

curator.pro

CURATOR

DDoS, БОТЫ И BGP-ИНЦИДЕНТЫ

1 КВАРТАЛ

2025

СТАТИСТИКА И ТРЕНДЫ

Ключевые факты и выводы

Крупнейший DDoS-ботнет, который мы обнаружили в марте 2025 года, за год значительно вырос — с 1,33 млн до 13,5 млн зараженных устройств. Основную долю составляют устройства из США, Бразилии и Индии.

Наиболее интенсивная DDoS-атака 1 кв. 2026 года была направлена на организацию из сегмента «Онлайн-ставки». В пике она достигала более 2 Тбит/с и около 1 Vpps. При этом фаза высокой интенсивности продолжалась более 40 минут, что нетипично долго для настолько масштабных атак.

Доля мультивекторных DDoS-атак в 1 кв. 2026 года выросла по сравнению с 2025 годом с 8,0% до 10,7% от всех инцидентов.

Доля атак, сочетающих L3-L4 и L7, увеличилась еще заметнее: с 3,6% до 6,2% от всех инцидентов.

Наибольшее число DDoS-атак в 1 кв. 2026 года было направлено на сегменты «Финтех» (44,2%), «ИТ и Телеком» (19,3%) и

«Онлайн-ставки» (10,0%). На эти три сегмента суммарно пришлось почти три четверти всех зафиксированных нами атак.

В число микросегментов, которые чаще всего атаковали в 1 кв. 2026 году, вошли «Банки» (22,8%), «Платежные системы» (15,9%), «Онлайн-букмекеры» (10,0%), «Хостинговые платформы» (6,8%) и «Системные интеграторы» (6,4%).

В 1 кв. 2026 года крупнейшими источниками L7 DDoS-атак стали Бразилия (12,1%), США (11,5%) и Россия (7,3%). При этом доля первой пятерки стран снизилась по сравнению с прошлым годом с 56,5% до 42,0% — то есть распределение источников атак по странам стало в целом более равномерным.

В 1 кв. 2026 года среднеемесячное количество заблокированных запросов «плохих» ботов выросло на 12% по сравнению с 2025 годом и составило 2,5 млрд.

Общий «индекс ботовости» в 1 кв. 2026 года составил 1,97%, что несколько ниже среднего значения за 9 последних месяцев 2025 года (2,1%), но все еще достаточно много.

Самая длительная атака «плохих» ботов в 1 кв. 2026 года была направлена на организацию из сегмента «Электронная коммерция». Она продолжалась более двух недель, за это время было заблокировано более 178 млн запросов ботов.

В 1 кв. 2026 года число уникальных АС, допустивших утечки маршрутов, осталось на уровне прошлого года. При этом количество АС, совершивших BGP-перехваты, снизилось примерно на 17% по сравнению с 1 кв. 2025 года.

Количество глобальных инцидентов BGP в 1 кв. 2026 года было достаточно высоким — мы зафиксировали 7 утечек маршрутов и один BGP-перехват.

Преобладающие векторы DDoS-атак в 1 кв. 2026 года

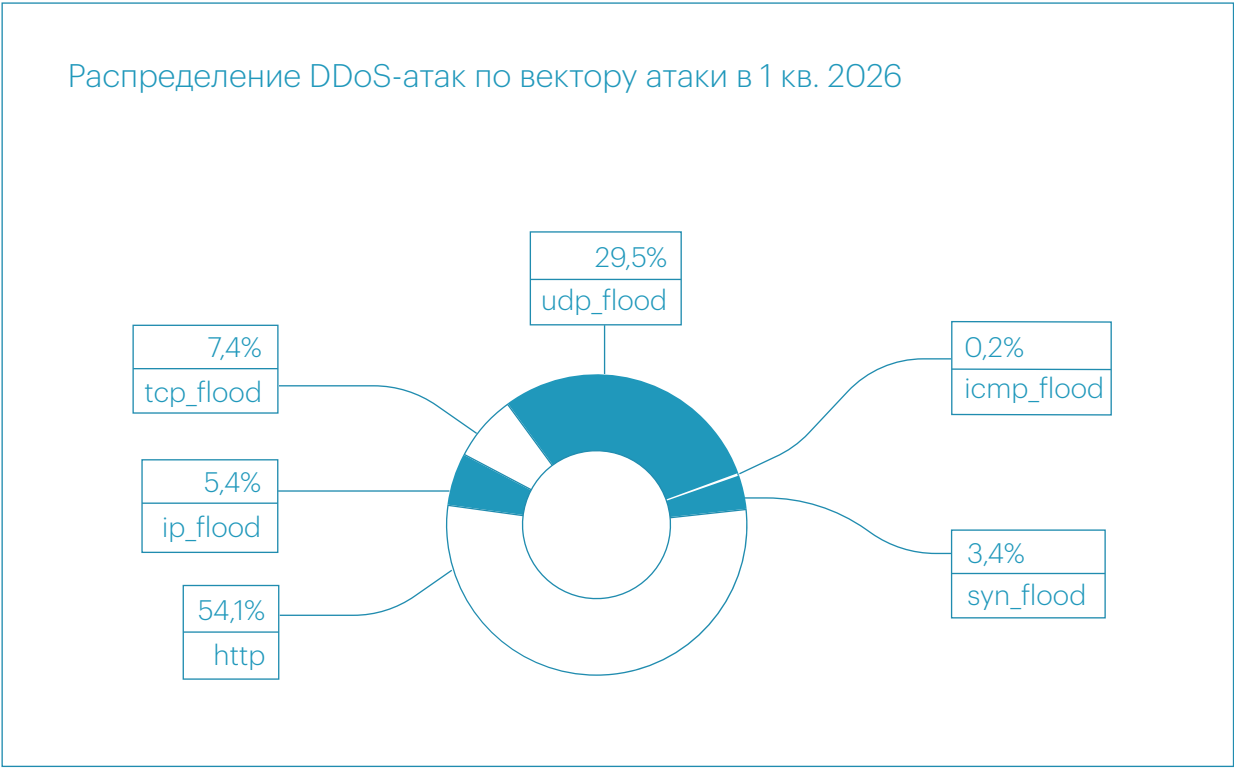
Начиная со 2 квартала 2025 года мы изменили нашу методику анализа DDoS-атак. До этого момента мы учитывали отдельно атаки на сетевом и транспортном уровнях (L3-L4 DDoS) и отдельно атаки на уровне приложений (L7 DDoS). Теперь мы используем единую статистику, оперирующую инцидентами, которые могут состоять из нескольких атак по разным векторам. Мы отсекаем L3-L4 DDoS-атаки интен-

сивностью менее 1 Гбит/с, считая их белым шумом. Для L7 DDoS-атак мы также используем пороговые значения: не менее 100 заблокированных IP-адресов и скорость не менее 1000 запросов в секунду. Критерий объединения нескольких отдельных волн атаки в единый инцидент — временная разница между ними в пределах одного часа.

В 1 квартале 2026 года основная доля DDoS-атак пришлась на HTTP, то есть атаки на уровне приложений (L7). Их было 54,1% от общего числа зафиксированных нами атак, что примерно совпадает с уровнем последних девяти месяцев прошлого года (56,4%). Второе место занял UDP flood, доля которого заметно выросла по

сравнению с прошлым годом (22,9%—29,5%).

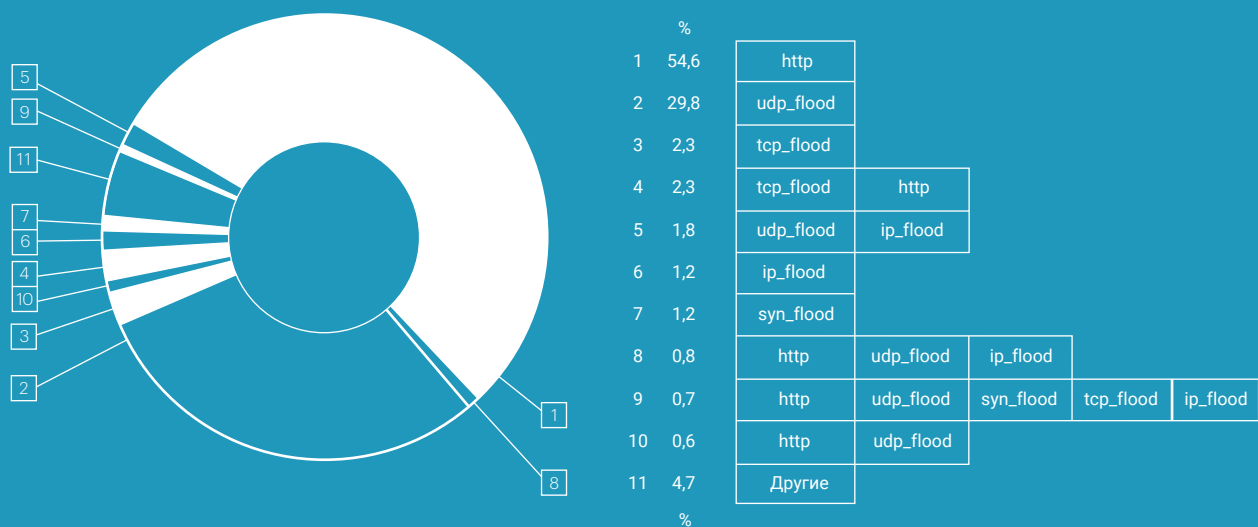
Популярность IP flood у атакующих заметно снизилась (13,8%—5,4%), что позволило TCP выйти на третье место (4,2%—7,4%). Относительное количество атак SYN flood и ICMP flood осталось примерно на уровне прошлого года.



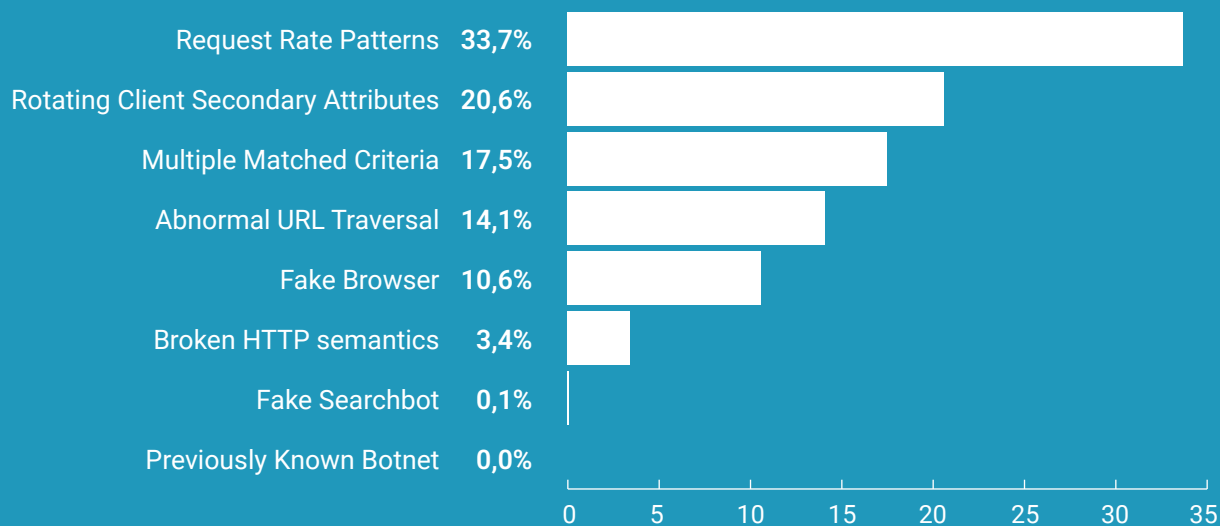
В 1 кв. 2026 года доля мультивекторных атак заметно выросла по сравнению с последними 9 месяцами 2025 года — с 8,0% до 10,7% от общего числа зафиксированных инцидентов. Также существенно увеличилась

доля мультивекторных атак, в которых сочетались L3-L4 и L7: если в 2025 году их было 3,6% от всех инцидентов, то в 1 кв. 2026 года это число увеличилось до 6,2%.

Мультивекторные DDoS-атаки в 2026 году



L7 DDoS-атаки по типу в 1 кв. 2026



Распределение DDoS-атак по индустриям в 1 кв. 2026 года

Основными целями DDoS-атак в 1 кв. 2026 года были организации из сегментов «Финтех» (44,2%), «ИТ и Телеком» (19,3%) и «Онлайн-ставки» (10,0%). На эти сегменты суммарно пришлось почти три четверти всех зафиксированных нами инцидентов.

Повышенную активность в сегмен-

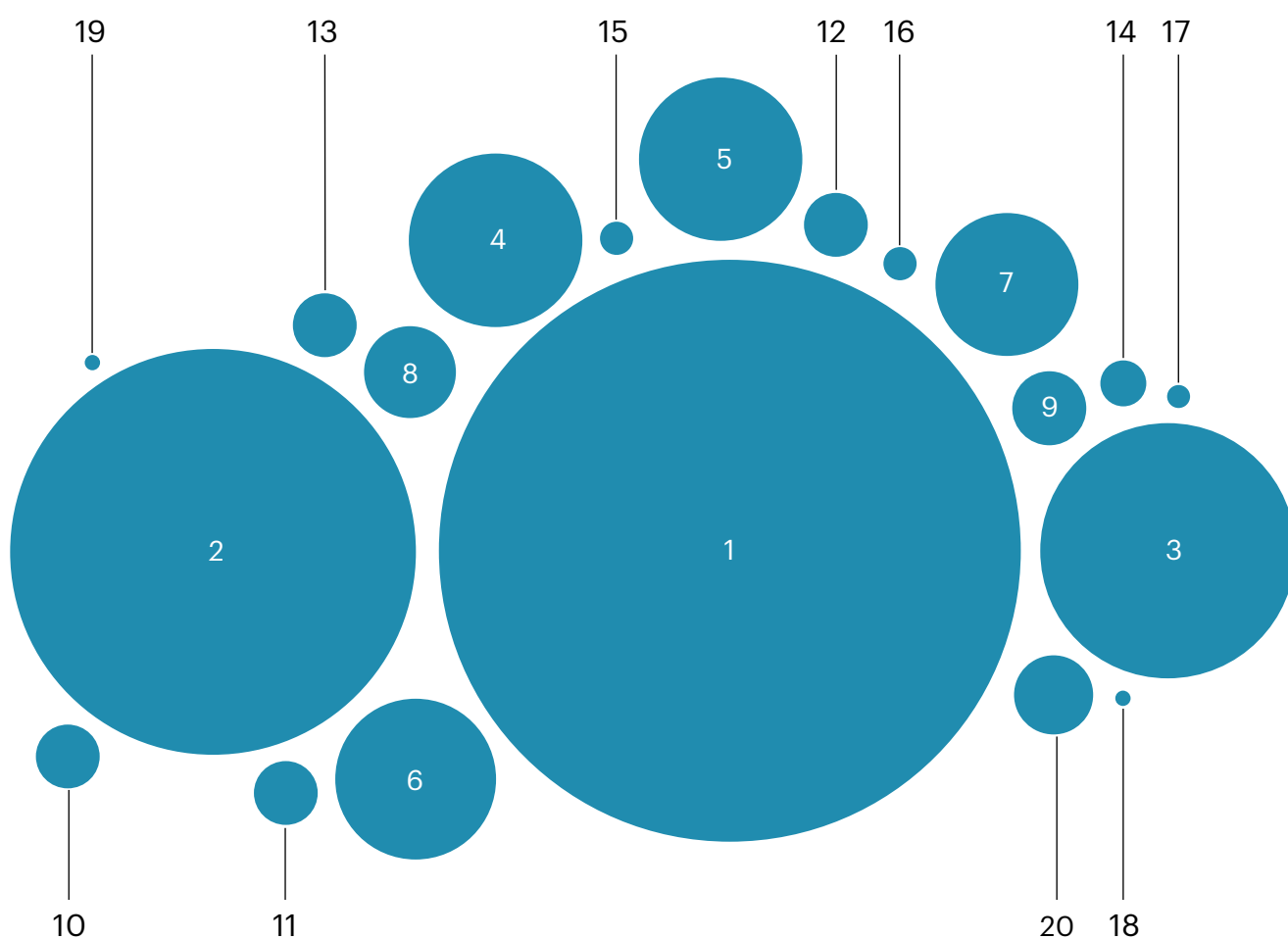
те «Онлайн-ставки» стоит отметить отдельно — помимо заметно большего, чем в прошлом году, количества инцидентов, в нем также была зафиксирована и самая интенсивная, и самая продолжительная DDoS-атака 1 квартала (подробнее об этом поговорим ниже).

Макросегментация DDoS-атак в 1 кв. 2026



Если говорить о более детальной сегментации, то в 1 кв. 2026 года основное количество DDoS-атак было направлено на микросегменты «Банки» (22,8%), «Платежные системы» (15,9%), «Онлайн-букмекеры» (10,0%), «Хостинговые платформы» (6,8%) и «Системные интеграторы» (6,4%). Суммарно на эти пять микросегментов пришлось почти две трети (62,0%) от всех атак, зафиксированных нами в 1 кв. 2026 года.

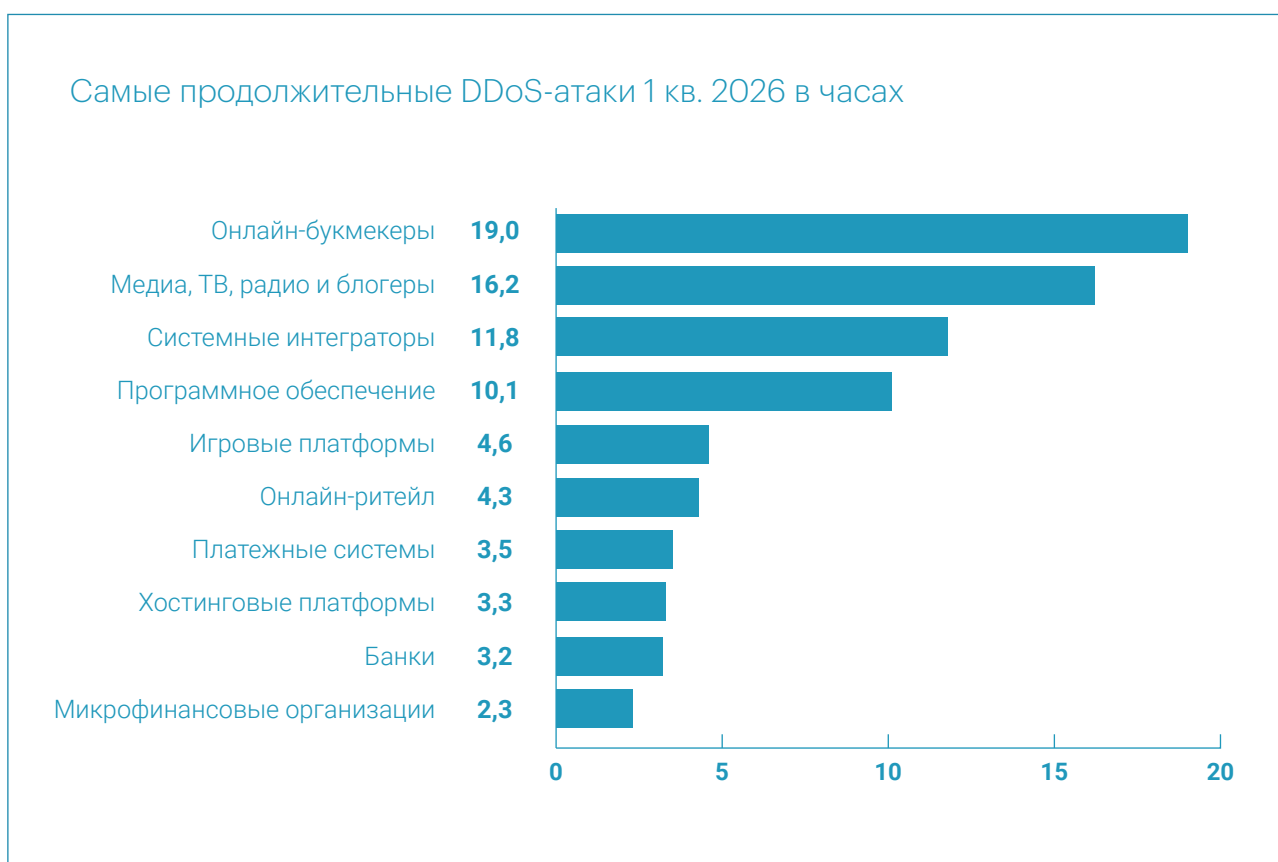
Микросегментация DDoS-атак в 1 кв. 2026



1	22,8%	Банки	11	2,5%	Телеком-операторы
2	15,9%	Платежные системы	12	2,5%	Социальные сети
3	10,0%	Онлайн-букмекеры	13	2,5%	Рестораны и доставка еды
4	6,8%	Хостинговые платформы	14	1,8%	Криптовалюты
5	6,4%	Системные интеграторы	15	1,3%	Онлайн-ритейл
6	6,3%	Медиа, ТВ, радио и блогеры	16	1,3%	Игровые платформы
7	5,6%	Онлайн-образование	17	0,9%	Нефть и газ
8	3,6%	Программное обеспечение	18	0,6%	Аэропорты
9	2,9%	Forex	19	0,6%	Медицинские лаборатории
10	2,5%	Электронные доски объявлений	20	3,1%	Другое

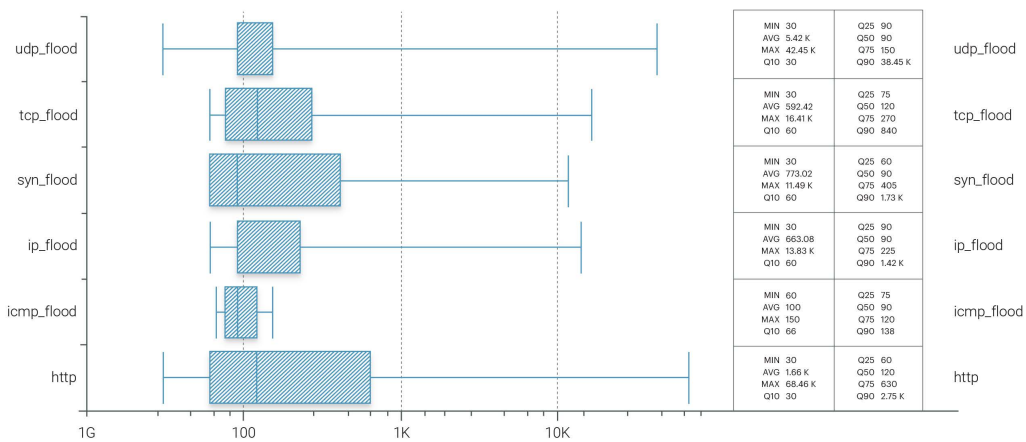
Продолжительность DDoS-атак в 1 кв. 2026 года

Самые продолжительные DDoS-атаки в 1 кв. 2026 года были направлены на сегменты «Онлайн-букмекеры» (19,0 ч), «Медиа, ТВ, радио и блогеры» (16,2 ч), «Системные интеграторы» (11,8 ч) и «Программное обеспечение» (10,1 ч). Это сравнительно короткие атаки — напомним, что рекордом 2025 года был инцидент длительностью 119,2 ч.



Несмотря на достаточно скромные максимумы, средняя длительность атак в 1 кв. 2026 года несколько выросла по сравнению с 2025 годом: с 2268 до 3221 секунды. Медианная продолжительность осталась той же — 120 секунд.

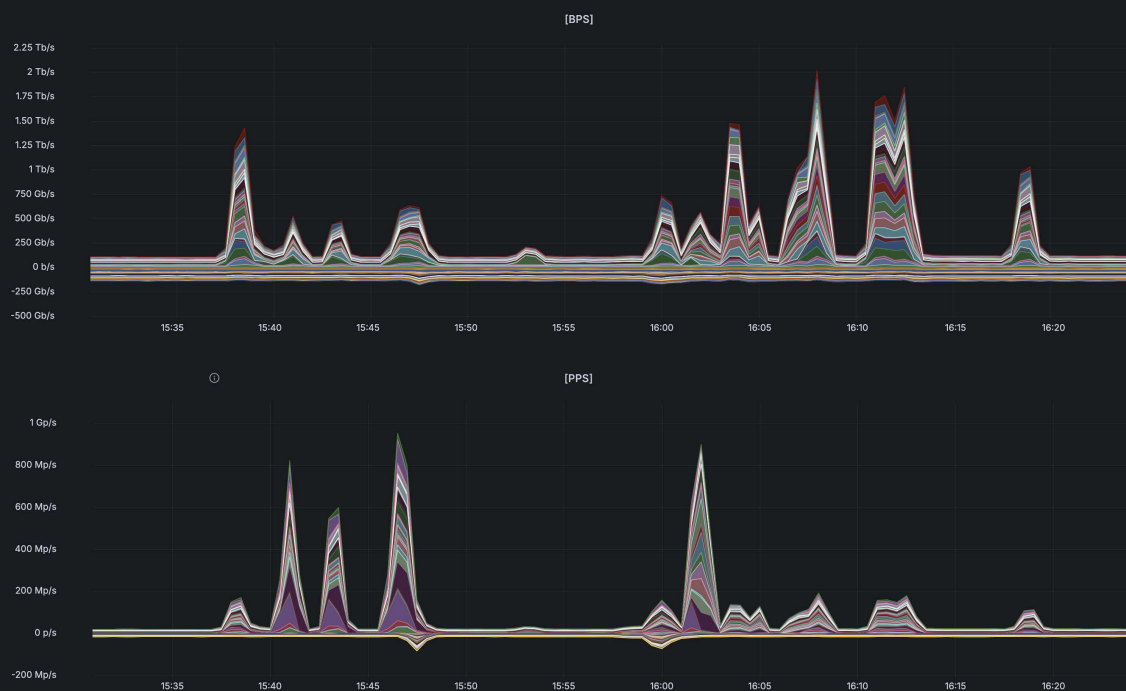
Продолжительность DDoS-атак в секундах по вектору атаки в 1 кв. 2026



Интенсивность L3-L4 DDoS-атак в 1 кв. 2026 года

Самая интенсивная атака 1 кв. 2026 года произошла в середине марта и была направлена на организацию из сегмента «Онлайн-ставки». Битрейт данной атаки в пике достигал 2065 Гбит/с, а максимальная скорость передачи пакетов составила 953 Mpps, лишь немного не дотянув до 1 Vpps.

Самая интенсивная атака 1 кв. 2026

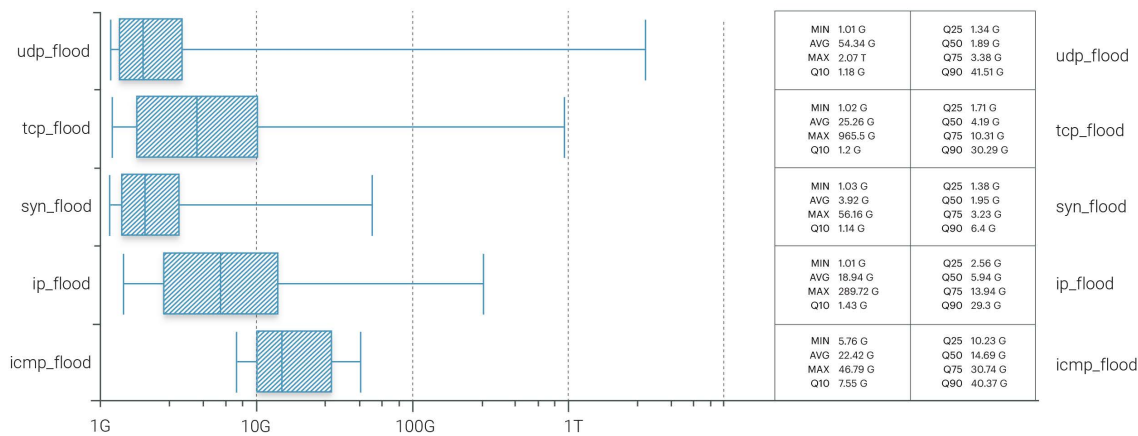


Что особенно нехарактерно для настолько интенсивной атаки, ее острая фаза продолжалась не в течение секунд, как это обычно бывает, а целых 40 минут. За это время мы наблюдали 11 всплесков, четыре из которых превышали 1 Тбит/с. Это указывает на попытки атакующих адаптировать стратегию и поддерживать длительное давление на инфраструктуру. Несмотря на эти попытки, атаку удалось

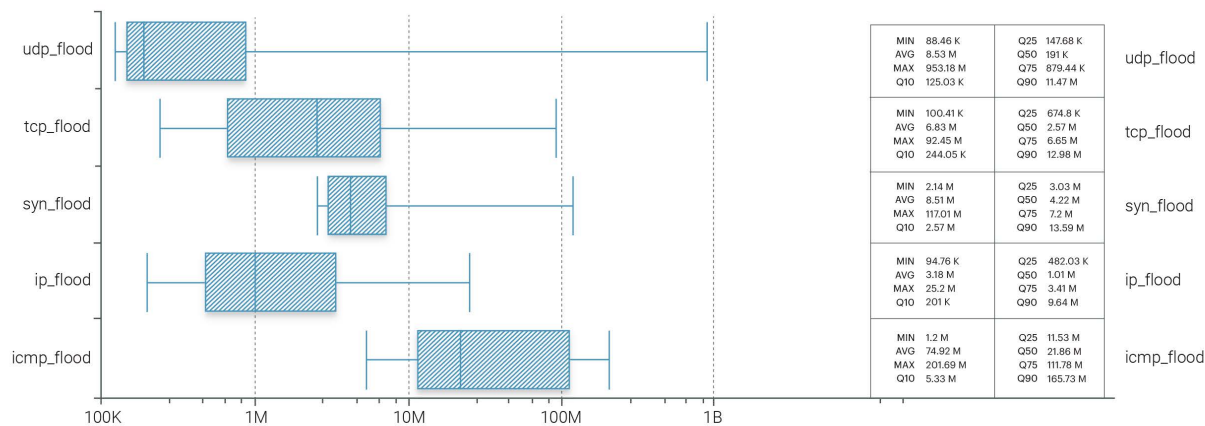
успешно нейтрализовать без влияния на доступность сервиса.

Если в прошлом году атаки интенсивностью более 1 Тбит/с были скорее исключением, то в этом году они становятся обычной практикой. В 1 кв. 2025 года мы не зафиксировали ни одной атаки интенсивностью более 1 Тбит/с, а в 1 кв. 2026 года таких атак произошло уже четыре.

Объем L3-L4 DDoS-атак в битах в секунду (bps) по вектору атаки в 1 кв. 2026



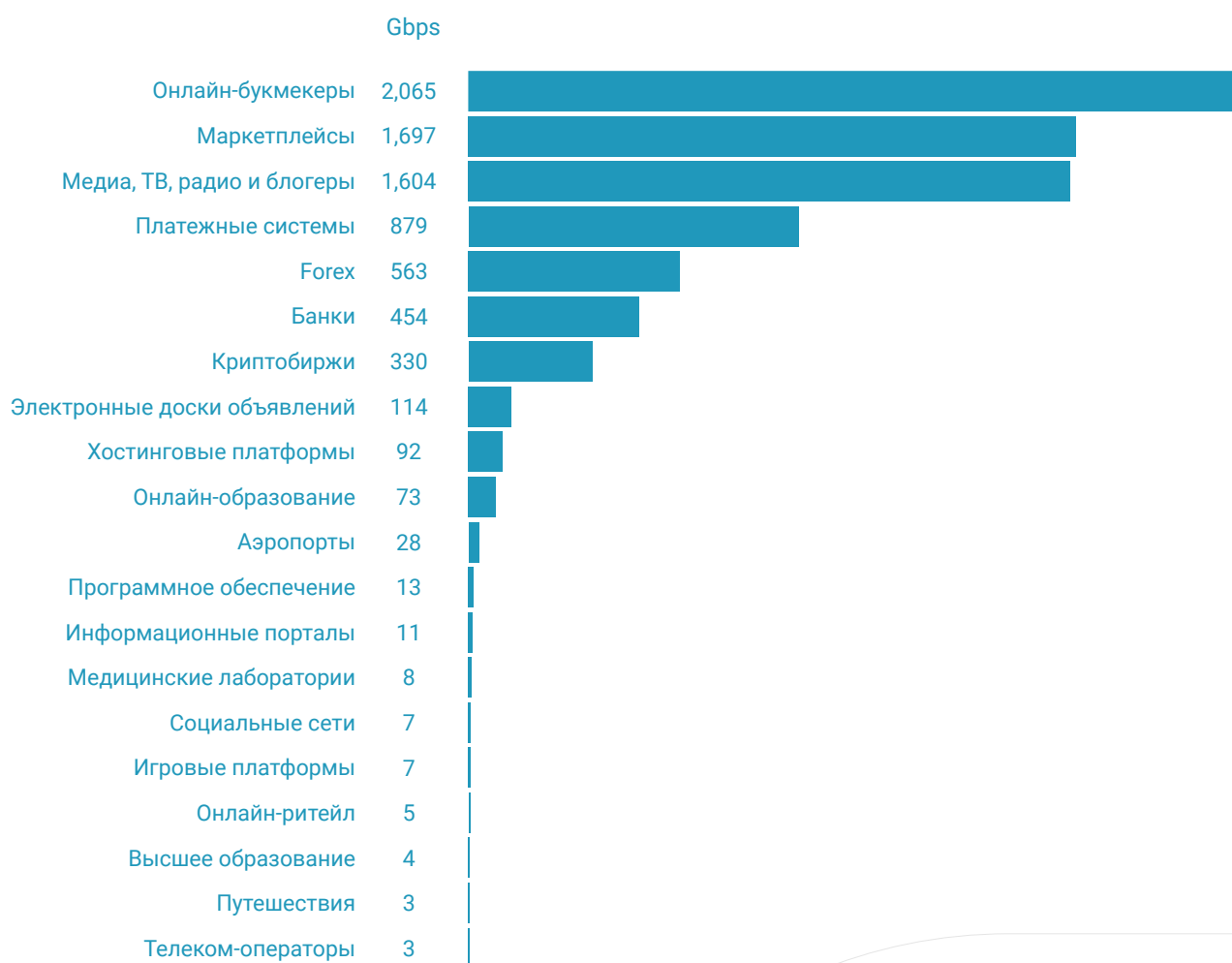
Объем L3-L4 DDoS-атак в пакетах в секунду (pps) по вектору атаки в 1 кв. 2026



Первая пятерка микросегментов, на которые в 1 кв. 2026 года были направлены наиболее интенсивные L3-L4 DDoS-атаки, выглядит следующим образом: «Онлайн-букмекеры» (2065 Гбит/с),

«Маркетплейсы» (1697 Гбит/с), «Медиа, ТВ, радио и блогеры» (1604 Гбит/с), «Платежные системы» (879 Гбит/с) и «Forex» (563 Гбит/с).

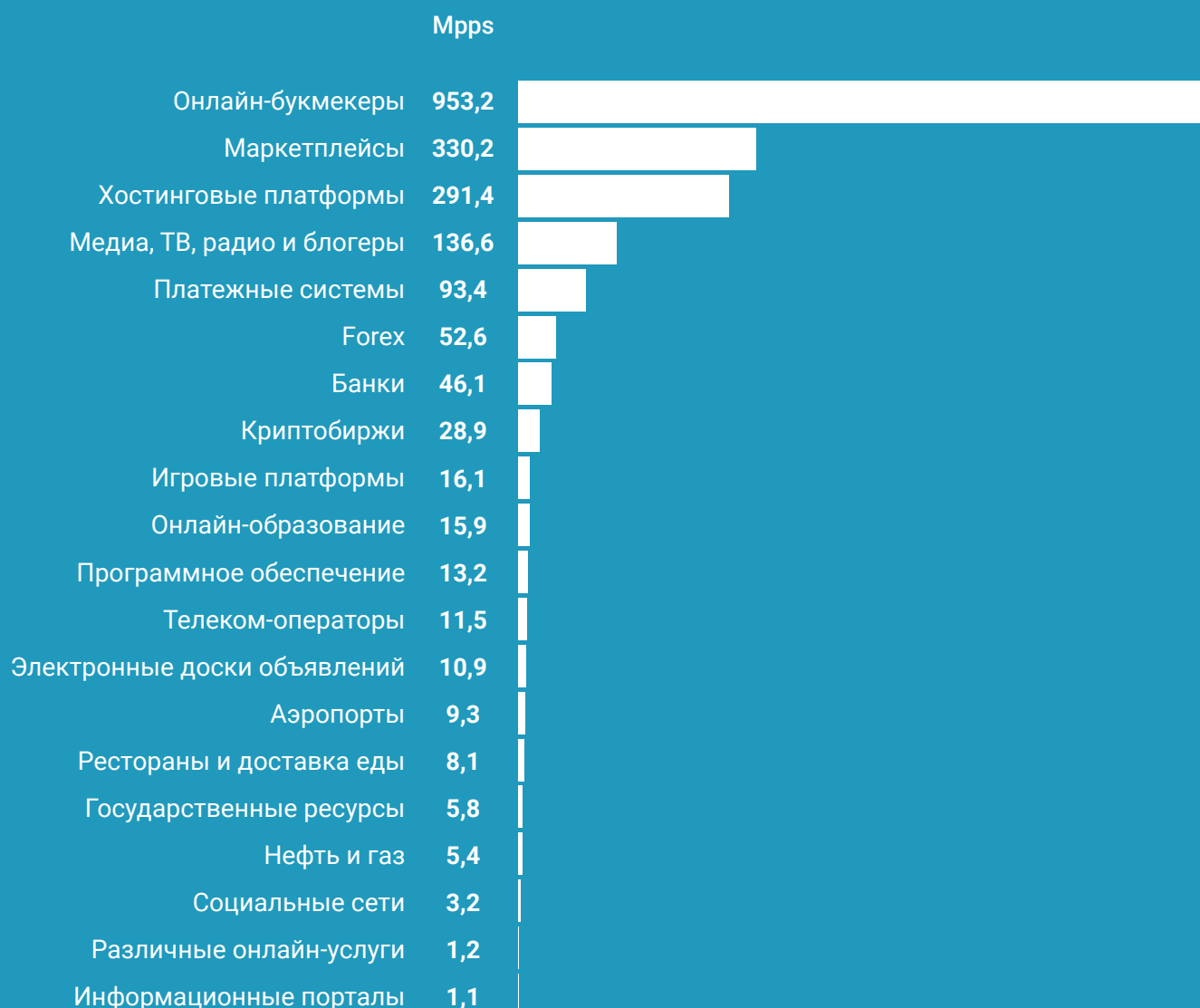
Макс. битрейт L3-L4 DDoS-атак по сегментам в 1 кв. 2026



Если говорить о максимальной скорости передачи пакетов, то в 1 кв. 2026 года это были атаки на микросегменты «Онлайн-букмекеры» (953,2 Mpps),

«Маркетплейсы» (330,2 Mpps), «Хостинговые платформы» (291,4 Mpps), «Медиа, ТВ, радио и блогеры» (136,6 Mpps) и «Платежные системы» (93,4 Mpps).

Макс. скорость передачи пакетов L3-L4 DDoS-атак по сегментам в 2025 году

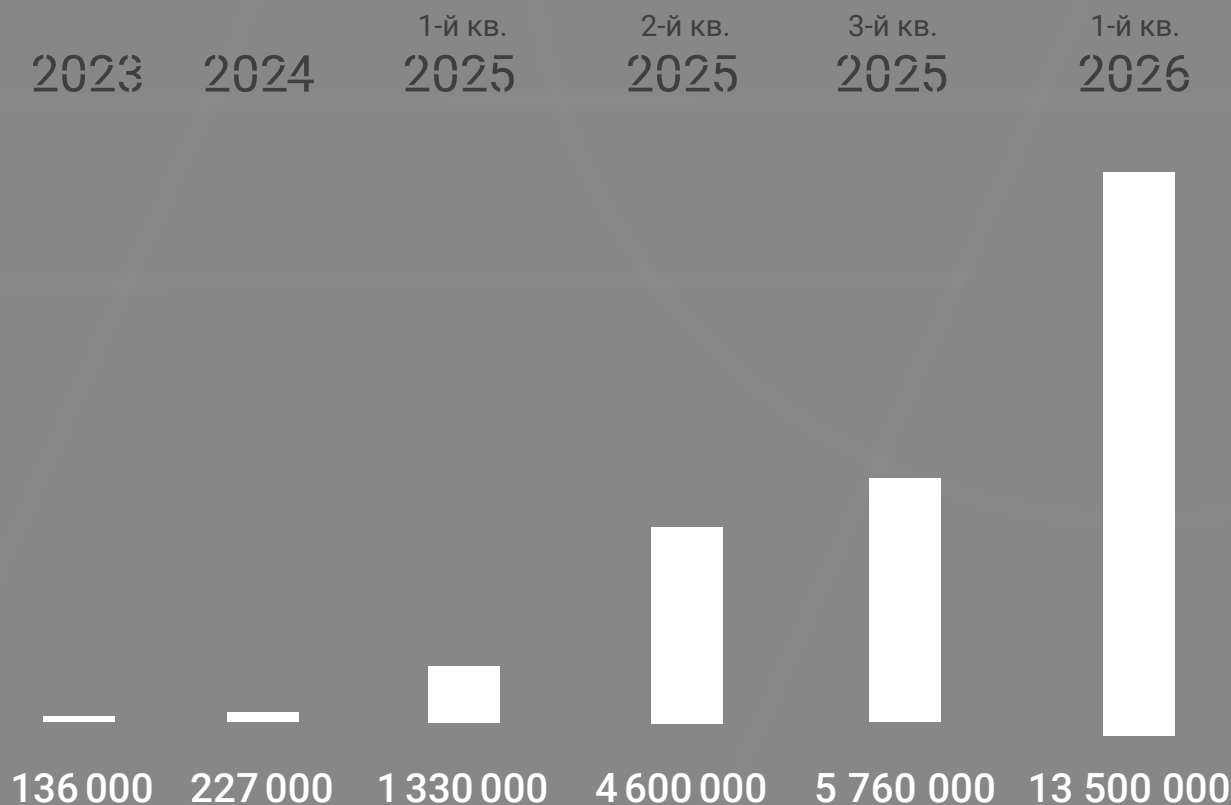


Самый большой DDoS-ботнет 1 кв. 2026 года

Уже второй год мы наблюдаем за деятельностью огромного DDoS-ботнета, который впервые обнаружили 26 марта 2025 года. За это время ботнет значительно увеличился: если год назад, при отражении первой зафиксированной нами атаки данного ботнета, мы заблокировали 1,33 миллиона IP-адресов, то во время нейтрализации волны атак в 1 кв. 2026 года мы заблокировали уже 13,5 миллиона. Таким образом, за год ботнет вырос более чем в 10 раз.

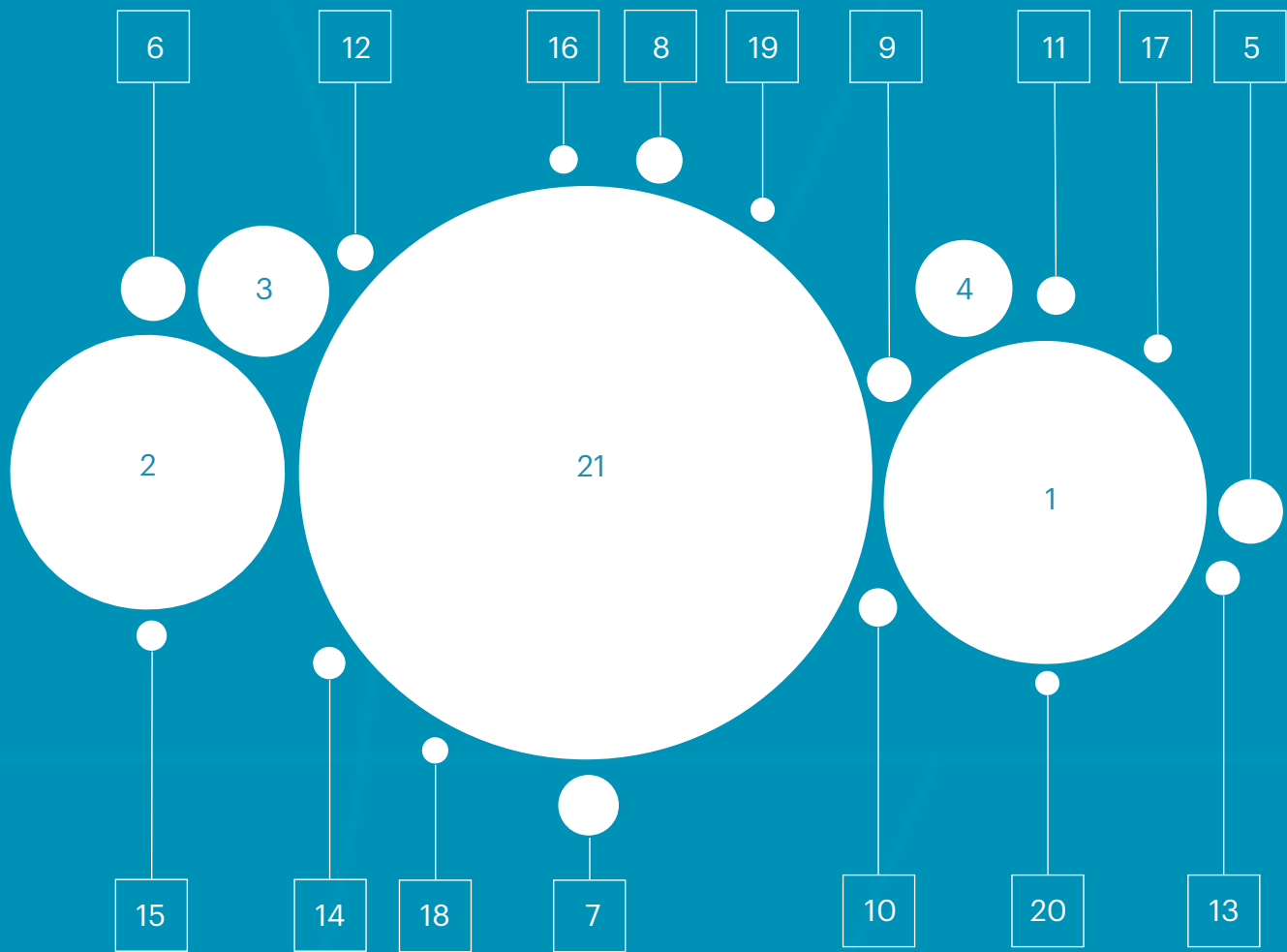
САМЫЙ БОЛЬШОЙ БОТНЕТ

1 КВ. 2026 ГОДА



Также за год заметно изменилась география ботнета. В 1 кв. 2025 года в нем преобладали устройства из Бразилии (51,1%), в меньшей степени — из других развивающихся стран: Аргентины (6,1%), России (4,6%), Ирака (3,2%) и Мексики (2,4%). В 1 кв. 2026 года на первое место вышли устройства из США (16,0%), при этом доля Бразилии снизилась до 13,6%. Также в первую пятерку вошли Индия (6,5%), Великобритания (4,8%) и Турция (3,2%).

География самого большого ботнета 1 кв. 2026



1	16,0%	США	12	1,8%	Филиппины
2	13,6%	Бразилия	13	1,7%	Канада
3	6,5%	Индия	14	1,6%	Марокко
4	4,8%	Великобритания	15	1,5%	Испания
5	3,2%	Турция	16	1,4%	Индонезия
6	3,2%	Саудовская Аравия	17	1,4%	Украина
7	3,0%	Россия	18	1,3%	Германия
8	2,3%	Мексика	19	1,2%	ЮАР
9	2,2%	Пакистан	20	1,2%	Ирак
10	1,9%	Аргентина	21	28,4%	Другие
11	1,9%	Франция			

Данные показывают, что операторы этого ботнета не только постоянно добавляют в него большое количество новых зараженных устройств, но и уделяют внимание географической диверсификации. Это делает простые геоблокировки неэффективными для нейтрализации DDoS-атак данного ботнета: атакующие готовы в любой момент задействовать IP-адреса из любых стран.

Географическое распределение источников L7 DDoS-атак в 1 кв. 2026 года

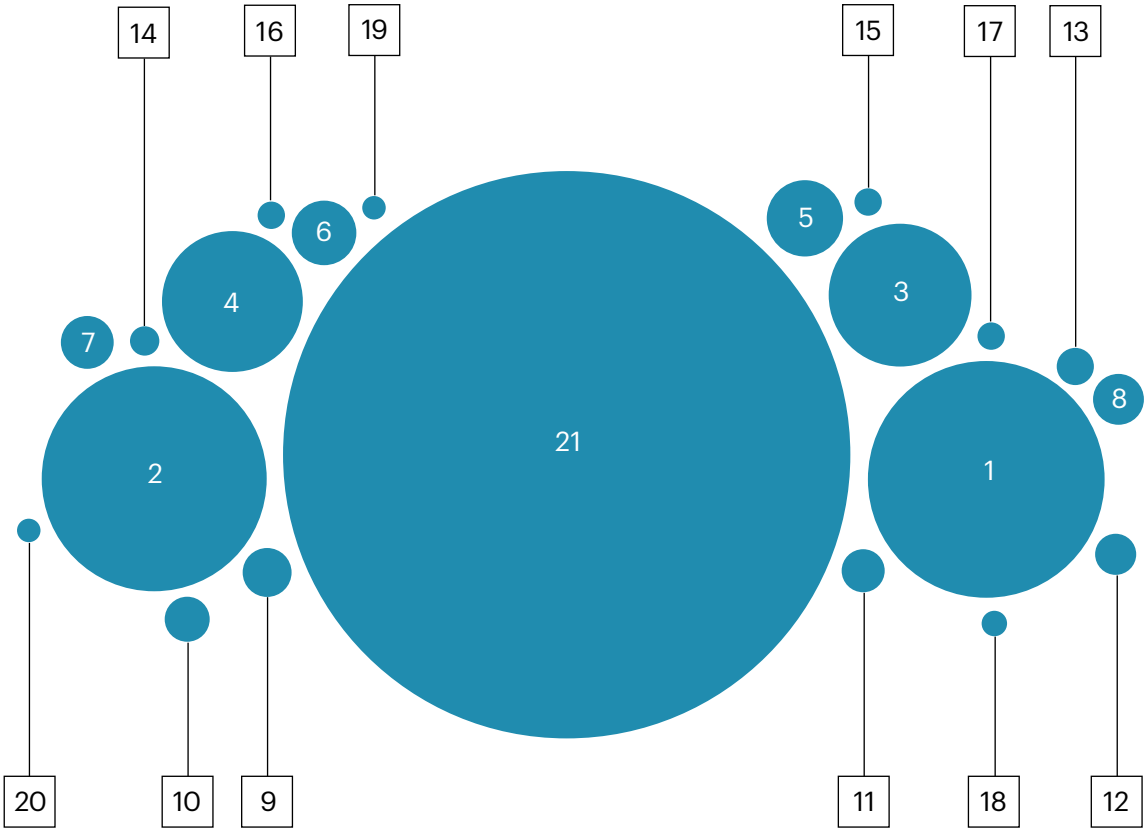
Весь прошлый год мы наблюдали устойчивый тренд быстрого увеличения доли развивающихся стран среди основных источников DDoS-атак на уровне приложений. При этом основной рост пришелся на несколько стран — в первую очередь Бразилию, Вьетнам и Аргентину.

Судя по данным за 1 квартал 2026 года, этот тренд несколько трансформируется: IP-адреса из развивающихся стран по-прежнему занимают значительную часть в рейтинге, но теперь доли распределяются более равномер-

но. Если по итогам 2025 года на первую пятерку стран пришлось 56,5% всех заблокированных адресов, то в 1 кв. 2026 года — лишь 42%.

Еще одно примечательное изменение рейтинга в 1 кв. 2026 года — резкий рост доли США, который в итоге вывел эту страну на второе место с долей 11,5%. Бразилии удалось удержать первое место в рейтинге с долей 12,1%. На третьем месте разместилась Россия с долей 7,3%, достаточно скромной по сравнению с прошлым и тем более позапрошлым годом.

География источников L7 DDoS-атак в 1 кв. 2026



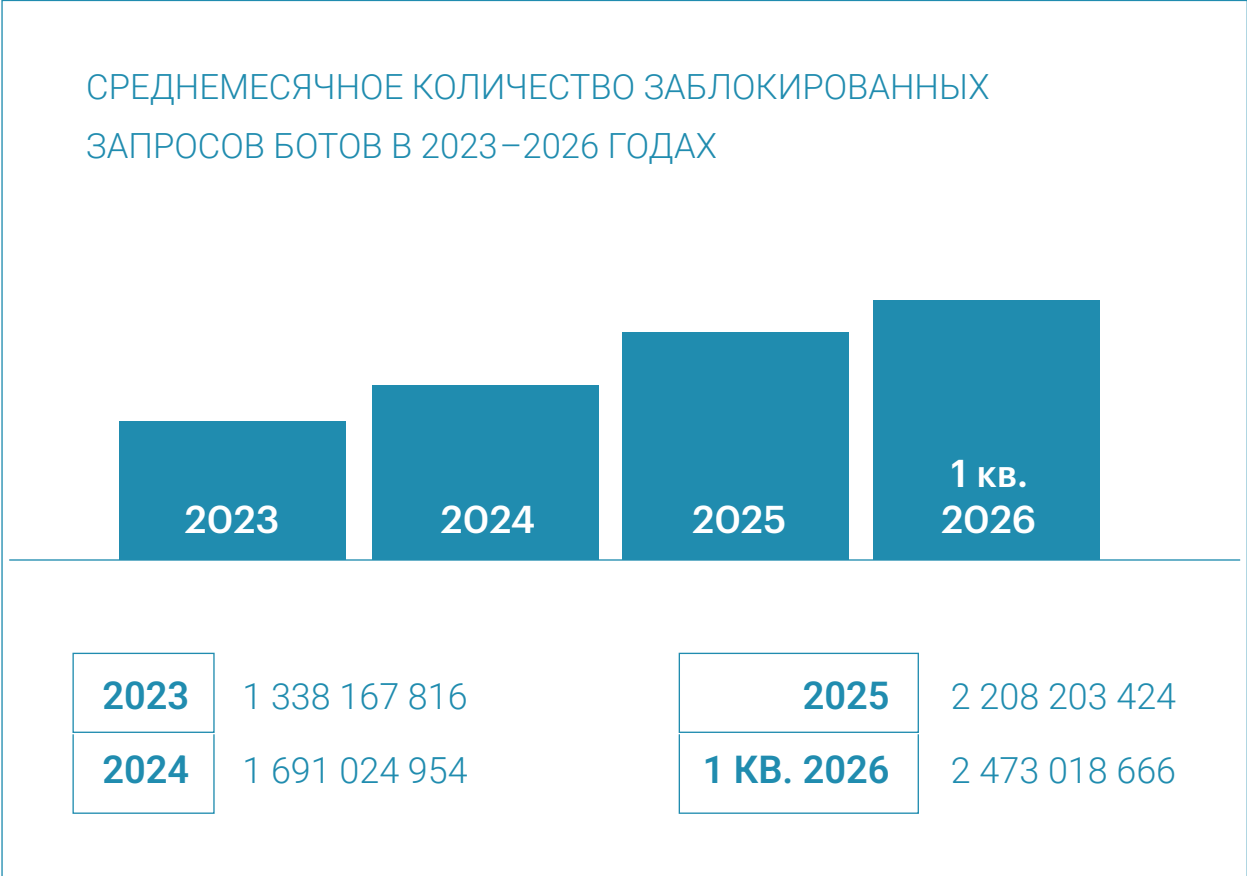
1	12,1%	Бразилия	8	2,6%	Бангладеш	15	1,4%	Сингапур
2	11,5%	США	9	2,5%	Мексика	16	1,4%	ЮАР
3	7,3%	Россия	10	2,3%	Великобритания	17	1,4%	Венесуэла
4	7,2%	Вьетнам	11	2,2%	Пакистан	18	1,3%	Колумбия
5	3,9%	Аргентина	12	2,1%	Нидерланды	19	1,2%	Индонезия
6	3,3%	Индия	13	1,9%	Германия	20	1,2%	Франция
7	2,7%	Ирак	14	1,5%	Китай	21	29,0%	Другие

Эти данные подтверждают ускоряющуюся географическую диверсификацию IP-адресов, используемых организаторами DDoS-атак. Как уже отмечалось выше, следствием этой диверсификации является неэффективность простых геоблокировок при противодействии масштабным атакам.

Статистика защиты от «плохих» ботов в 1 кв. 2026 года — CURATOR.ANTIBOT

Напомним, что под «плохими» ботами подразумеваются автоматизированные системы, которые пытаются взаимодействовать с сайтами, притворяясь настоящими пользователями. Их цели состоят в сборе данных, накрутке показателей, брутфорсе учетных записей и тому подобной нежелательной деятельности. Однако в отличие от деструктивных DDoS-ботов, «плохие» боты не стремятся нарушить работоспособность сайта.

В 1 кв. 2026 году среднеемесячное количество заблокированных запросов «плохих» ботов достигло уровня около 2,5 миллиарда бот-запросов. По сравнению с 1 кв. 2025 года рост составил примерно 40%, а относительно всего 2025 года — 12%.



При этом важно отметить, что в 2025 году мы наблюдали ярко выраженную сезонность бот-трафика с двумя периодами повышенной активности, которые пришлись на 2-й и 4-й кварталы. Эти всплески были связаны с двумя особенно масштабными атаками,

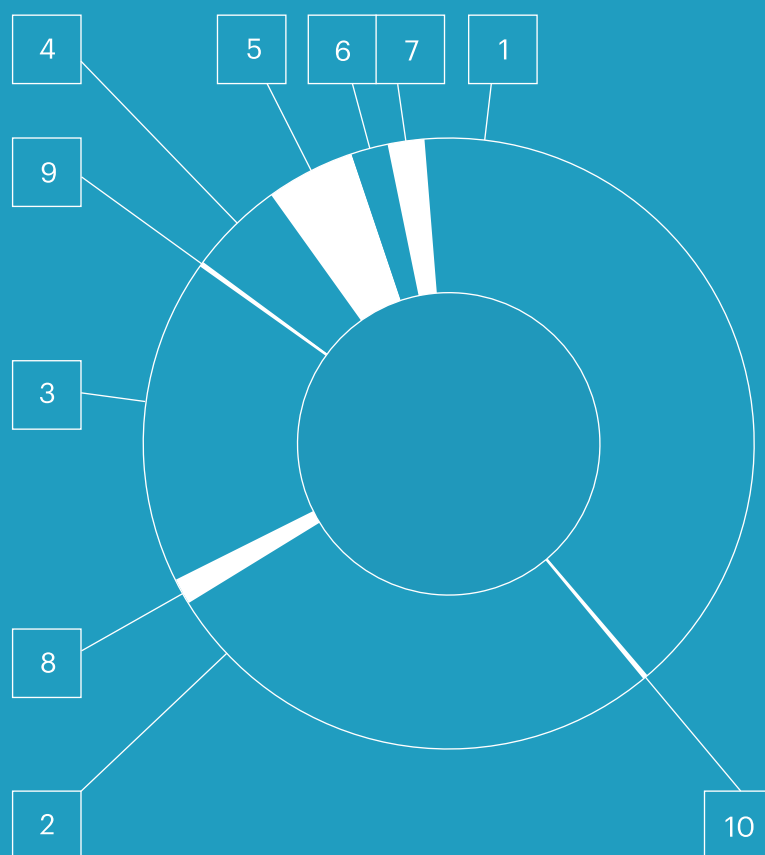
каждая из которых продолжалась около месяца. В 2026 году настолько масштабных бот-атак мы еще не фиксировали — пока бот-трафик распределяется по защищаемым ресурсам более равномерно.



В 1 кв. 2026 года наибольшее число атак ботов, как обычно, было направлено на сегмент «Электронная коммерция» (40,21% от всей бот-активности). На втором месте — сегмент «Онлайн-

ставки» (27,09%), что также достаточно привычно. Третье место в этом квартале неожиданно занял сегмент «Транспорт и логистика» (17,34%).

Активность ботов по сегментам в 1 кв. 2026



	%	
1	40,21	Электронная коммерция
2	27,09	Онлайн-ставки
3	17,34	Транспорт и логистика
4	4,91	Здравоохранение
5	4,66	Медиа

	%	
6	2,03	Образовательные технологии
7	1,97	Финтех
8	1,48	Недвижимость
9	0,19	ИТ и Телеком
10	0,12	Реклама и развлечения

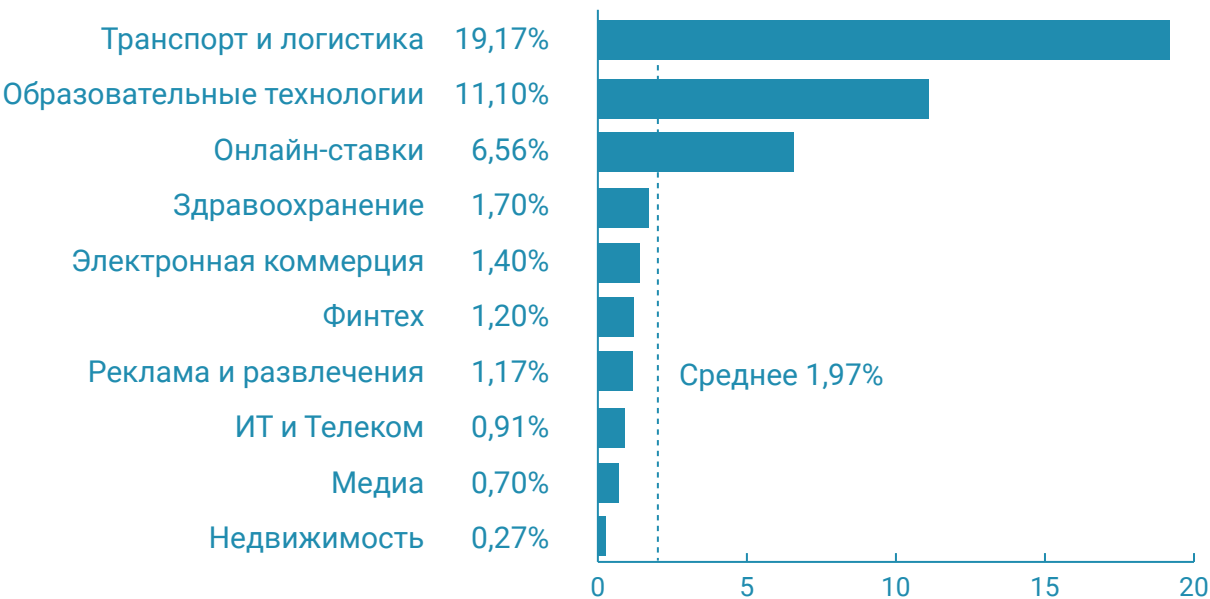
Еще одна аномалия, связанная с сегментом «Транспорт и логистика» — это крайне высокая доля бот-трафика от общего объема трафика на защищаемые нами ресурсы «индекс ботовости»).

В 1 кв. 2026 года для данного сегмента этот показатель составил 19,17% — то есть практически каждый пятый запрос отправлялся ботами.

Также высокая доля бот-трафика наблюдалась в сегментах «Образовательные технологии» (11,10%) и «Онлайн-ставки» (6,56%). В среднем же по всем сегментам индекс ботовости

в 1 кв. 2026 года составил 1,97%, что несколько ниже показателя последних девяти месяцев 2025 года, но все еще остается на высоком уровне

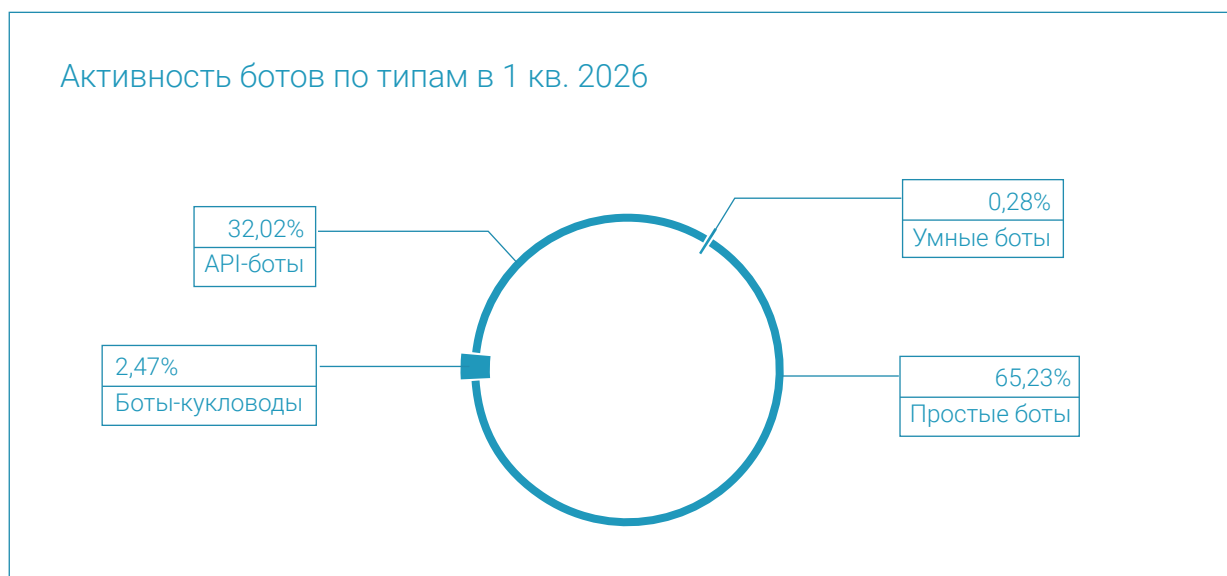
Доля бот-запросов от общего трафика по сегментам в 1 кв. 2026



Заметим, что CURATOR.ANTIBOT позволяет заказчикам самостоятельно настраивать, на каких страницах и на каких доменах будет работать защита. Поэтому «индекс ботовости» может не учитывать значительную часть бот-трафика.

Распределение ботов по типам в 1 кв. 2026 году было следующим:

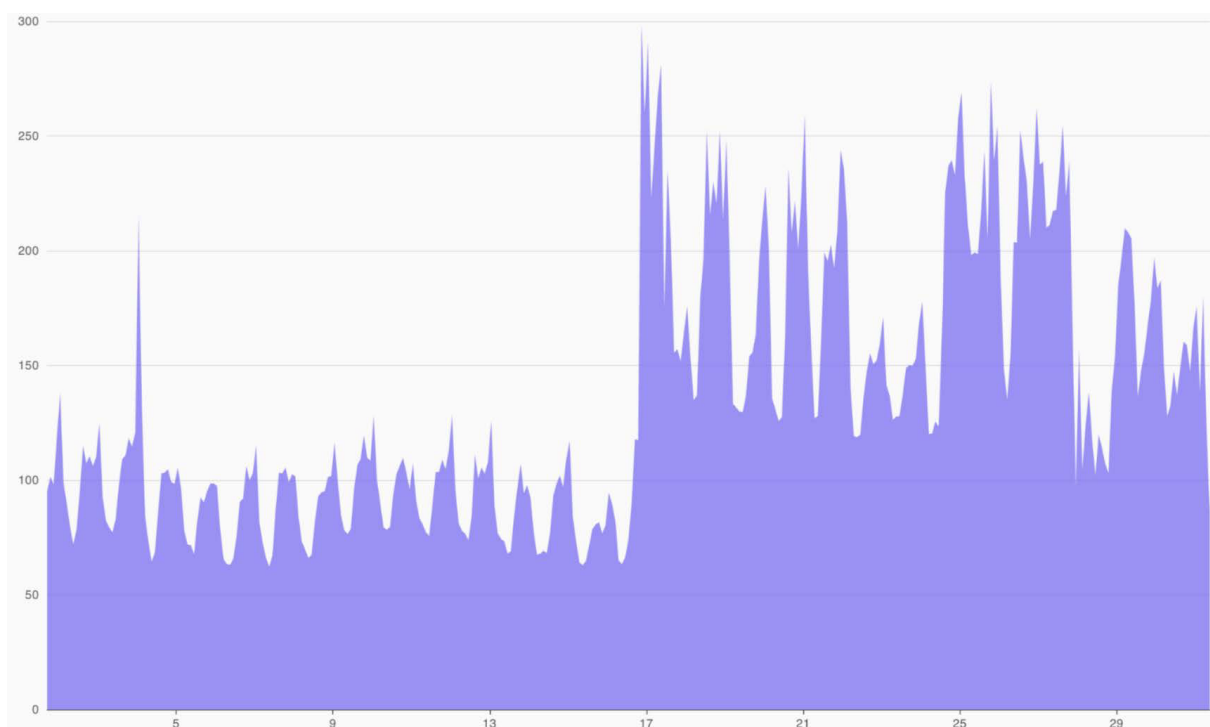
основную часть составляли простые скриптовые боты (65,23%). Боты-кукловоды — роботы, имитирующие окружение обычного пользователя, но с внешней автоматизацией — заняли 2,47%. На умных ботов, то есть роботов, которые знают о проверках и пытаются их обходить, пришлось 0,28%. Наконец, доля API-ботов составила 32,02%.



Наиболее заметные атаки «плохих» ботов в 1 кв. 2026 года

Самая продолжительная бот-атака 1 кв. 2026 года произошла в марте и длилась более двух недель. Атака была направлена на организацию из

сегмента «Электронная коммерция». Суммарное количество заблокированных запросов превысило 178 миллионов.



Самая длительная бот-атака 1 кв. 2026 года

Самая интенсивная атака, заблокированная решением CURATOR.ANTIBOT в 1 кв. 2026 года, была зафиксирована в начале марта, и ее целью также была организация из сегмента «Электронная коммерция». Максимальная интенсивность превысила 120 тысяч вредоносных запросов в секунду. Данная атака не была направлена на сбор каких-либо данных или на взлом ресурса, она представляла собой DDoS-атаку на уровне приложений.

1 КВАРТАЛ



BGP-ИНЦИДЕНТЫ

Количество уникальных автономных систем (АС), ответственных за утечки маршрутов, в 1 кв. 2026 года оставалось на уровне прошлого года: в среднем их было 1913 в месяц.

При этом число уникальных АС, совершавших BGP-перехваты, заметно снизилось по сравнению с прошлым годом: среднемесячное значение упало с 8587 в 2025 году до 7619 в 1 кв. 2026 года, то есть более чем на 10%.

УНИКАЛЬНЫЕ АС, ОТВЕТСТВЕННЫЕ ЗА УТЕЧКИ МАРШРУТОВ	1-й кв. 2026 года	УНИКАЛЬНЫЕ АС, ОТВЕТСТВЕННЫЕ ЗА BGP-ПЕРЕХВАТЫ
1 823	Январь	9 432
1 960	Февраль	6 294
1 955	Март	7 130

ГЛОБАЛЬНЫЕ BGP-ИНЦИДЕНТЫ

Напомним, что для выделения глобальных BGP-инцидентов команда CURATOR.BGP использует ряд пороговых значений. Эти условия включают количество затронутых префиксов и автономных систем, а также степень распространения аномалии по таблицам маршрутизации.

Количество глобальных инцидентов BGP в 1 кв. 2026 года было высоким. Всего за прошедший квартал мы зафиксировали 7 глобальных утечек маршрутов и один глобальный BGP-перехват.





curator.pro
sales@curator.pro
8-800-333-35-22

