

qrator.net



2024 DDOS ATTACKS, BOTS AND BGP INCIDENTS STATISTICS AND OVERVIEW

Executive summary

- The total number of DDoS attacks in 2024 increased by 53% compared to 2023.
- The largest number of L3-L4 DDoS attacks in 2024 targeted the “Fintech” (25.8%), “E-commerce” (20.5%), and “Media” (13.5%) segments.
- The most powerful DDoS attack of 2024 peaked at 1.14 Tbps, which is 65% higher than the previous year’s record of 0.69 Tbps.
- The largest botnet we detected in 2024 consisted of 227,000 devices (compared to the largest botnet in 2023, which included “just” about 136,000 devices). This rapid growth in botnet size is attributed to the rising number of outdated devices in developing countries.
- The longest DDoS attack in 2024 lasted 19 days, compared to the 2023 record of just 3 days. The increase in attack duration on protected systems may be attributed to the aforementioned growth in botnet size, which has likely made attacks more cost-effective for threat actors.
- The share of multivector attacks in 2024 increased by 8% compared to 2023.
- More than half (52%) of all L7 DDoS attacks in 2024 targeted the “Fintech” segment. Notably, nearly one-third of all attacks this year (31.9%) were directed at the “Banks” microsegment.
- The “E-commerce” macrosegment ranked second in the number of application-level attacks, accounting for 18%, while the “Online retail” (10%) ranked second among microsegments.
- The longest L7 attack of 2024 lasted 49.1 hours. The most intense attack reached 1.56 million rps. The highest number of devices involved in an attack was 1,472,941.

- The top sources of DDoS attacks in 2024 were Russia (32.4%), the United States (20.6%), and Brazil (5.8%). China, which had consistently ranked third in the past, fell out of the top three by year-end.
- Average monthly bot activity in 2024 increased by 30% compared to 2023.
- The number of BGP incidents in 2024 saw a slight increase compared to 2023: the average monthly number of BGP route leaks rose by 10%, while BGP hijacks increased by 24%.
- The number of global BGP incidents also grew significantly: in 2024, we recorded 59% more global BGP route leaks and 25% more global BGP hijacks compared to 2023.
- In the third quarter, we recorded a successful prevention of a global route leak between IXs, enabled by the use of the RFC 9234 standard developed by Qrator Labs experts.

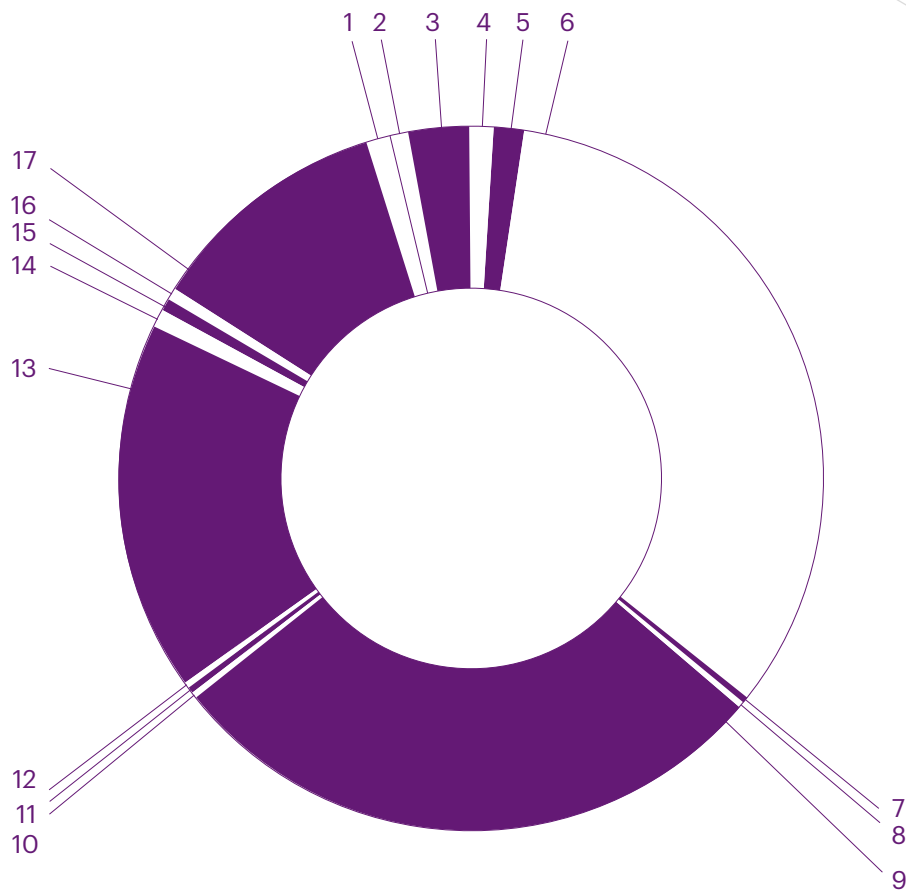
DDoS Attacks Targeting the Network and Transport Layers (L3-L4)

We remind you that since the first quarter of 2024, we updated our data collection methodology to account for the increase in channel capacity and attack volume. We now exclude all incidents with an intensity of less than 1 Gbps as “background noise,” which helps us focus on the most significant events. First and foremost, it is worth noting a significant increase in the to-

tal number of DDoS attacks we recorded in 2024, which grew by 53% compared to the previous year.

Regarding attack vector distribution, UDP flood attacks led the way with a 33.6% share for the year. IP fragmentation flood attacks ranked second at 28%, followed by TCP flood attacks in third place with a 17% share.

Attack vectors concurrency

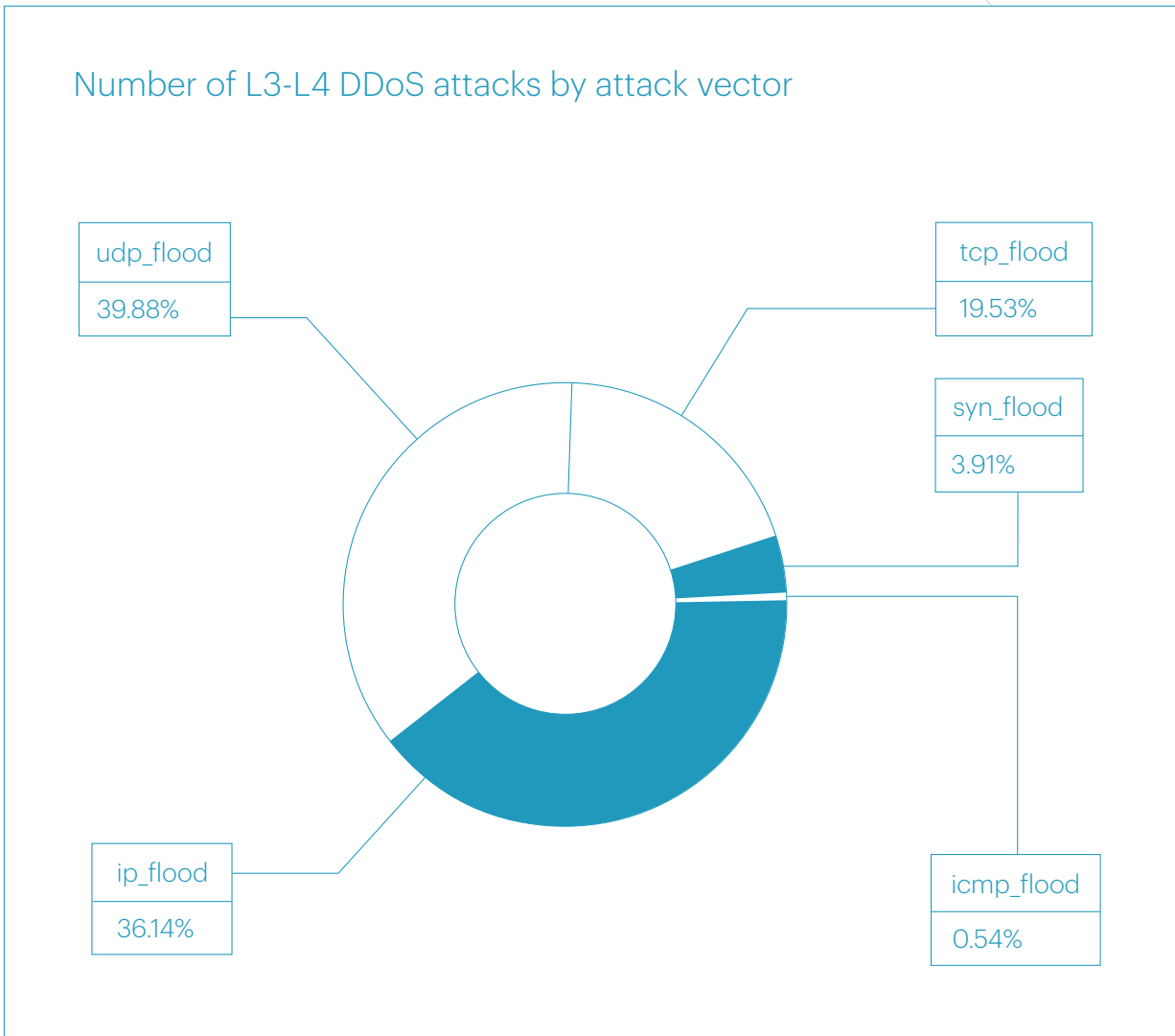


1	1.04%	syn_flood			
2	0.77%	tcp_flood	udp_flood		
3	2.86%	tcp_flood	ip_flood	udp_flood	
4	1.18%	tcp_flood	syn_flood	ip_flood	udp_flood
5	1.11%	tcp_flood	ip_flood		
6	33.57%	udp_flood			
7	0.14%	ip_flood	icmp_flood		
8	0.14%	tcp_flood	udp_flood	ip_flood	icmp_flood
9	27.99%	ip_flood			
10	0.14%	icmp_flood			
11	0.35%	tcp_flood	syn_flood	udp_flood	
12	0.35%	syn_flood	ip_flood		
13	16.99%	tcp_flood			
14	0.70%	tcp_flood	syn_flood	ip_flood	
15	0.63%	tcp_flood	syn_flood		
16	0.49%	syn_flood	ip_flood	udp_flood	
17	11.21%	ip_flood	udp_flood		

The total share of multivector attacks in 2024 saw a modest increase, reaching 20.3% — approximately 8% higher than in 2023. This once again highlights the fact that DDoS attackers recognize the effectiveness of multivector attacks, particularly against unprotect-

ted or poorly secured infrastructures, and continue to exploit their advantages.

Excluding mixed attack vectors, the distribution of “pure” vectors in 2024 was as follows:



L3-L4 DDoS Attacks Duration

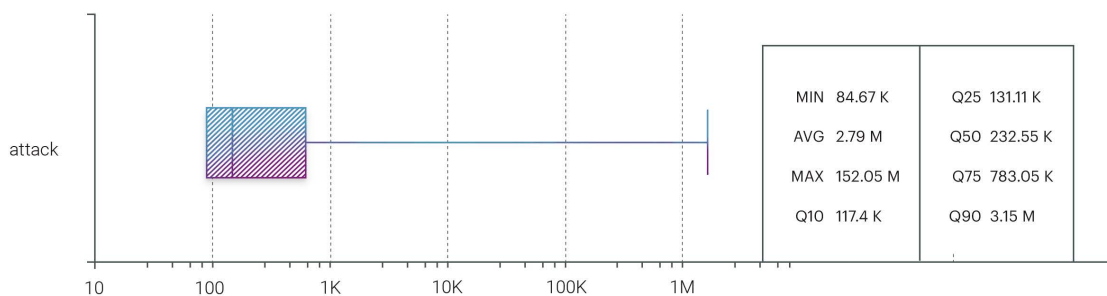
The longest attack in 2024 lasted nearly 464 hours, or over 19 days — several times longer than the 2023 record of approximately 72 hours. This attack occurred in the first quarter and targeted the “E-commerce” segment, specifically the “Online retail” microsegment.

A possible explanation for the sharp increase in maximum attack duration could be the use of massive botnets composed of outdated and vulnerable consumer devices (discussed further below). These botnets provide attackers with nearly inexhaustible resources.

In the past, attackers were incentivized to stop an attack if it failed to achieve the desired effect (as a reminder, all attacks we monitor target protected systems and are therefore inherently unsuccessful). However, with access to free and virtually unlimited botnet resources, attackers may completely disregard the effectiveness of an attack, continuing it for weeks even when it serves no practical purpose.

One could even envision a scenario where such a botnet continues an endless DDoS attack because its operator loses control of the botnet or simply ceases to function (for instance, due to an accident).

L3-L4 DDoS attack duration in seconds



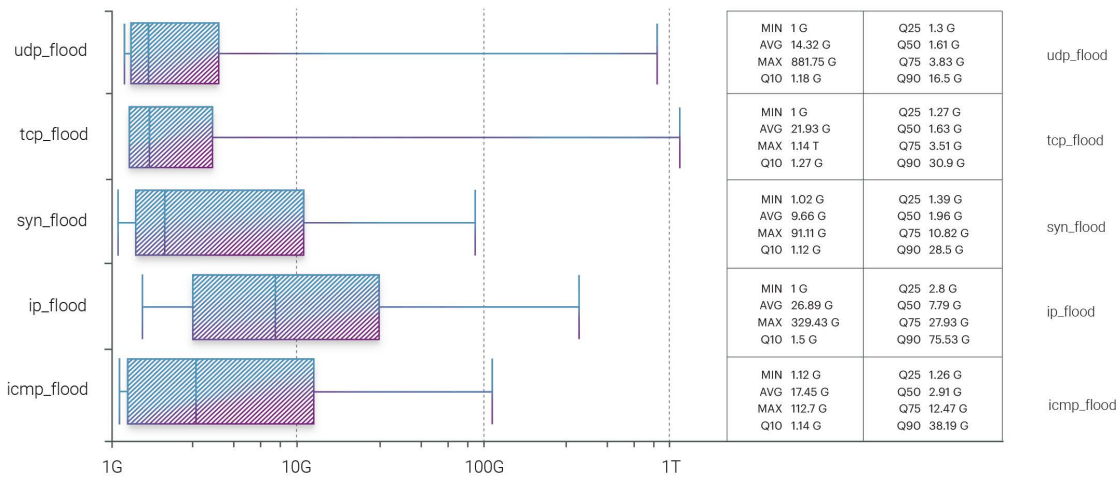
L3-L4 DDoS Attacks Bitrate And Packet Rate

The most powerful L3-L4 DDoS attack in 2024 reached a bitrate of 1.14 Tbps — 65% higher than last year’s record of 0.69 Tbps. This attack occurred in the fourth quarter and targeted the “Media, TV, radio, bloggers” microsegment.

The full statistics for maximum attack bitrates across different attack vectors in 2024 are as follows:

- TCP flood: 1140 Gbps
- UDP flood: 882 Gbps
- IP fragmented flood: 329 Gbps
- ICMP flood: 113 Gbps
- SYN flood: 91 Gbps

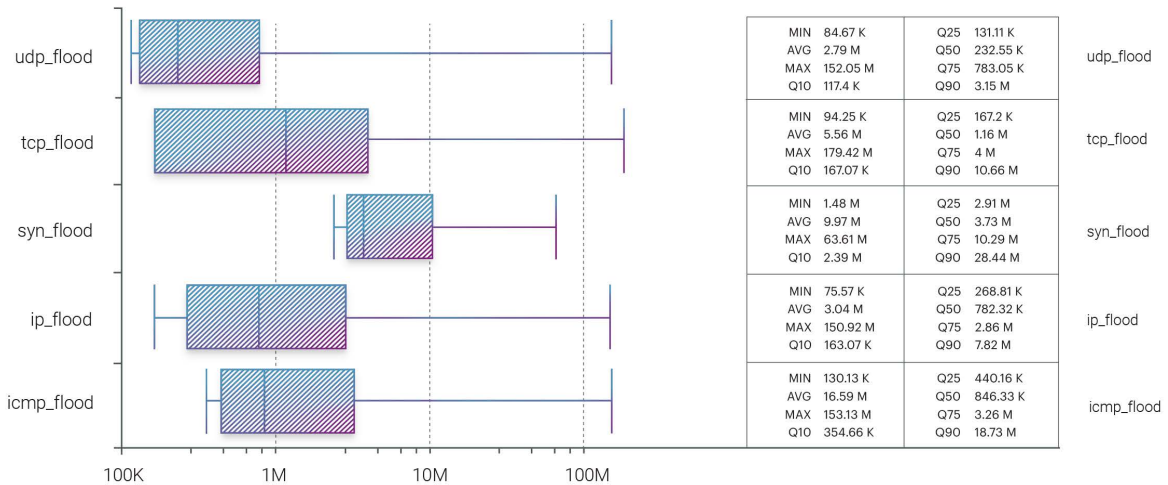
L3-L4 DDoS attack volume in bits per second (bps) by attack vector



The attack intensity by packet rate in 2024 is as follows:

- TCP flood: 179 Mpps
- ICMP flood: 153 Mpps
- UDP flood: 152 Mpps
- IP fragmented flood: 151 Mpps
- SYN flood: 64 Mpps

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

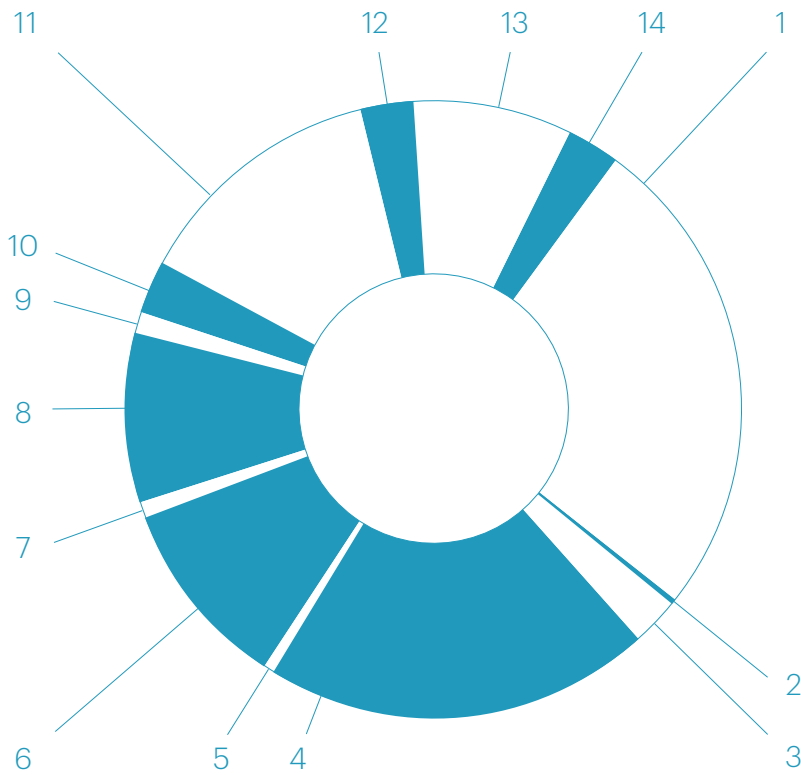


L3-L4 DDoS Attacks Distribution by Industry Segment

The primary targets of L3-L4 DDoS attacks in 2024 were the “Fintech” (25.8%) and “E-commerce” (20.5%) segments. Together, these two accounted for nearly half of all attacks recorded during the year.

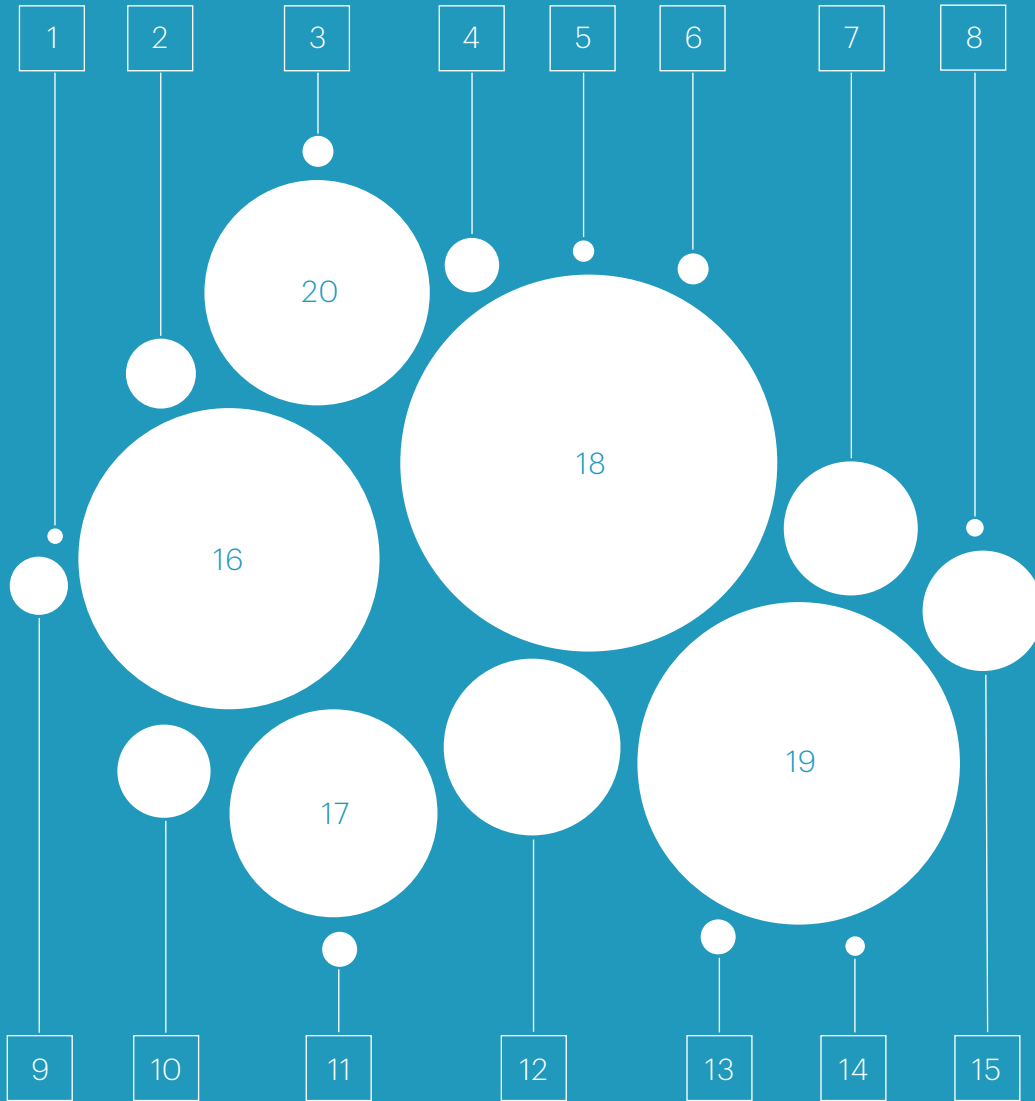
The top five most targeted sectors also included “Media” (13.5%), “IT&Telecom” (10.1%), and “Betting” (8.9%). Collectively, these top five segments represented nearly 80% of all attacks registered in 2024.

Macrosegmentation of L3-L4 DDoS attacks



1	25.83	FinTech	8	8.86	Betting
2	0.25	Ads&Entertainment	9	1.08	Industrial
3	2.32	Games	10	2.73	Other
4	20.45	E-commerce	11	13.49	Media
5	0.50	Healthcare	12	2.73	Transport&Logistics
6	10.10	IT&Telecom	13	8.36	EdTech
7	0.75	Real Estate	14	2.57	Government

A more detailed segmentation shows that the largest number of attacks in 2024 targeted the microsegments "Banks" (16.1%), "Online retail" (13.7%), "Media, TV, radio, bloggers" (12.8%), "Betting shops" (8.9%), and "Digital education" (7.5%). Together, these five microsegments accounted for nearly 60% of all L3-L4 attacks in 2024.



1	0.66%	Social networks	11	1.49%	Food retail
2	2.98%	Hosting platforms	12	7.53%	Digital education
3	1.32%	Forex	13	1.49%	Microfinance organizations
4	2.32%	Game platforms	14	0.83%	InsurTech
5	0.91%	Airports	15	5.13%	Payment systems
6	1.32%	Telecom operators	16	12.83%	Media, TV, Radio, Bloggers
7	5.71%	Software services	17	8.86%	Betting shops
8	0.75%	Logistics	18	16.06%	Banks
9	2.48%	Governmental resources	19	13.74%	Online retail
10	3.97%	Classified ads	20	9.60%	Other

L3-L4 DDoS Attacks Duration by Industry Segment

The five longest DDoS attacks of 2024 were led by the previously mentioned attack on “Online retail,” which lasted nearly three weeks (463.9 hours). The second and third longest attacks targeted the microsegments “Airports” and “Betting

shops,” lasting approximately three days each (72 and 71.8 hours, respectively).

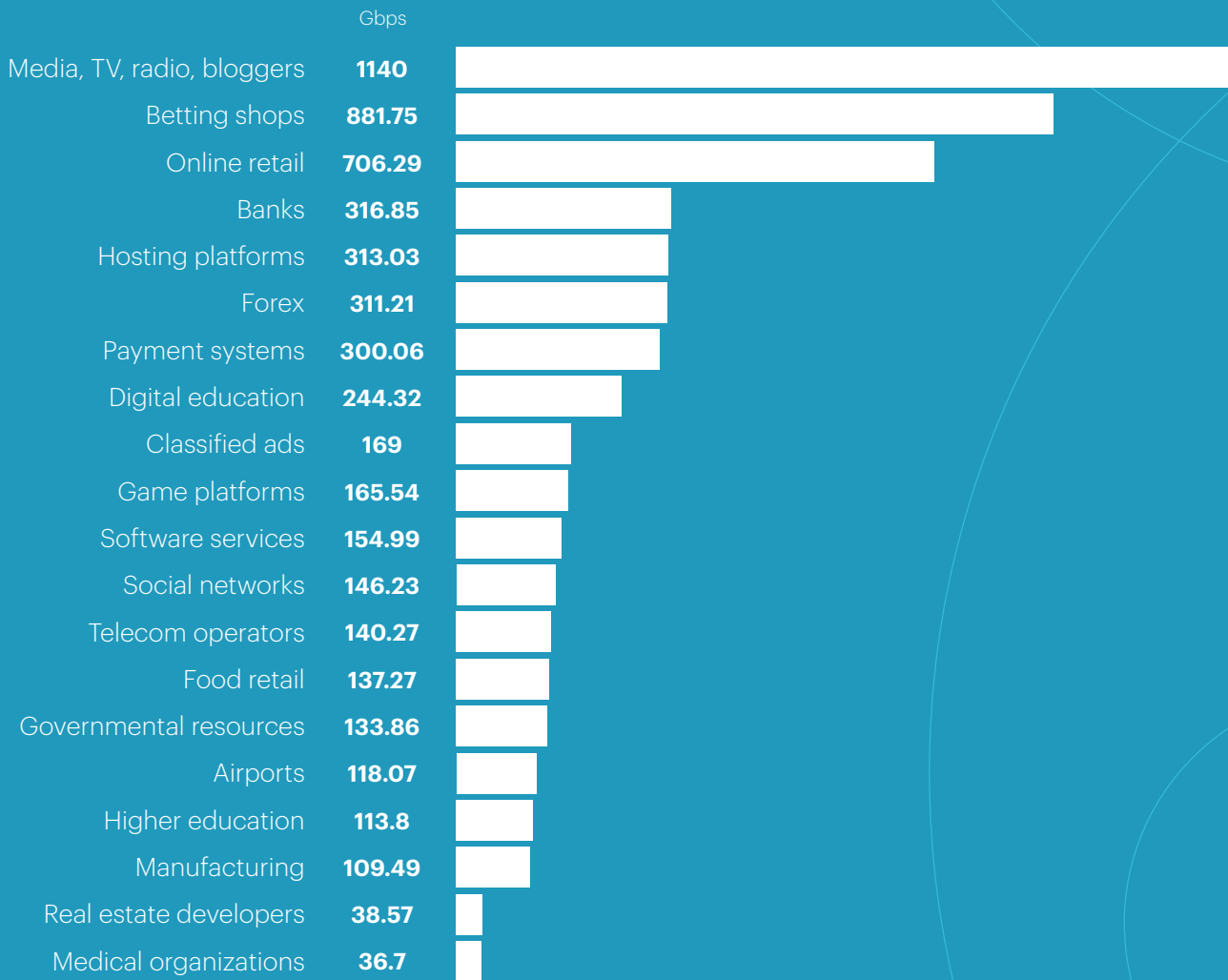
Other relatively lengthy attacks were directed at the microsegments “Banks” (22.3 hours), “Services” (14.2 hours), and “Media, TV, radio, bloggers” (13 hours).

L3-L4 DDoS Attacks Bitrate and Packet Rate by Industry Segment

As mentioned earlier, the most powerful L3-L4 attack of 2024 targeted the “Media, TV, radio, bloggers” microsegment, reaching a bitrate of over 1 Tbps — 1140 Gbps. Two other significant attacks in 2024 were recorded in the “Betting shops” (882 Gbps) and “Online retail” (706 Gbps) microsegments. All three of these attacks surpassed the 2023 record of 690 Gbps.

Additionally, in 2024, we recorded four more attacks exceeding 300 Gbps. These targeted the microsegments “Banks” (317 Gbps), “Hosting platforms” (313 Gbps), “Forex” (311 Gbps), and “Payment systems” (300 Gbps).

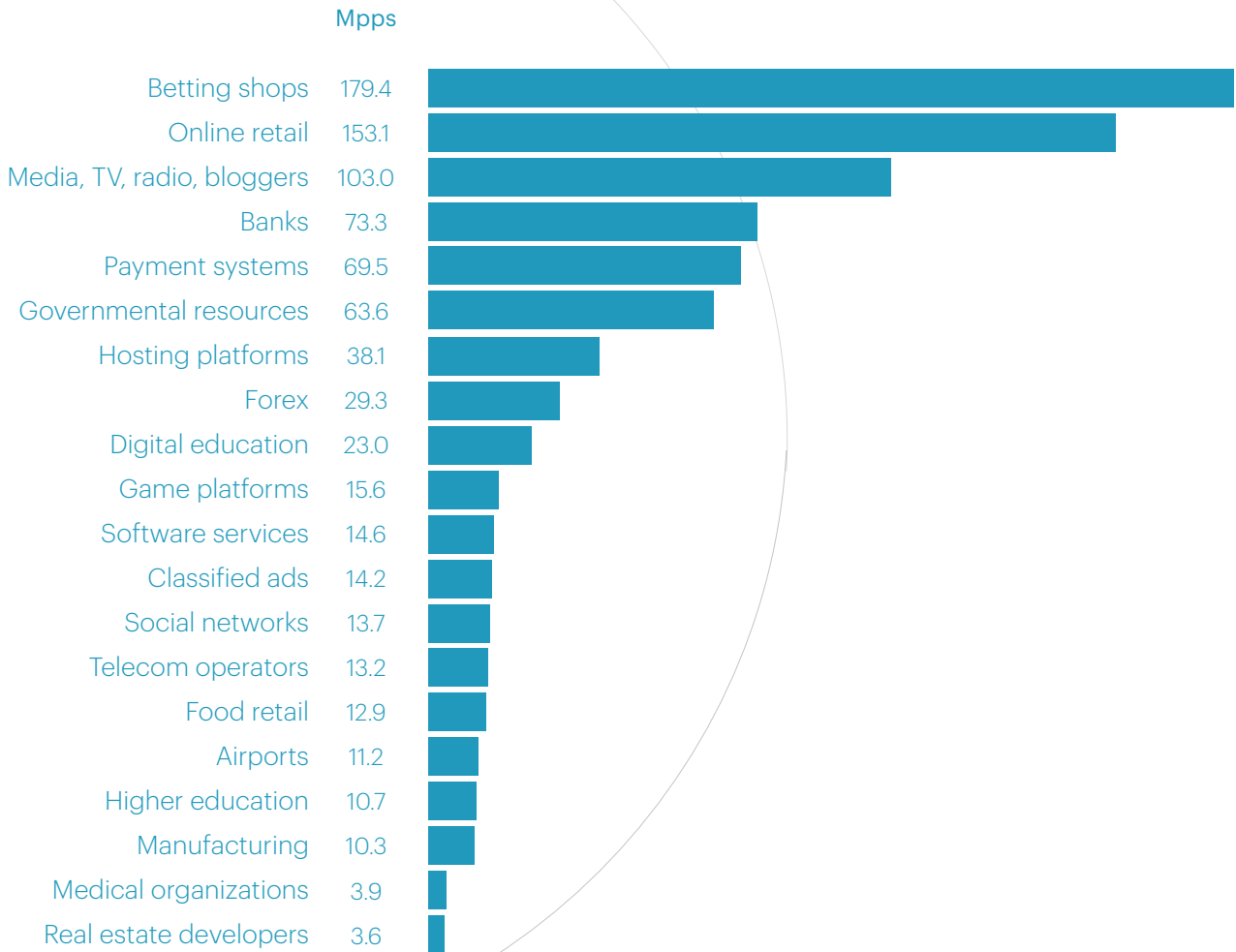
Max L3-L4 DDoS attack bitrate by industry



In terms of maximum packet transmission rate, the top three most targeted microsegments remain the same but appear in a slightly different order: the

“Betting shops” microsegment takes the top spot (179 Mpps), followed by “Online retail” (153 Mpps), with “Media, TV, radio, bloggers” in third place (103 Mpps).

Max L3-L4 DDoS attack packet rate by industry



The Largest Botnet

The largest botnet of 2024 was detected in the fourth quarter. At its peak, it consisted of 227,000 devices — 67%

more than the largest botnet of 2023, which was composed of approximately 146,000 devices.

THE LARGEST BOTNET



This botnet targeted the “Banks” micro-segment, with the attack unfolding in several stages. The first wave (November 19) involved 165,000 devices. A few days later, on November 23, the second and most significant wave occurred, utilizing over 227,000 bots. The third phase (November 26) was considerably weaker than the first two, involving only 69,000 devices.

In terms of geographic distribution, the botnet primarily consisted of devices from Brazil (77.4%), Vietnam (5.7%), Argentina (1.7%), Russia (1.3%), and Ecuador (1.1%). Additionally, smaller numbers of devices (less than 1% from each country) came from Turkey, South Africa, Iraq, Colombia, Morocco, Pakistan, Tunisia, and Venezuela.

GEOGRAPHIC DISTRIBUTION OF THE LARGEST BOTNET

77.4%	BRAZIL
5.7%	VIETNAM
1.7%	ARGENTINA
1.3%	RUSSIA
1.1%	ECUADOR
0.9%	TÜRKIYE
0.9%	SOUTH AFRICA
0.9%	IRAQ
0.8%	COLOMBIA
0.7%	MOROCCO
0.6%	PAKISTAN
0.5%	TUNISIA
0.5%	VENEZUELA

We predict that such massive botnets will become increasingly common in the future. This trend is driven by three key factors:

- 1 Slowing growth in the performance and functionality of digital devices. As a result, people replace their devices less frequently, often using them for five years or more. This is particularly true for users in developing countries.
- 2 Short product life cycle of these devices. The duration of software support for these devices remains very limited, typically extending to only 3–4 years at best.
- 3 Continued improvements in connection quality and speed.

As a result, tens or even hundreds of millions of permanently vulnerable devices are connected to fast and reliable networks worldwide, particularly in developing

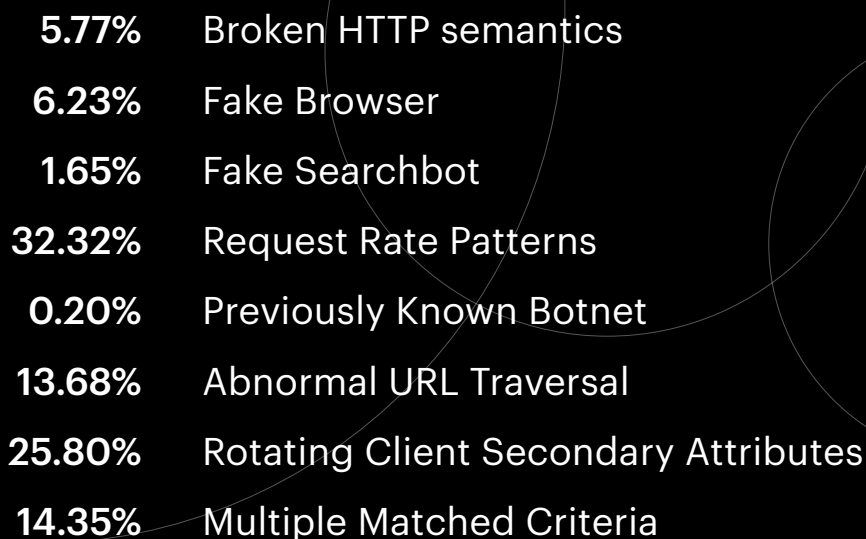
countries. This provides attackers with free and virtually unlimited resources for DDoS attacks.

DDoS Attacks Targeting the Application Layer (L7)

The number of application layer attacks in 2024 saw a slight decline compared to the previous year. The top three most common attack classes remained unchanged: the largest share belonged to Request Rate Patterns (32.3%), characterized by request frequencies deviating from the expected behavior of legitimate users.

The second most common class was Rotating Client Secondary Attributes (25.8%) — attacks with an unusual set of headers in the request. Multiclass attacks categorized under Multiple Matching Criteria (14.4%) took third place.

L7 DDOS ATTACKS BY TYPE

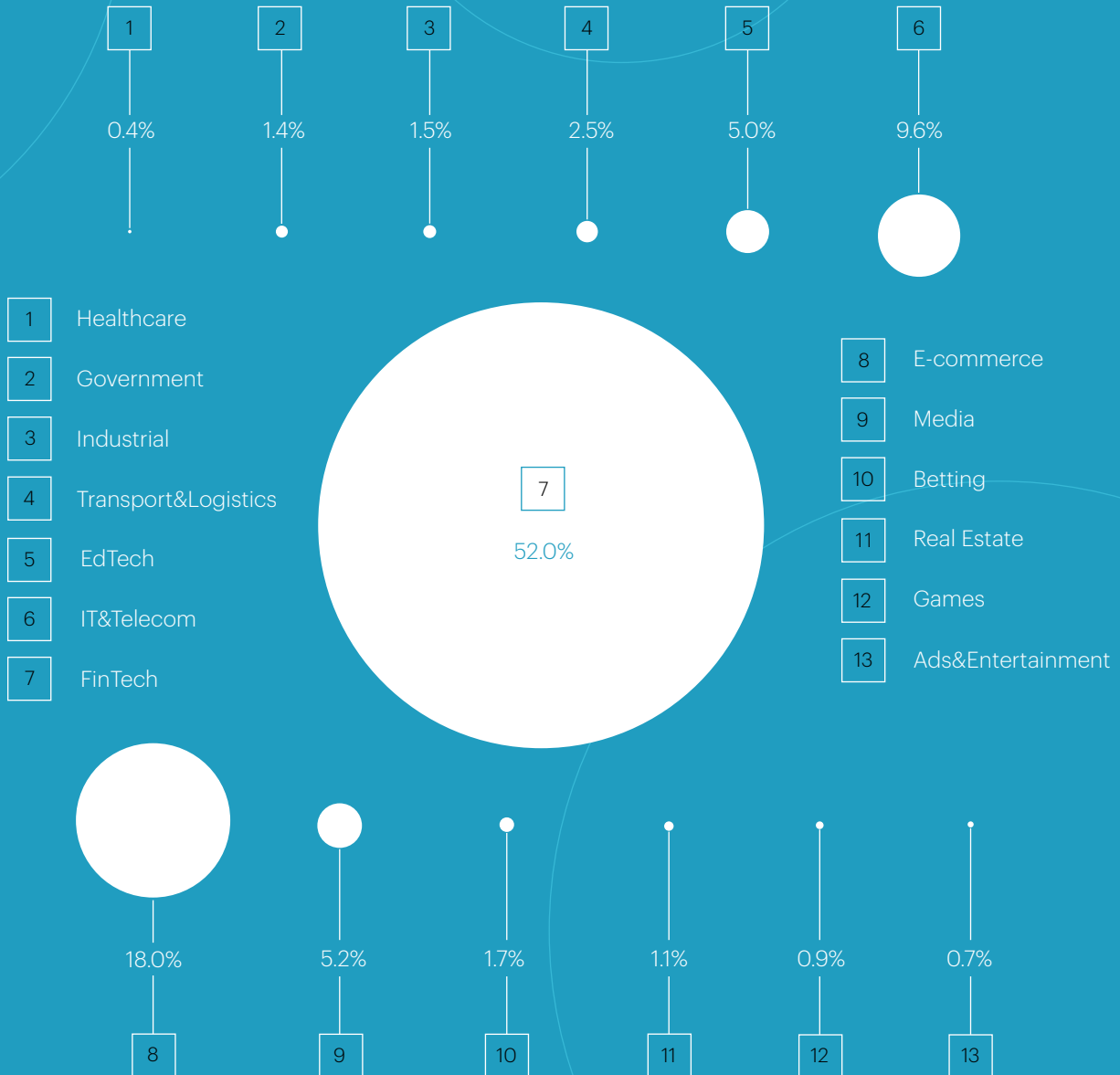


5.77%	Broken HTTP semantics
6.23%	Fake Browser
1.65%	Fake Searchbot
32.32%	Request Rate Patterns
0.20%	Previously Known Botnet
13.68%	Abnormal URL Traversal
25.80%	Rotating Client Secondary Attributes
14.35%	Multiple Matched Criteria

L7 DDoS Attacks Distribution by Industry Segment

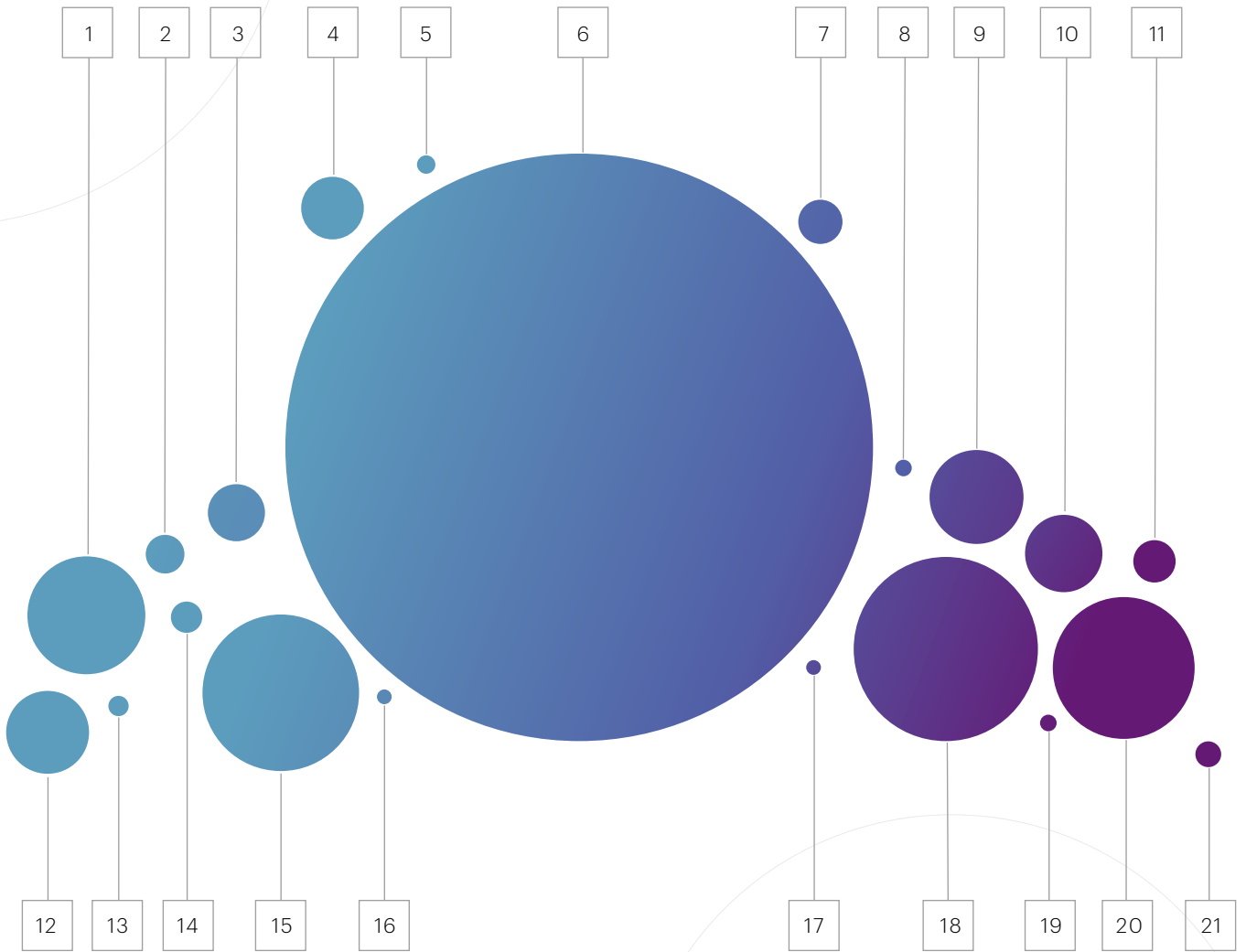
The largest number of L7 DDoS attacks in 2024 targeted the macrosegments “Fin-tech” (52%), “E-commerce” (18%), and “IT&Telecom” (9.6%). Together, these three segments accounted for nearly 80% of all application-level attacks we recorded in 2024

Macrosegmentation of L7 DDoS Attacks



Among microsegments, the most targeted were “Banks” (31.9%), “Online retail” (10%), “Payment systems” (7.7%), “Software” (6.4%), and “InsurTech” (5.1%).

Microsegmentation of L7 DDoS attack sources



- | | | |
|---------------------------------|---|-------------------------------------|
| 1 Software services 6.4% | 8 Real estate developers 0.9% | 15 Other 8.5% |
| 2 Hosting platforms 2.1% | 9 InsurTech 5.1% | 16 Telecom operators 0.8% |
| 3 Classified ads 3.1% | 10 Media, TV, radio, bloggers 4.2% | 17 Travel 0.8% |
| 4 Food retail 3.4% | 11 Microfinance organizations 2.3% | 18 Online retail 10.0% |
| 5 Social networks 1.0% | 12 Digital education 4.5% | 19 Manufacturing 0.9% |
| 6 Banks 31.9% | 13 Investment platforms 1.1% | 20 Payment systems 7.7% |
| 7 Forex 2.4% | 14 Betting shops 1.7% | 21 Government resources 1.4% |

L7 DDoS Attacks Duration and RPS by Industry Segment

The longest L7 DDoS attack of 2024 occurred in the second quarter and targeted the “Telecom operators” microsegment. It began on April 10 and lasted for over two days — 49.1 hours.

The second longest attack of the year also took place in the second quarter, shortly before the first one. It targeted the “Payment systems” microsegment and similarly lasted just over two days — 48.2 hours.

Finally, the third longest attack of 2024 was recorded in the fourth quarter and targeted the “Online Classifieds” microsegment. It lasted 35.9 hours.

The top three most intense attacks in 2024 were as follows:

- 1.56 million rps: The attack occurred in the second quarter and targeted the “Betting Shops” microsegment.
- 0.95 million rps: The attack took place in the third quarter and was aimed at the “Online Classifieds” microsegment.
- 0.68 million rps: Like the first attack, this one also occurred in the second quarter and targeted the “Betting Shops” microsegment.

For comparison, the longest application-level attack in 2023 lasted 76.8 hours, and the maximum attack intensity last year reached 0.98 million rps.

As for the maximum number of devices involved in an attack, all records were set quite recently, in the fourth quarter:

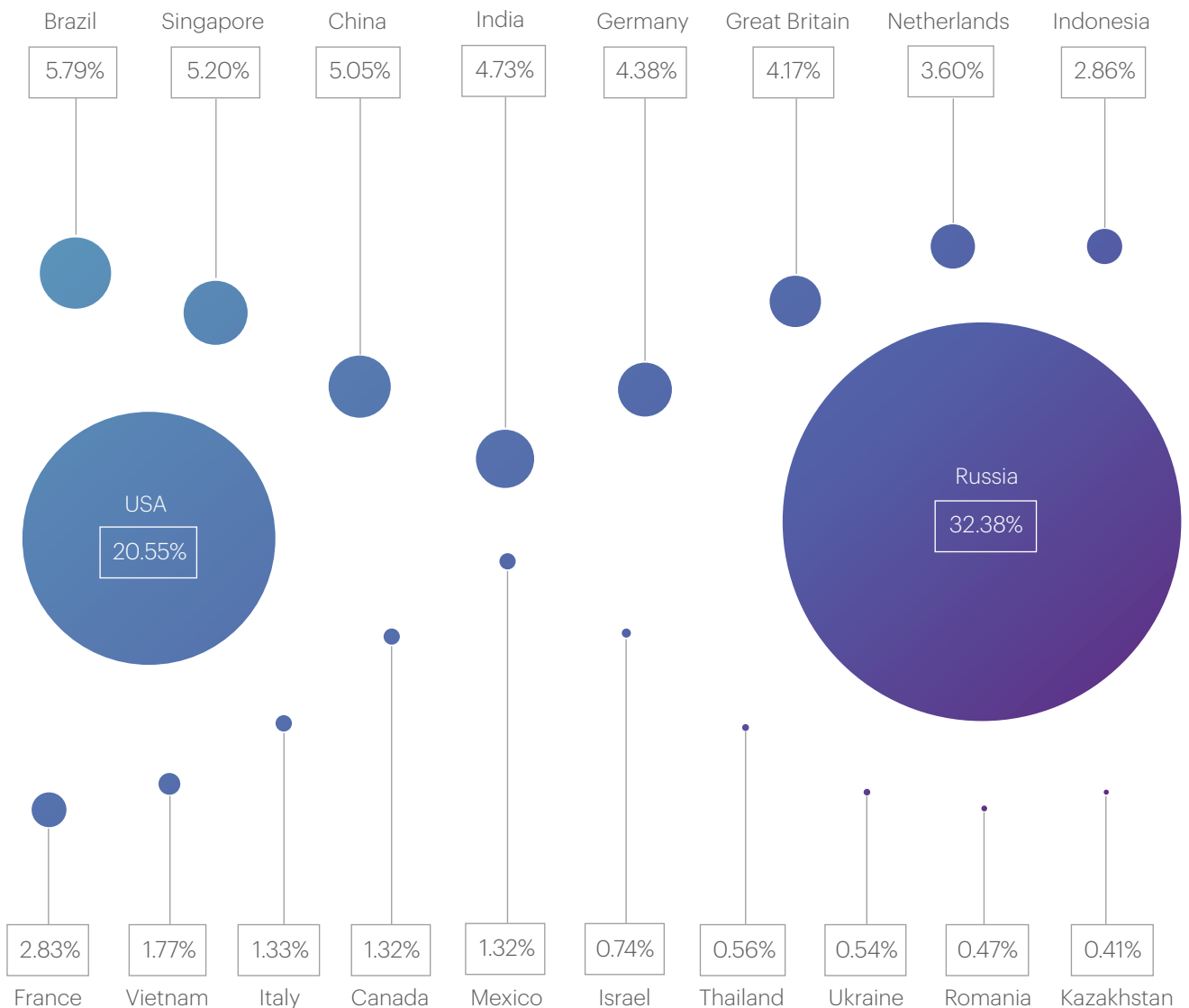
- 1,472,941 devices — an attack targeting the “Government Resources” microsegment.
- 1,335,104 devices — another attack on the “Government Resources” microsegment.
- 923,770 devices — an attack targeting the “Payment Systems” microsegment.

Geographical Distribution of DDoS Attack Sources

The list of countries most frequently serving as sources of DDoS attacks saw minor changes in 2024 compared to 2023. Russia (32.4%) and the United States (20.6%) retained the top two spots. However,

China, which had consistently held third place, dropped out of the top three starting in the second quarter. By the end of the year, Brazil had taken its place with 5.8%.

Geographical distribution of DDoS attack sources



Singapore (5.2%), China (5.1%), India (4.7%), Germany (4.4%), the United Kingdom (4.2%), the Netherlands (3.6%), and Indonesia (2.9%) also ranked among the top

10 sources of malicious traffic in 2024. Collectively, these ten countries were responsible for nearly 90% of all blocked IP addresses.

Bot Protection Statistics

In 2024, the number of blocked bot requests increased by 30% compared to 2023. On average, we blocked 1.69 billion such

requests per month, up from 1.3 billion last year.

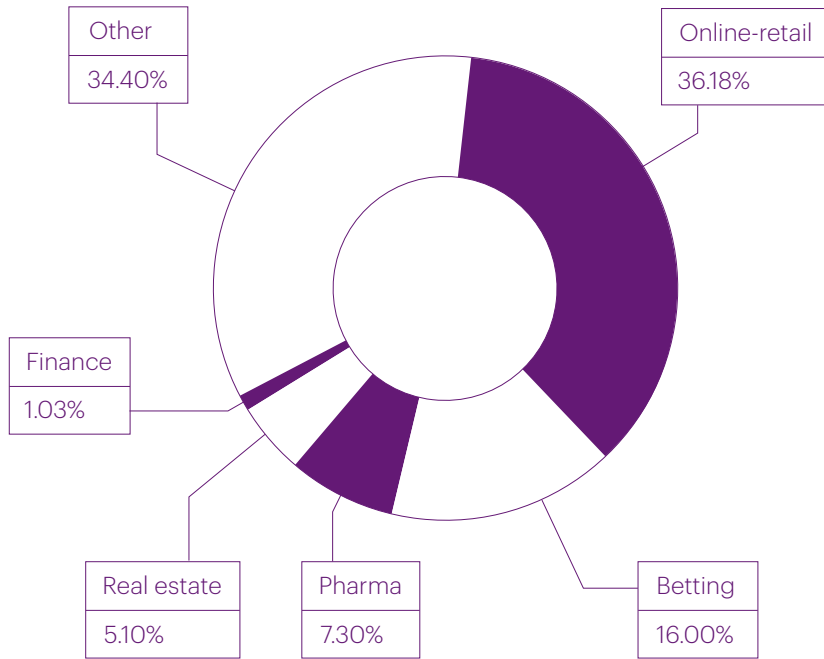
Blocked Bot Requests in 2024

January	1 846 761 745
February.....	1 526 249 372
March.....	1 664 472 828
April	1 770 183 997
May	1 812 334 702
June.....	1 728 255 045
July.....	1 629 675 334
August	1 787 765 095
September	1 601 082 336
October.....	1 704 215 635
November.....	1 530 278 403
Total.....	18 601 274 492

The most targeted segment this year was "Online retail" (36.2% of total bot activity), followed by "Betting" (16%), "Pharma" (7.3%), "Real estate" (5.1%), and "Banks"

(1%). Together, these five categories accounted for almost two-thirds of all bot attacks we recorded in 2024.

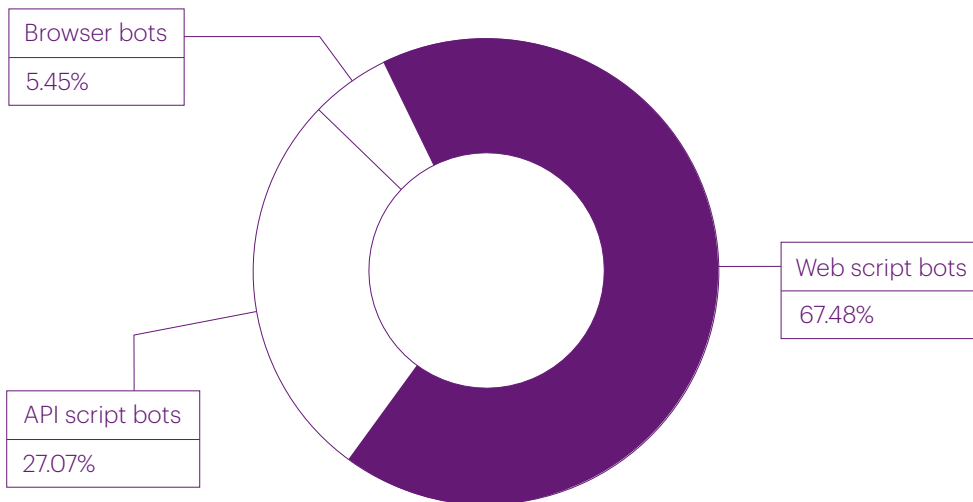
Bad bot activity by industry in 2024



The largest bot attack of 2024 occurred on March 2, targeting the “Betting” segment. During this attack we blocked a total of 22,258,587 bot requests. The fastest bot attack of 2024 also targeted the “Betting” segment. It occurred

on February 19, with a peak rate of 79,300 requests per second. The distribution of bot types in 2024 was as follows: the majority were script bots (67.5%), followed by API bots (27.1%) and browser bots (5.4%).

Bad bot activity by type in 2024



We predict that the share of attacks targeting the “Online retail” segment in overall bot activity will continue to grow in the coming year. Attacks on the “Betting” segment are likely to maintain the sharp intensity spikes observed in 2024. Meanwhile, bot activity in other segments will likely remain more stable, exhibiting a “background” pattern similar to this year.

A notable global trend is that online resources continue to remove content from public access, hiding it from unauthorized users. This approach not only protects content from bots but also enables the collection of more visitor data.

2024

BGP INCIDENTS

The number of unique autonomous systems (ASes) responsible for BGP route leaks remained relatively stable throughout the year. Compared to 2023, the average monthly number of ASes that were responsible for BGP route leaks in 2024 increased by approximately 10%.

The number of ASes involved in BGP hijacks fluctuated significantly from month to month. On average, there were 24% more ASes that were responsible for BGP hijacks per month in 2024 compared to the previous year.

UNIQUE ROUTE LEAKER ASes	2024	UNIQUE HIJACKER ASes
1 815	January	9 488
2 057	February	12 085
2 249	March	10 935
1 932	April	9 137
2 003	May	19 584
2 024	June	10 485
2 036	July	9 711
2 040	August	9 465
1 883	September	4 570
2 130	October	10 902
1 899	November	9 113
1 763	December	8 817

Global BGP Incidents

As a reminder, to identify global BGP incidents, the Qrator.Radar team uses a set of threshold values. These criteria include the number of affected prefixes and autonomous systems, as well as the extent of the anomaly's spread across routing tables.

The number of recorded global incidents in 2024 increased significantly compared to 2023. In particular, the number of global BGP route leaks rose by 59%, while the number of global BGP traffic hijacks grew by 25%.

GLOBAL BGP ROUTE LEAKS	2024	GLOBAL BGP HIJACKS
3	January	1
4	February	0
2	March	0
0	April	0
2	May	1
4	June	0
3	July	1
3	August	1
5	September	0
2	October	1
2	November	0
2	December	0

One notable event was the successful prevention of a BGP route leak between Internet Exchanges (IXs) in the third quarter of 2024. This was made possible through the application of the RFC 9234

standard, developed by Qrator Labs experts in collaboration with other specialists as part of the Internet Engineering Task Force (IETF).

Detailed Findings

- The total number of DDoS attacks in 2024 experienced a notable increase compared to 2023 (+53%).
- The share of multivector attacks in 2024 also rose slightly, showing an 8% increase over the previous year.
- The most powerful L3-L4 attack of 2024 was recorded in the “Media, TV, radio, bloggers” microsegment. It occurred in the fourth quarter of 2024 and reached a bitrate of over 1 Tbps — 1140 Gbps. This is 65% higher than the previous year’s record of 0.69 Tbps.
- The largest botnet we detected in 2024 consisted of 227,000 devices (compared to the largest botnet of 2023, which had around 136,000 devices). This rapid growth in botnet size can be attributed to the increasing number of outdated and vulnerable devices in developing countries.
- The longest DDoS attack of 2024 lasted 463.9 hours, or over 19 days. In comparison, the record for 2023 was just 3 days. The increase in attack duration on protected systems may be linked to the previously mentioned growth in botnet size, along with the simultaneous increase in internet connection speeds. Together, these factors provide attackers with not only free but also virtually unlimited resources for their attacks.
- The “Fintech” macrosegment saw the highest number of L3-L4 attacks in 2024, with a share of 25.8%. Among microsegments, “Banks” were the most targeted, accounting for 16.1% of all attacks.

- The “E-commerce” macrosegment ranked second in terms of L3-L4 attacks (20.5%), with the “Online retail” microsegment accounting for 13.7%. In third place were the “Media” macrosegment (13.5%) and the “Media, TV, radio, bloggers” microsegment (12.8%).
- In addition to the record-breaking attack on the “Media, TV, radio, bloggers” microsegment, which reached 1.14 Tbps, other high-intensity attacks in 2024 were recorded in the “Betting shops” (882 Gbps), “Online retail” (706 Gbps), “Banks” (317 Gbps), “Hosting platforms” (313 Gbps), “Forex” (311 Gbps), and “Payment systems” (300 Gbps) microsegments.
- The largest share of L7 DDoS attacks in 2024 targeted the “Fintech” (52%), “E-commerce” (18%), and “IT&Telecom” (9.6%) macrosegments.
- Among microsegments, the most targeted were “Banks” (31.9%), “Online retail” (10%), and “Payment systems” (7.7%).
- The longest L7 attack of 2024 lasted over two days — 49.1 hours.
- The most powerful L7 attack recorded in 2024 reached a peak intensity of 1.56 million rps.
- The highest number of devices involved in a single attack was 1,472,941.
- The top three countries identified as the primary sources of DDoS attacks in 2024 were Russia (32.4%), the United States (20.6%), and Brazil (5.8%). China, which had long held the third position, experienced a sharp decline starting in the second quarter and dropped out of the top three by the end of the year.
- Bot activity in 2024 increased significantly compared to the previous year: the average monthly number of blocked requests rose by 30% compared to 2023.
- The largest bot attack of 2024 occurred on March 2, targeting the “Betting” segment and resulting in a total of 22,258,587 blocked bot requests.

- The fastest bot attack of 2024 also targeted the “Betting” segment. It occurred on February 19 and reached a peak speed of 79,300 requests per second.
- The majority of bot attacks in 2024 targeted the “Online retail” segment (36.2% of total bot activity), followed by “Betting” (16%), “Pharma” (7.3%), “Real estate” (5.1%), and “Finance” (1%).
- The total number of BGP incidents, as well as global BGP incidents, increased significantly in 2024 compared to the previous year.
- The number of ASes that were responsible for BGP incidents increased significantly in 2024 compared to the previous year.
- The average monthly number of ASes that were responsible for BGP route leaks rose by 10%.
- The average monthly number of ASes that were responsible for BGP hijacks increased by 24%.
- The number of global BGP hijacks rose by 25%.
- In the third quarter of 2024, a global route leak between IXs was successfully prevented through the use of the RFC 9234 standard developed by Qrator Labs experts.



web: qrator.net

e-mail: sales@qrator.net

tel.: +420 602 558 144