).

Maximum bitrate of L3-L4 DDoS attacks by segment in Q1 2026



In terms of maximum packet rate, the most intensive attacks in Q1 2026 targeted the following microsegments: Betting shops (953.2 Mpps), Marketplaces (330.2 Mpps), Hosting platforms (291.4 Mpps), Media, TV, radio, and bloggers (136.6 Mpps), and Payment systems (93.4 Mpps).

Maximum packet rate of L3-L4 DDoS attacks by segment in Q1 2026

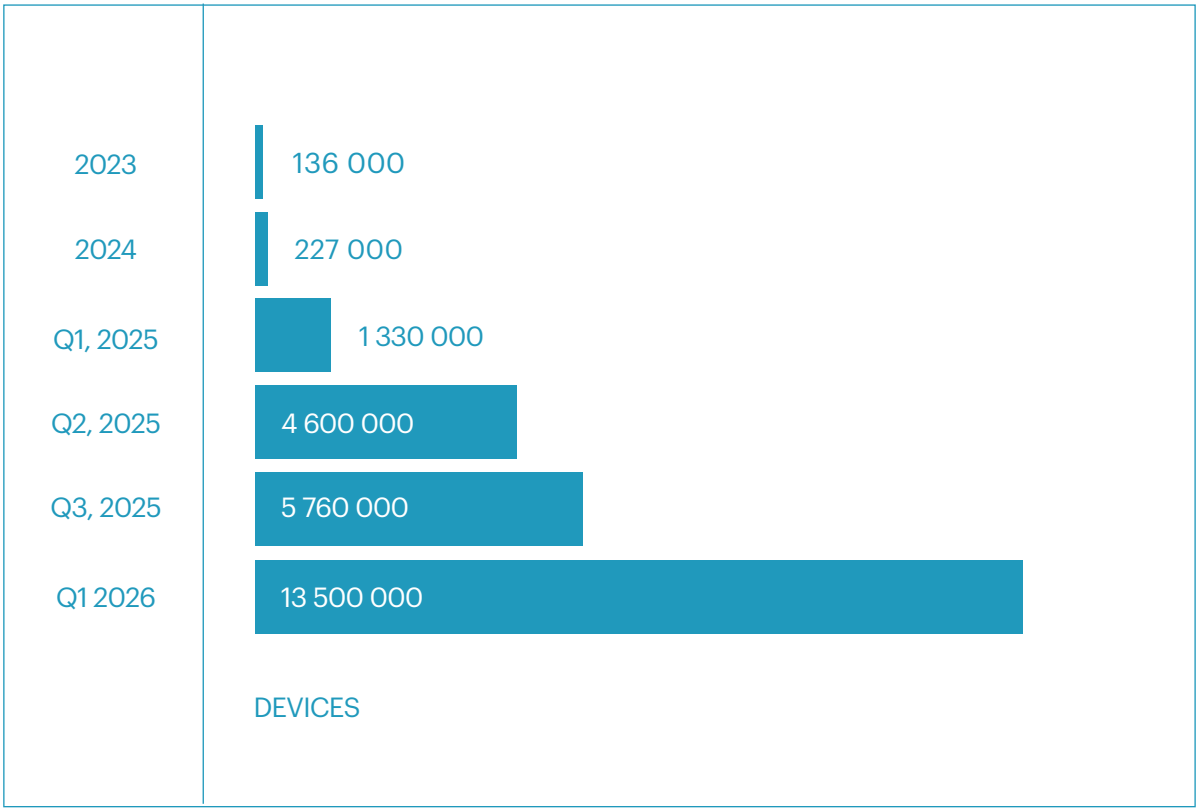


Betting shops	1	11	Software services
Marketplaces	2	12	Telecom operators
Hosting platforms	3	13	Classified ads
Media, TV, radio, and bloggers	4	14	Airports
Payment systems	5	15	Food retail
Forex	6	16	Government resources
Banks	7	17	Oil&Gas
Cryptocurrency exchanges	8	18	Social media
Game platforms	9	19	Various online services
Digital education	10	20	Government information portals

The largest DDoS botnet of Q1 2026

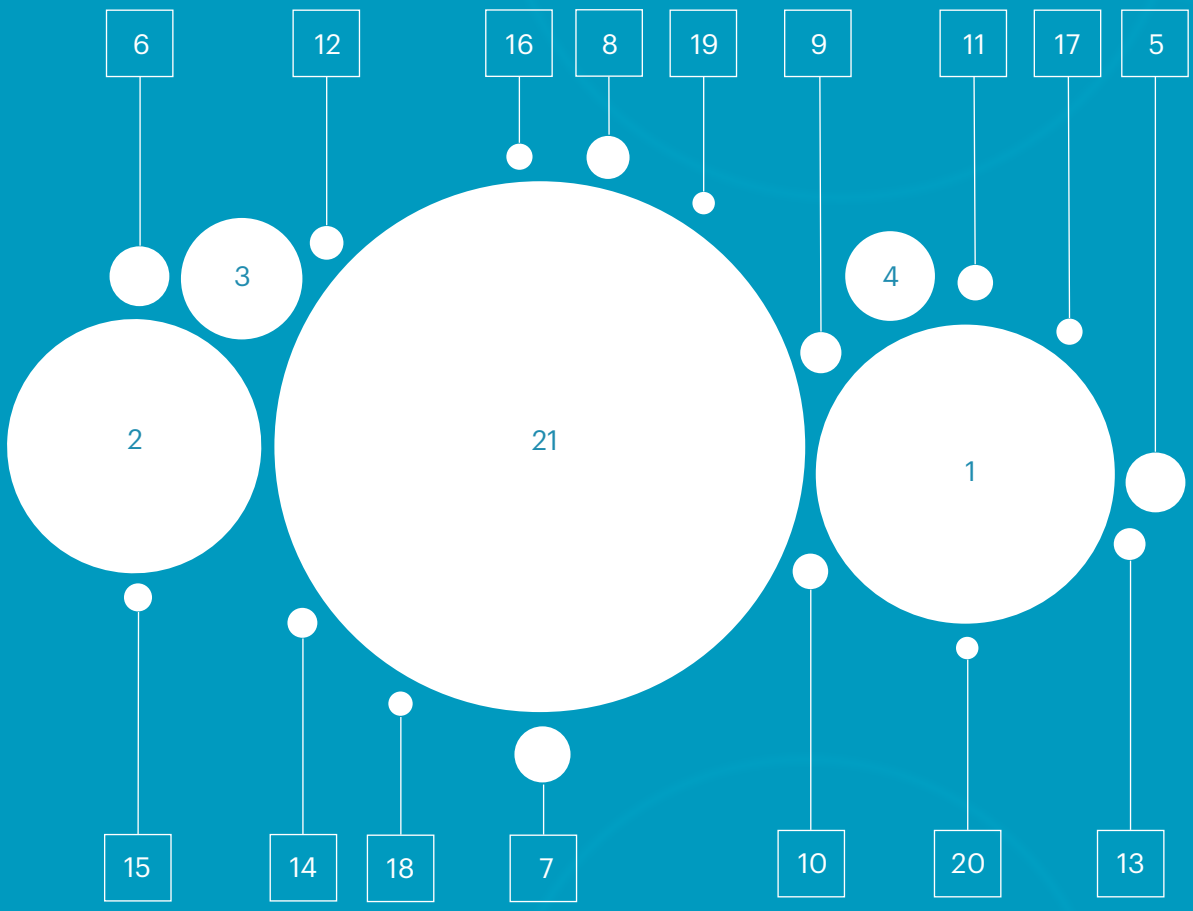
For the second year in a row, we have been monitoring the activity of a large DDoS botnet that we first detected on March 26, 2025. Over this period, the botnet has grown significantly: during the first attack we recorded a year ago, we blocked 1.33 million IP addresses, while during a wave of attacks in Q1 2026, this number reached 13.5 million. This represents more than a tenfold increase over the year.

The Largest botnet Q1, 2026



Also, the geographic distribution of the botnet changed significantly over the year. In Q1 2025, it was dominated by devices from Brazil (51.1%), with smaller shares from other developing countries, including Argentina (6.1%), Russia (4.6%), Iraq (3.2%), and Mexico (2.4%). By Q1 2026, the United States accounted for the largest share (16.0%), while Brazil's share declined to 13.6%. India (6.5%), the United Kingdom (4.8%), and Turkey (3.2%) also ranked among the top five.

Geographic distribution of the largest botnet of Q1 2026



1	16.0%	USA
2	13.6%	Brazil
3	6.5%	India
4	4.8%	Great Britain
5	3.2%	Turkey
6	3.2%	Saudi Arabia
7	3.0%	Russia

8	2.3%	Mexico
9	2.2%	Pakistan
10	1.9%	Argentina
11	1.9%	France
12	1.8%	Philippines
13	1.7%	Canada
14	1.6%	Morocco

15	1.5%	Spain
16	1.4%	Indonesia
17	1.4%	Ukraine
18	1.3%	Germany
19	1.2%	South Africa
20	1.2%	Iraq
21	28.4%	Others

The data shows that the operators of this botnet are not only continuously adding large numbers of newly infected devices, but also focusing on geographic diversification. This makes simple geo-blocking ineffective against DDoS attacks from this botnet, as the attackers can leverage IP addresses from virtually any country at any time.

Another notable development in Q1 2026 was the discovery of a new botnet loader known as Aeternum C2, which introduces a fundamentally different approach to command and control. Unlike traditional botnets that rely on centralized servers or domains, Aeternum uses the Polygon blockchain as its primary communication channel. Commands are written to smart contracts and retrieved by infected devices via public RPC endpoints, eliminating the need for conventional infrastructure.

This architecture makes the botnet highly resistant to disruption. There is no central server to seize, no domain to suspend, and no hosting provider to subpoena. As a result, traditional takedown strategies become significantly less effective. Combined with reduced operational costs, this model lowers the barrier to deploying persistent and scalable botnets.

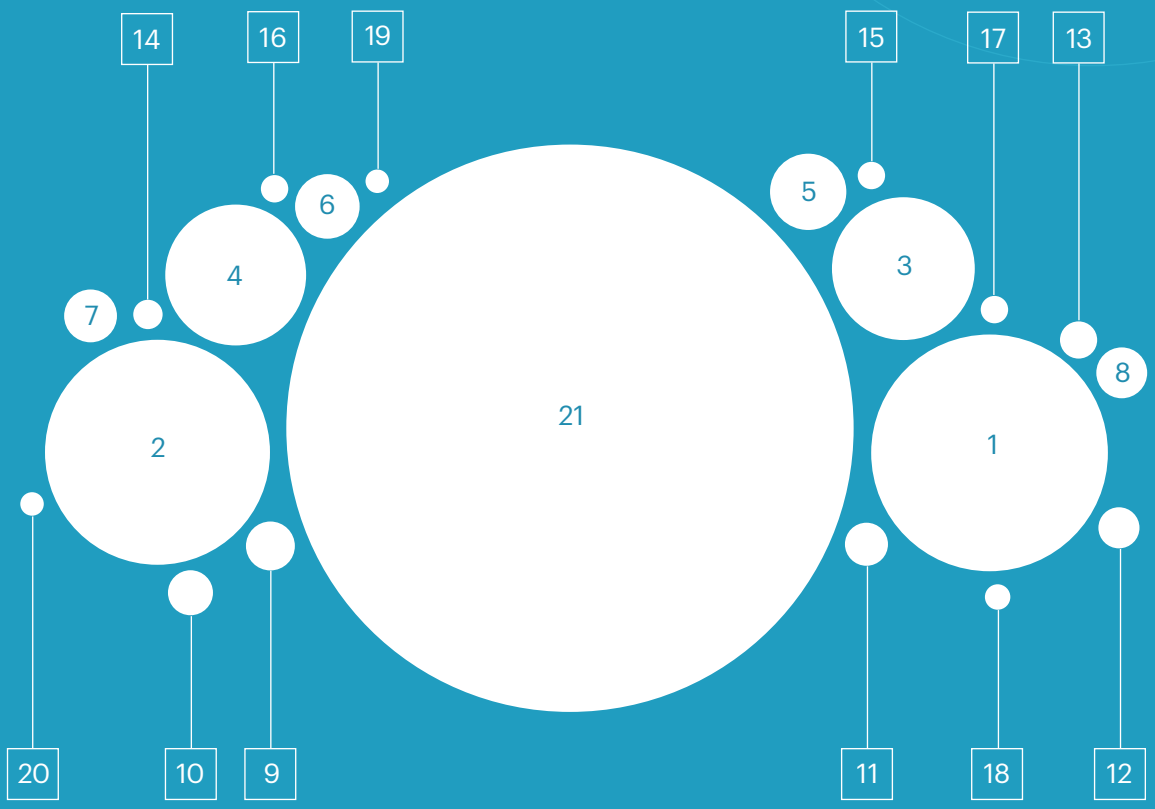
Geographic distribution of L7 DDoS attack sources in Q1 2026

Throughout the past year, we observed a steady trend of a rapidly increasing share of developing countries among the main sources of application-layer DDoS attacks. Most of this growth was concentrated in a few countries, primarily Brazil, Vietnam, and Argentina.

Based on the data for Q1 2026, this trend appears to be evolving: IP addresses from developing countries still account for a significant share of attack sources, but their distribution has become more even. While the top five countries accounted for 56.5% of all blocked IP addresses in 2025, their combined share declined to 42.0% in Q1 2026.

Another notable shift in Q1 2026 was the sharp increase in the share of the United States, which moved into second place with 11.5%. Brazil retained the top position with 12.1%, while Russia ranked third with 7.3% — a relatively modest share compared to both 2025 and 2024.

Geographic distribution of L7 DDoS attack sources in Q1 2026



1	12,1%	Brazil
2	11,5%	USA
3	7,3%	Russia
4	7,2%	Vietnam
5	3,9%	Argentina
6	3,3%	India
7	2,7%	Iraq
8	2,6%	Bangladesh
9	2,5%	Mexico
10	2,3%	Great Britain
11	2,2%	Pakistan
12	2,1%	Netherlands
13	1,9%	Germany
14	1,5%	China
15	1,4%	Singapore
16	1,4%	South Africa
17	1,4%	Venezuela
18	1,3%	Colombia
19	1,2%	Indonesia
20	1,2%	France
21	29,0%	Others

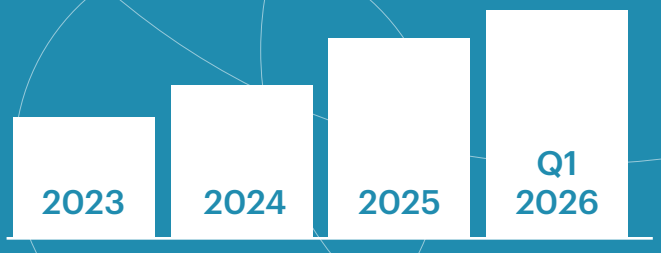
This data confirms the accelerating geographic diversification of IP addresses used by DDoS operators. As noted above, one consequence of this diversification is that simple geo-blocking becomes ineffective when mitigating large-scale attacks.

Bad bot protection statistics in Q1 2026 — Qrator.AntiBot

> "Bad bots" refer to automated systems that attempt to interact with websites while impersonating real users. Their typical objectives include data scraping, metric manipulation, credential stuffing, and other forms of unwanted activity. However, unlike destructive DDoS bots, bad bots usually do not aim to disrupt the availability of a website.

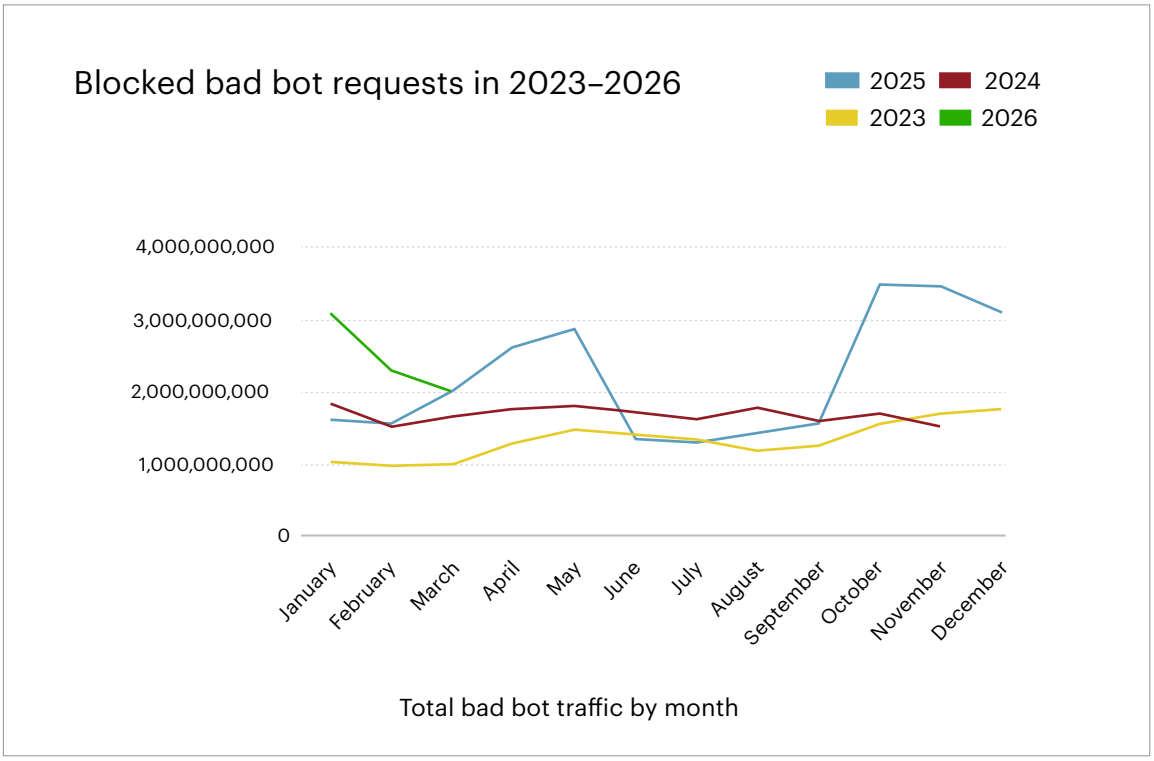
In Q1 2026, the average monthly number of blocked bad bot requests reached approximately 2.5 billion. Compared to Q1 2025, this represents an increase of about 40%, and a 12% increase relative to the overall average for 2025.

AVERAGE MONTHLY NUMBER OF BLOCKED BAD BOT REQUESTS IN 2023–2026



2023	1,338,167,816
2024	1,691,024,954
2025	2,208,203,424
Q1 2026	2,473,018,666

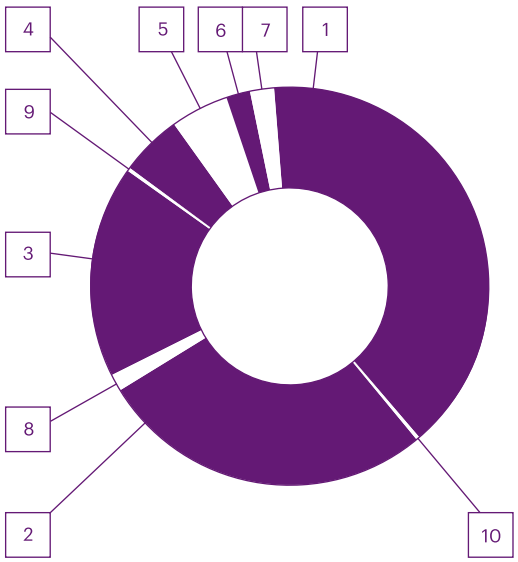
It is important to note that in 2025 we observed two periods of heightened bad bot activity, in Q2 and Q4. These spikes corresponded to two particularly large-scale attacks, each lasting for about a month. In 2026, we have not yet recorded bot attacks of comparable scale — so far, bot traffic is distributed more evenly across the protected resources.



Total bad bot traffic by month

In Q1 2026, as usual, the largest share of bad bot attacks targeted the E-commerce segment (40.21% of total bad bot activity). The Betting segment ranked second (27.09%), which is also typical. The Transport&Logistics segment ranked third this quarter, which is an unusual development (17.34%).

Bad bot activity by industry in Q1 2026

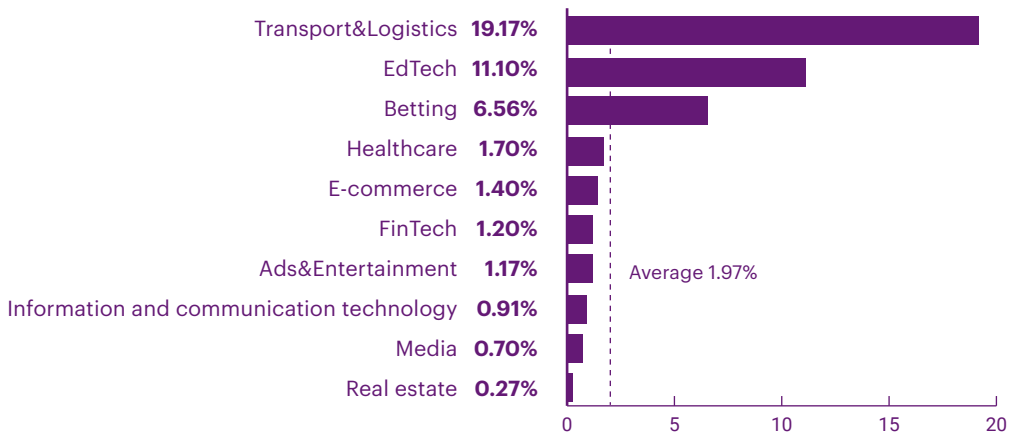


	%	
1	**40.21**	E-commerce
2	**27.09**	Betting
3	**17.34**	Transport&Logistics
4	**4.91**	Healthcare
5	**4.66**	Media
6	**2.03**	EdTech
7	**1.97**	FinTech
8	**1.48**	Real estate
9	**0.19**	Information and communication technology
10	**0.12**	Ads&Entertainment
	%	

Another anomaly observed in the Transport&Logistics segment is the exceptionally high share of bot traffic relative to total traffic on the protected resources (which we call the "bot index"). In Q1 2026, this figure reached 19.17%, meaning that nearly every fifth request in the Transport&Logistics segment was generated by bots.

A high share of bot traffic was also observed in the EdTech (11.10%) and Betting (6.56%) segments. Across all segments, the average bot index in Q1 2026 stood at 1.97%, slightly below the level observed over the last nine months of 2025, but still remaining high.

Share of bad bot requests in total traffic by industry in Q1 2026



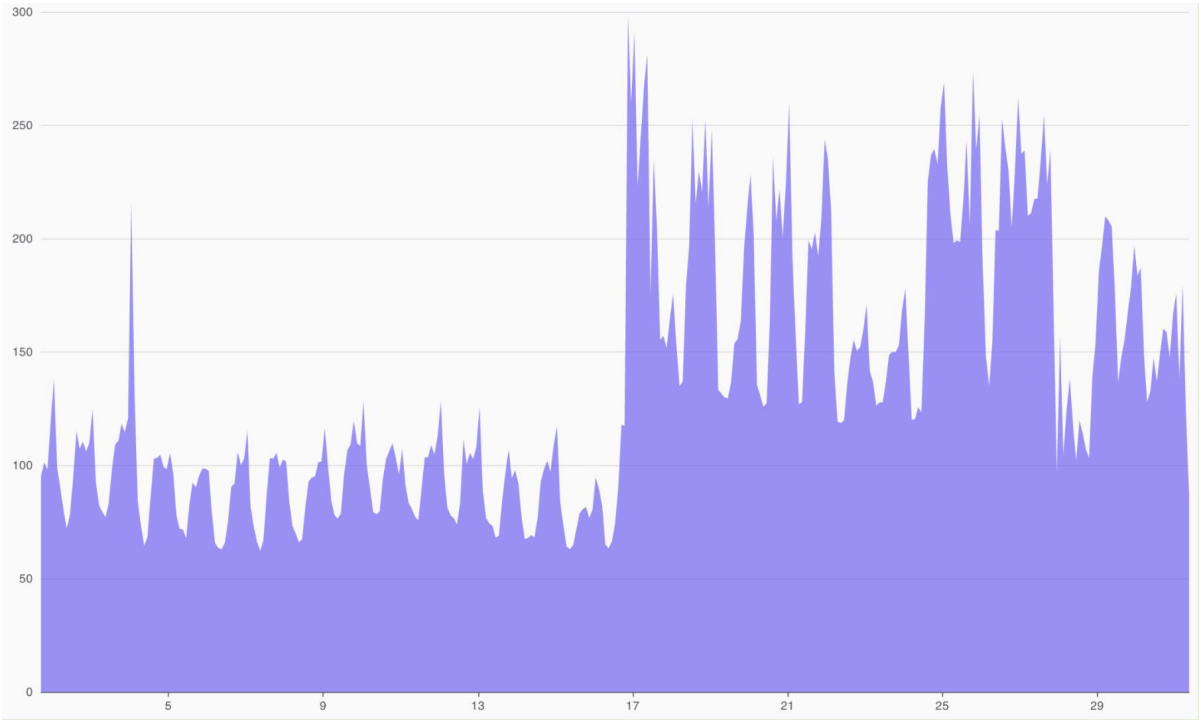
It should be noted that Qrator.AntiBot allows customers to configure where protection is applied — including specific pages and domains. As a result, our bot index may not account for a significant portion of bot traffic.

The distribution of bots by type in Q1 2026 was as follows: simple scripted bots accounted for the majority (65.23%). “Puppeteer” bots — those that simulate a real user environment while being controlled through external automation — made up 2.47%. Smart bots, which are aware of detection mechanisms and attempt to bypass them, accounted for 0.28%. Finally, API bots represented 32.02% of bot traffic.

Bad bot activity by type in Q1 2026

Most notable bad bot attacks in Q1 2026

The longest bad bot attack of Q1 2026 occurred in March and lasted for more than two weeks. It targeted an organization in the E-commerce segment, with the total number of blocked requests exceeding 178 million.



The longest bad bot attack of Q1 2026

The most intensive attack blocked by Qrator.AntiBot in Q1 2026 was recorded in early March and also targeted an organization in the E-commerce segment. Its peak intensity exceeded 120 thousand malicious requests per second. The attack was not aimed at data exfiltration or compromising the resource — it was a DDoS attack at the application layer.

BGP INCIDENTS in Q1 2026

The number of unique autonomous systems (ASes) responsible for route leaks in Q1 2026 remained at the level of the previous year, averaging 1,913 per month. Meanwhile, the number of unique ASes involved in BGP hijacks decreased noticeably compared to the previous year: the monthly average fell from 8,587 in 2025 to 7,619 in Q1 2026, representing a decline of more than 10%.

UNIQUE ROUTE LEAKER ASes	Q1, 2026	UNIQUE BGP HIJACKER ASes
1,823	January	9,432
1,960	February	6,294
1,955	March	7,130

Global BGP incidents in Q1 2026

To identify global BGP incidents, the Qrator.Radar team applies a set of threshold criteria, including the number of affected prefixes and autonomous systems, as well as the extent of anomaly propagation across routing tables.

The number of global BGP incidents in Q1 2026 was high: over the course of the quarter, we recorded seven global route leaks and one global BGP hijack.

GLOBAL BGP ROUTE LEAKS	Q1, 2026	GLOBAL BGP HIJACKS
0	January	0
4	February	0
3	March	1

web: qrator.net
e-mail: sales@qrator.net
tel.: +420 602 558 144