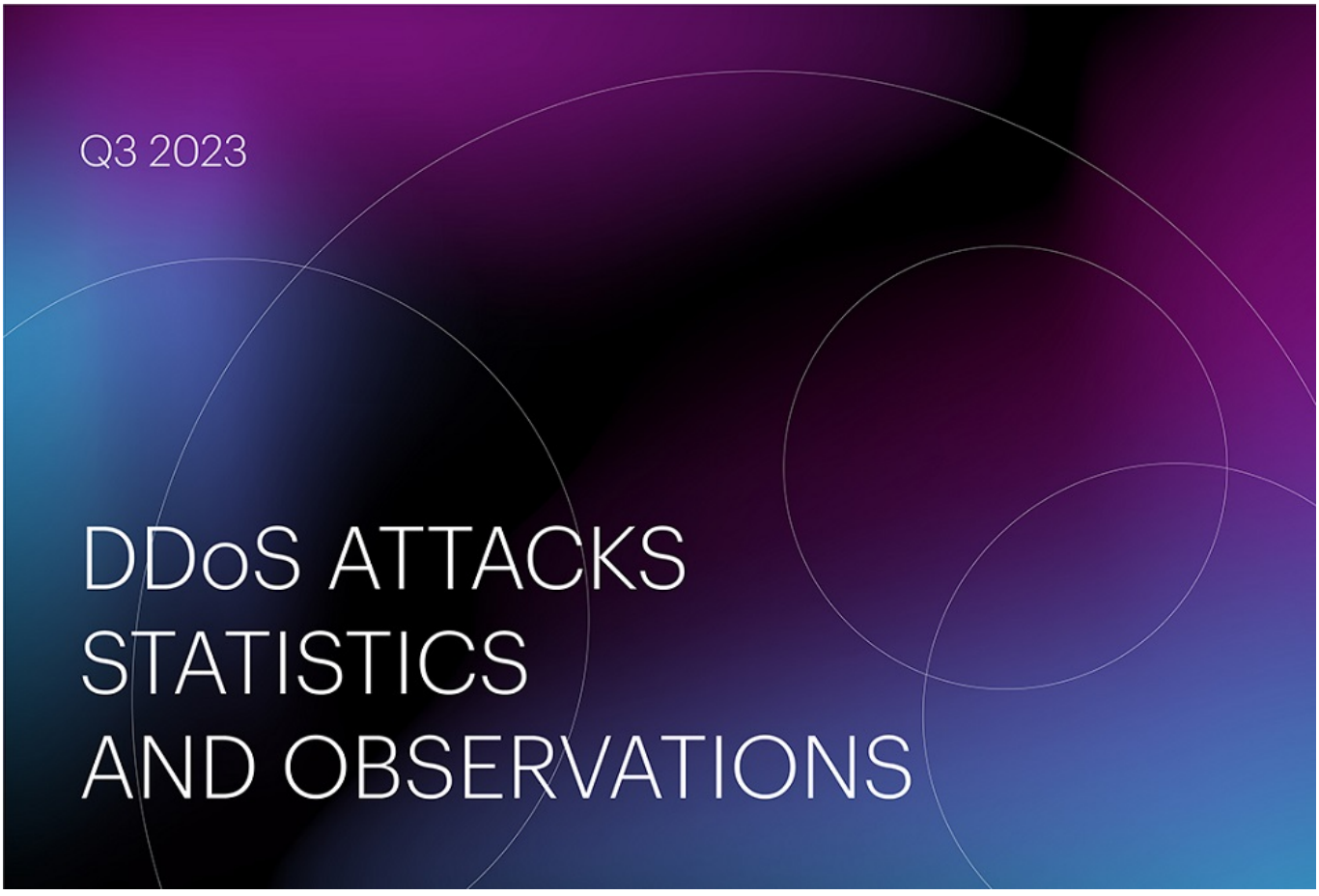
1 НОЯБРЯ 2023 Г., 12:12

Статистика и наблюдения за 3 кварталом 2023 года по DDoS-атакам

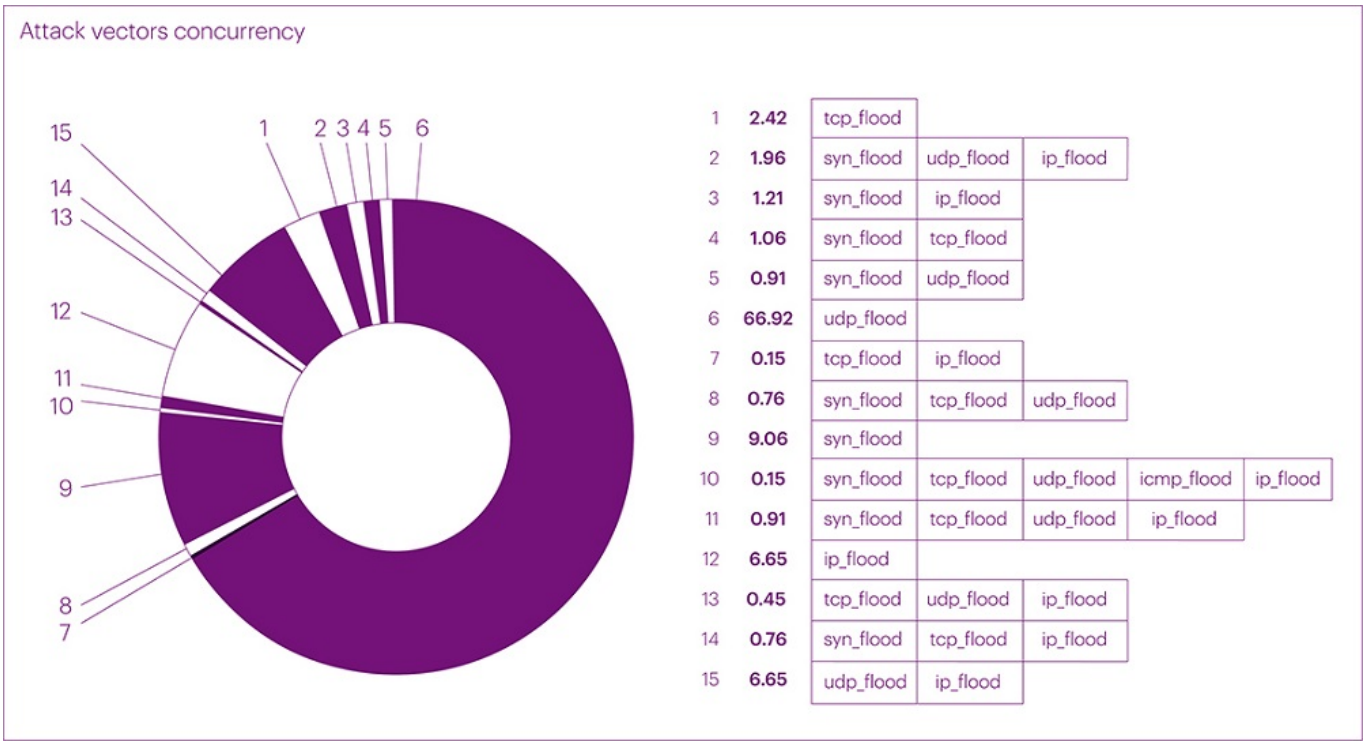
Отчеты



DDoS-атаки с использованием векторов

Третий квартал 2023 года ознаменовался серией интересных выводов и подтверждением некоторых тенденций, которые мы наблюдали в предыдущем квартале.
Давайте начнем с распределения векторов атак по количеству. За прошедший квартал

увеличился на 6,82%, а по сравнению с аналогичным периодом прошлого года - на 14,73%.



Напомним, что в предыдущем отчете за второй квартал 2023 года мы выявили тенденцию к неуклонному увеличению количества UDP-флуд-атак. Мы объяснили это двумя основными причинами. Во-первых, изменение инфраструктуры большинства предприятий и переход на UDP с протоколом DTLS для повышения производительности и масштабируемости. Во-вторых, расширение интернет-каналов в контексте растущей тенденции удаленных офисов и внедрения дополнительных средств коммуникации. В-третьих, изменение модели поведения злоумышленников, которые все чаще используют UDP как более дешевый и простой метод атаки.

В целом распределение смешанных атак по векторам выглядит следующим образом:

- Флуд UDP: 66.92%
- SYN flood: 9.06%
- IP-флуд: 6.65%
- Наводнение по TCP: 2.42%

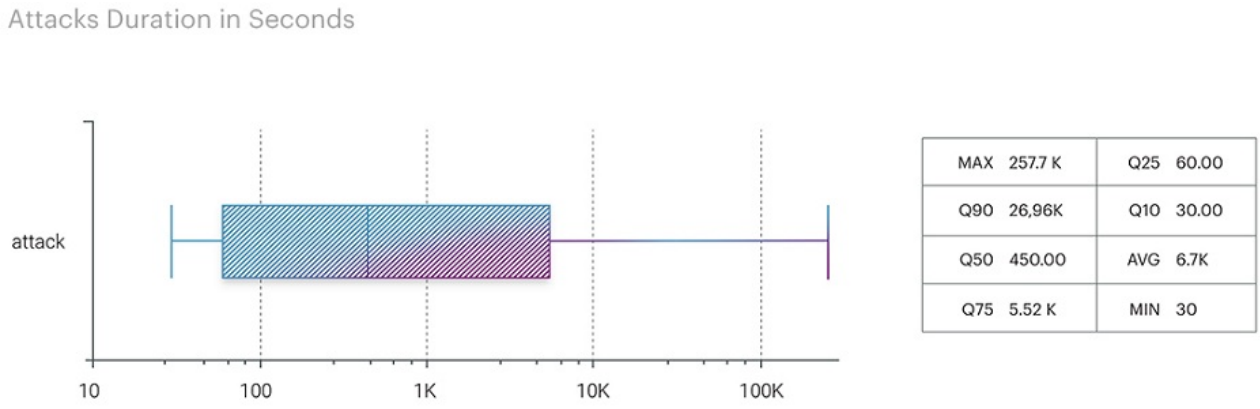
Многовекторные атаки (два или более векторов) занимают вторую позицию в этом распределении, на их долю приходится 14,96% всех атак. По сравнению с предыдущим кварталом этот показатель увеличился всего на 5,8% из-за более медленного роста простых атак. Однако именно комплексные (смешанные) атаки в текущем квартале отличались большей продолжительностью и более высокой пропускной способностью. В статистике чистого распределения векторов атак позиции также существенно не отличаются:

- Наводнение по TCP: 5.90%

По сравнению с предыдущим кварталом изменения в соотношении векторов атак незначительны, в пределах 10%, и не связаны с динамикой общего количества атак. Третий год подряд мы наблюдаем сезонное снижение общего количества атак в третьем квартале. В 2021 году снижение по сравнению с предыдущим кварталом составило 16,45%, в 2022 году - 10,77%, а в этом году оно снизилось на 13,46%. Это еще одно свидетельство изменения модели поведения злоумышленников в отношении UDP.

Продолжительность атак

Продолжительность атак в третьем квартале претерпела изменения по сравнению со вторым кварталом. Например, средняя продолжительность атак составила 66 минут, что на 19 минут больше показателя второго квартала и сопоставимо с показателем первого квартала.

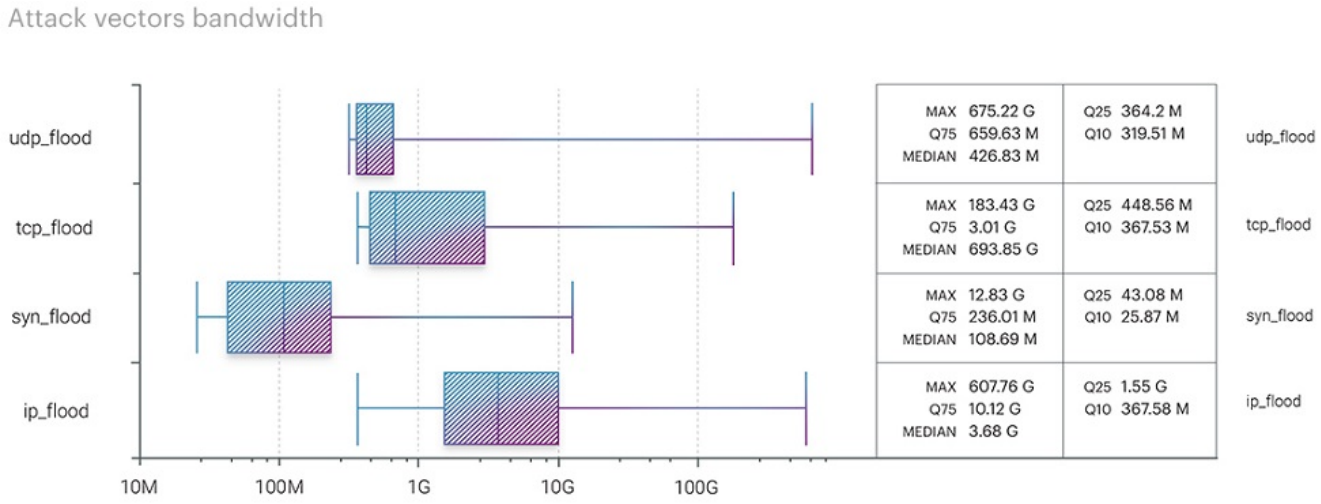


Однако максимальная продолжительность атак установила новый рекорд для этого года, превзойдя даже четвертый квартал предыдущего года, когда самая продолжительная атака длилась почти 70 часов. В конце августа произошла атака на сегмент транспорта и логистики (аэропорты), ставшая самой продолжительной непрерывной атакой в этом году, длившейся почти три дня (71 час 58 минут). Важно отметить, что это была сложная многовекторная атака – UDP + SYN + TCP.
В результате анализа данных за третий квартал продолжительность атак распределилась следующим образом:

- UDP-флуд - 71,58 часа
- SYN-флуд - 70,73 часа
- IP-флуд - 22,5 часа
- TCP flood - 13.29 часов

Векторы атак: пропускная способность

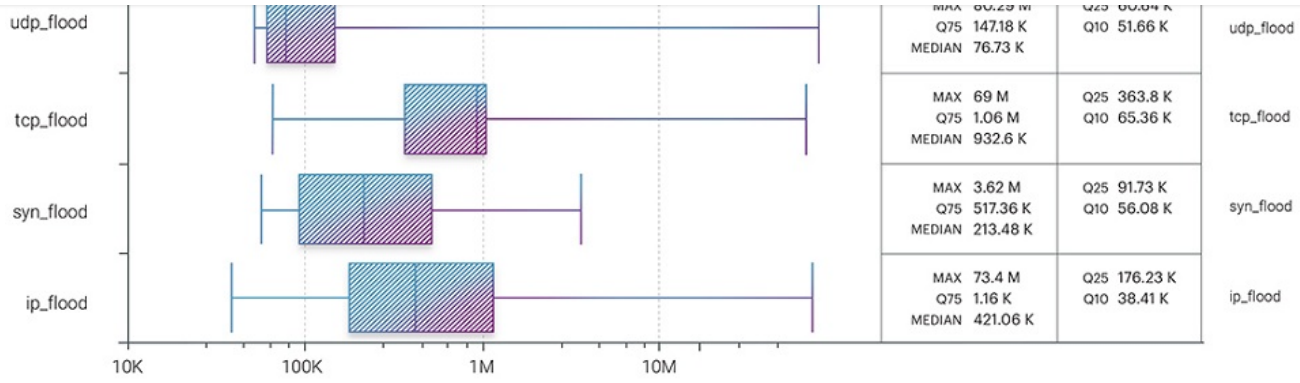
всего на 15 Гбит / с ниже показателя первого квартала (690,23 Гбит /с). В то же время скорость передачи данных IP flood установила новый максимум за последние девять месяцев на уровне 607,76 Гбит/с, что более чем в шесть раз превышает показатели двух предыдущих кварталов (83,49 Гбит/ с в первом квартале и 97,15 Гбит/с во втором квартале).



Интересным открытием стал пиковый битрейт потока ICMP, достигший 114,65 Гбит / с в рамках многовекторной атаки на хостинг-платформы в сегменте IT и Телеком. Напротив, максимальная скорость передачи данных TCP снизилась еще больше - до 183,43 Гбит / с по сравнению с 471,21 Гбит / с в первом квартале и 333,78 Гбит / с во втором.

1. Поток UDP - 675,22 Гбит / с
2. IP-флуд - 607,76 Гбит / с
3. TCP-флуд - 183,43 Гбит / с
4. ICMP-флуд - 114,65 Гбит / с
5. SYN flood - 12,83 Гбит / с

В рейтинге векторов атак, основанном на показателях интенсивности пакетов, сменился лидер. UDP flood, который в предыдущем квартале занимал первую позицию с показателем 69,55 млн. л.с., опустился на вторую позицию с показателем 80,29 млн.л.с., уступив первое место ICMP flood с показателем 155,78 млн.л.с. Однако это скорее исключение из правил, как и максимальный битрейт ICMP на уровне 114,65 Гбит / с. Повышенная скорость потока ICMP, аналогичная битрейту, была вызвана многовекторной атакой на хостинг-платформы в сегменте IT и Телеком, которая длилась всего несколько минут. Следовательно, этот факт не следует считать зарождающейся тенденцией.



В предыдущем квартале мы наблюдали еще одну тенденцию - увеличение битрейта атак в будущем за счет расширения канала и снижения затрат на организацию самих атак. Возвращение скорости передачи данных UDP к уровням начала года соответствует нашим ожиданиям.
Мы продолжаем следить за развитием этой тенденции, но уже сейчас можно сказать, что за последние три года средние показатели по разным векторам атак изменились. Например, скорость передачи данных по IP-каналу со средним пиком в первые три квартала 2021 года на уровне 511,74 Гбит / с, снизилась до 262,80 Гбит / с за первые три квартала этого года. Напротив, средние пиковые скорости передачи данных для UDP продолжают расти. Основываясь на исторических данных за первые три квартала 2021, 2022 и 2023 годов, тенденция выглядит следующим образом:

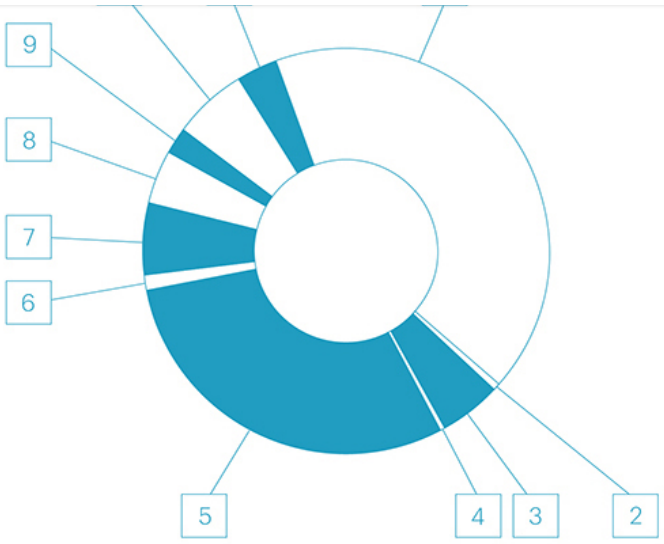
1. 2021 год - в среднем 282,03 Гбит / с на пике
2. 2022 год - в среднем 537,60 Гбит / с на пике
3. 2023 год - в среднем 553,03 Гбит / с на пике

Даже с учетом аномального всплеска трафика в третьем квартале 2022 года, достигшего 903,67 Гбит / с, очевидно, что средний пиковый битрейт UDP неуклонно увеличивается из года в год, редко опускаясь ниже 600 Гбит / с на пике.

DDoS-атаки: сегментация

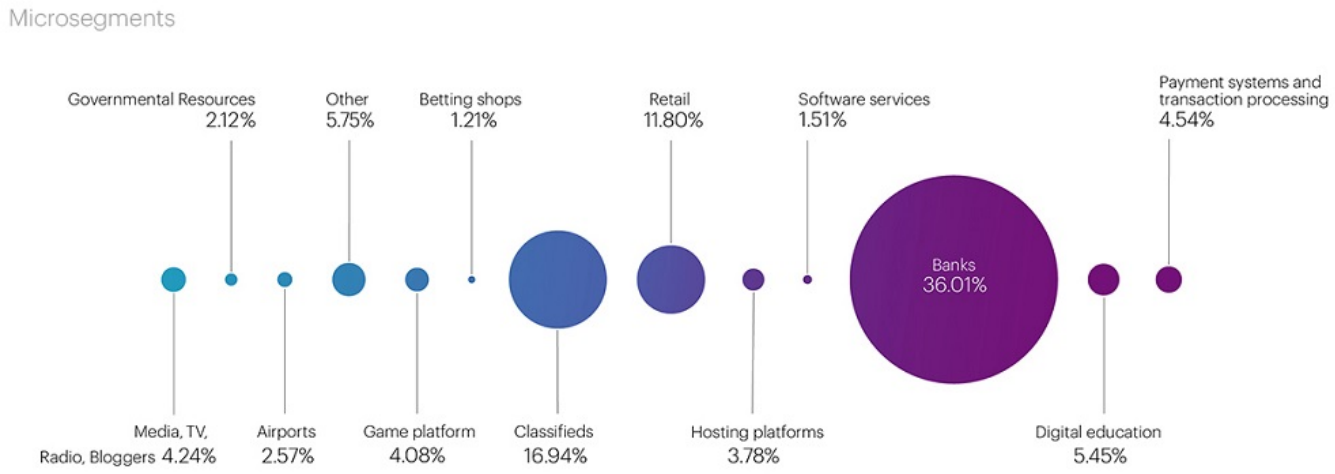
Распределение атак по отраслям (атаки по сегментам)

Как и в предыдущем квартале, сильнее всего пострадал финансовый сектор, на который пришлось 42,06% всех атак в третьем квартале 2023 года. Сегмент электронной коммерции занял второе место, на его долю пришлось 29,80% атак. Сегмент IT и телекоммуникаций занял третье место с 6,05%. Сегмент образовательных технологий на этот раз занял четвертое место с показателем 5,9%, что на 5,36% ниже, чем в предыдущем квартале. Пятерку самых целевых сегментов замкнул сектор СМИ с показателем 4,99%.



2	0.30%	Real Estate
3	4.99%	Media
4	0.15%	Ads&Entertainment
5	29.80%	E-commerce
6	1.21%	Betting
7	5.90%	EdTech
8	4.08%	Games
9	2.12%	Government
10	6.05%	IT&Telecom
11	3.33%	Transport&Logistics

Однако стоит отметить еще один сегмент, заслуживающий особого внимания в этом квартале, - Транспорт и логистику, который подвергся атакам всего в 3,33% случаев, но стал заметен в другом контексте, как мы объясняем ниже.
Рассматривая микросегменты, мы видим следующую разбивку:



В течение года ежеквартальный рейтинг трех наиболее целевых сегментов распределялся следующим образом:

	1 квартал'23	2 квартал'23	3 квартал'23
1	Доска объявлений	Baks	Банки
2	Цифровое образование	Цифровое образование	Доска объявлений
3	Платежные системы	Доска объявлений	Розничная торговля

место занял сегмент цифрового образования (9,5% всех атак). В пятерку лидеров также вошел сегмент платежных систем (6,71%), при этом сегменты розничной торговли и сми почти поровну разделили пятую позицию - 4,53% и 4,78% соответственно. Эти сегменты являются основными целями злоумышленников в этом году.

Распределение атак по сегментам по продолжительности

Присутствие банков, рекламных объявлений и розничной торговли в тройке наиболее целевых микросегментов можно объяснить подготовкой к осеннему сезону. В банках это связано с осенними предложениями по депозитам и кредитам, в то время как в электронной коммерции это связано с подготовкой к сезону возвращения в школу и запуском маркетинговых кампаний и распродаж.

Что касается аэропортов в сегменте транспорта и логистики, который мы выделили ранее, то, хотя он занимает последнюю позицию в нашем списке наиболее целевых сегментов, он подвергся самой продолжительной многовекторной атаке в текущем квартале. Хотя она была относительно небольшой по объему, достигнув максимума всего в 5,94 Гбит / с (UDP flood), атака началась 24 августа по трем направлениям: TCP flood, который длился один день, UDP и SYN flood, которые продолжались до 27 августа. В общей сложности атака длилась почти три дня (71,58 часа UDP-флуда и 70,73 часа SYN-флуда одновременно). В целом, на наш взгляд, эта атака имеет характеристики коммерческой (заказной) атаки.

Вторая по продолжительности атака была зафиксирована в сентябре в сегменте розничной торговли продуктами питания и длилась более 22 часов. Эта атака не только заняла второе место среди самых продолжительных непрерывных атак, но и вошла в пятерку лучших по максимальной интенсивности с пропускной способностью более 100 Гбит / с. Причиной этой атаки, по нашему мнению, стала масштабная маркетинговая кампания, запущенная одной из сетей быстрого питания.

По продолжительности атак сегменты были ранжированы следующим образом:

1. Аэропорты - 2,98 дня
2. Розничная торговля продуктами питания - 22,63 часа
3. Банки - 10.23 часа
4. Хостинг - 9,63 часа
5. Правительственные порталы - 7,8 часа

Самая продолжительная периодическая атака была зафиксирована в сегменте онлайн-игр. Атака, нацеленная на тот же домен, началась 26 июля и закончилась 1 августа, продлившись в общей сложности неделю. Перерывы между скачками трафика составляли не более 15 часов. Пиковый битрейт атаки достиг 183,43 Гбит / с при интенсивности передачи пакетов 15,49 Миль в секунду.

векторов (UDP + SYN + IP). Средняя скорость атаки составила 25,58 Гбит /с.

Во всех трех этих случаях пиковые значения битрейта были достигнуты в основном за счет потока UDP, что еще раз подтверждает нашу гипотезу об увеличении пропускной способности атак из-за перехода многих компаний на UDP.

Распределение атак внутри сегментов по пропускной способности

Что касается пропускной способности, то самая мощная серия атак была зафиксирована в сегменте IT и Телекома, нацеленных на хостинговую платформу. Многовекторная атака началась 20 августа, и трафик с перерывами перетекал в относительно небольших объемах до 1 сентября. Затем был двухнедельный перерыв, и 14 сентября домен подвергся атаке одновременно в четырех векторах с пиковыми нагрузками, достигнув рекордных значений для текущего квартала в трех из четырех векторов: UDP - 675,22 Гбит/с, IP - 607,76 Гбит/с, ICMP - 114,65 Гбит/с, TCP - 55,14 Гбит/с (не самое высокое значение квартала).
В тройку лидеров также вошли онлайн-игры и медиа. С точки зрения пропускной способности остальные сегменты были ранжированы в следующем порядке:

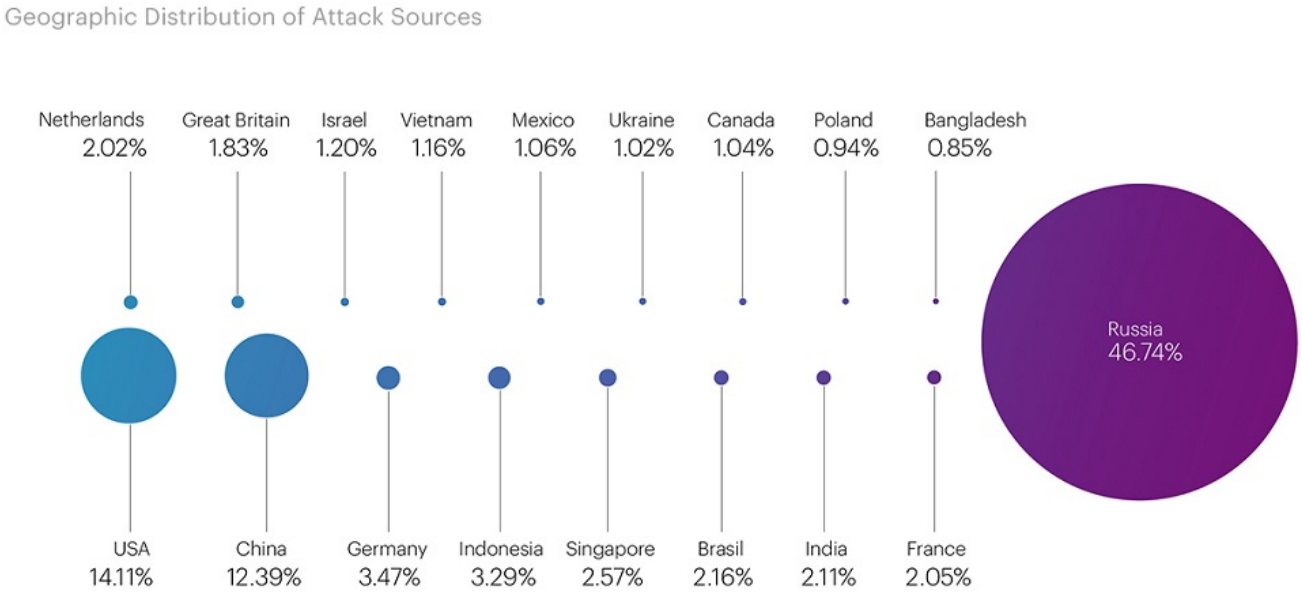
1. IT и Телеком: платформы хостинга - 675,22 Гбит / с
2. Онлайн-игры: игровые платформы - 183,43 Гбит / с
3. Сми: ТЕЛЕВИДЕНИЕ, радио, медиа - 144,97 Гбит / с
4. Электронная коммерция: Розничная торговля продуктами питания - 101,5 Гбит / с
5. Финансы: Платежные системы - 68,85 Гбит / с

Как видно из списка, медиа-сегмент, который занимал первую позицию в предыдущем квартале (333,78 Гбит /с), оказался на третьей позиции, а сегмент ставок вообще не попал в список (он занимал вторую позицию со скоростью 293,64 Гбит /с).

Все вышеупомянутые случаи, на наш взгляд, демонстрируют характеристики коммерческих атак, которые вновь набирают популярность в этом году. Это неудивительно, поскольку ранее мы обсуждали наблюдаемые тенденции, связанные с расширением каналов связи, переходом на новые протоколы для оптимизации работы удаленных офисов. Добавьте к этому легкость и низкую стоимость организации DDoS-атак, и мы получим эффективный инструмент воздействия на бизнес злоумышленников со всеми вытекающими последствиями: репутационными рисками, прямыми финансовыми потерями, упущенной выгодой, сорванными маркетинговыми кампаниями, ресурсами, потраченными на восстановление функциональности системы, и многим другим.

Географическое распределение источников атак

источники трафика, максимально приближенные к регионам их целей.
Общее количество заблокированных IP-адресов увеличилось на 116,42% по сравнению со вторым кварталом, с 18,5 млн до 40,15 млн.



Как и в предыдущем квартале, список возглавила Россия, где было заблокировано 18,7 млн адресов, что составляет почти половину от общего числа заблокированных IP-адресов (46,74%). В топ-3 снова входят США и Китай, 5,66 млн (14,11%) и 4,97 млн (12,39%) внесенных в черный список соответственно.

Германия (1,39 млн), Индонезия (1,32 млн), Сингапур (1,03 млн), Бразилия (867 000), Индия (847,000) и Франция (822,000) по-прежнему остаются в списке лидеров по количеству IP-адресов, внесенных в черный список.
Кроме того, в нашем списке появились новички по сравнению с предыдущим кварталом. Например, в Бангладеш, Израиле и Польше зарегистрировано 340 000, 483 000 и 377 000 заблокированных IP-адресов соответственно.

Крупнейший ботнет

По сравнению со вторым кварталом 2023 года показатель крупнейшего ботнета, обнаруженного нами за период исследования, снизился почти вдвое, составив 85 298 устройств из 20 стран (по сравнению с 136 590 устройствами во втором квартале). Атака ботнета была зафиксирована 10 августа в сегменте платежных систем. Наибольшее количество устройств ботнета было зафиксировано в Индии – 10 671 устройство. В топ-5 также вошли Индонезия (10 092 устройства), Россия (9 757 устройств), США (8 361 устройство), Иран (6497 устройств) и Вьетнам (5786 устройств).

Атаки прикладного уровня (модель L7 OSI)

В третьем квартале количество атак прикладного уровня продолжило снижаться. На этот раз показатель снизился на 26,67% по сравнению со вторым кварталом текущего года. В общей сложности снижение доли атак L7 составило 34% по сравнению с первым кварталом 2023 года.

Для увеличения количества атак L7 необходимы уязвимости, позволяющие создавать экономически эффективные атаки L7 с возможностью генерировать большое количество запросов в секунду. Без уязвимостей стоимость организации атак очень высока, потому что аренда реальных устройств и создание из них ботнета обходится очень дорого. Кроме того, необходимо быть уверенным в том, как обойти защитные механизмы жертвы и является ли это экономически выгодным для злоумышленника.

Вот почему такие атаки не носят массового характера, а скорее носят узконаправленный характер.

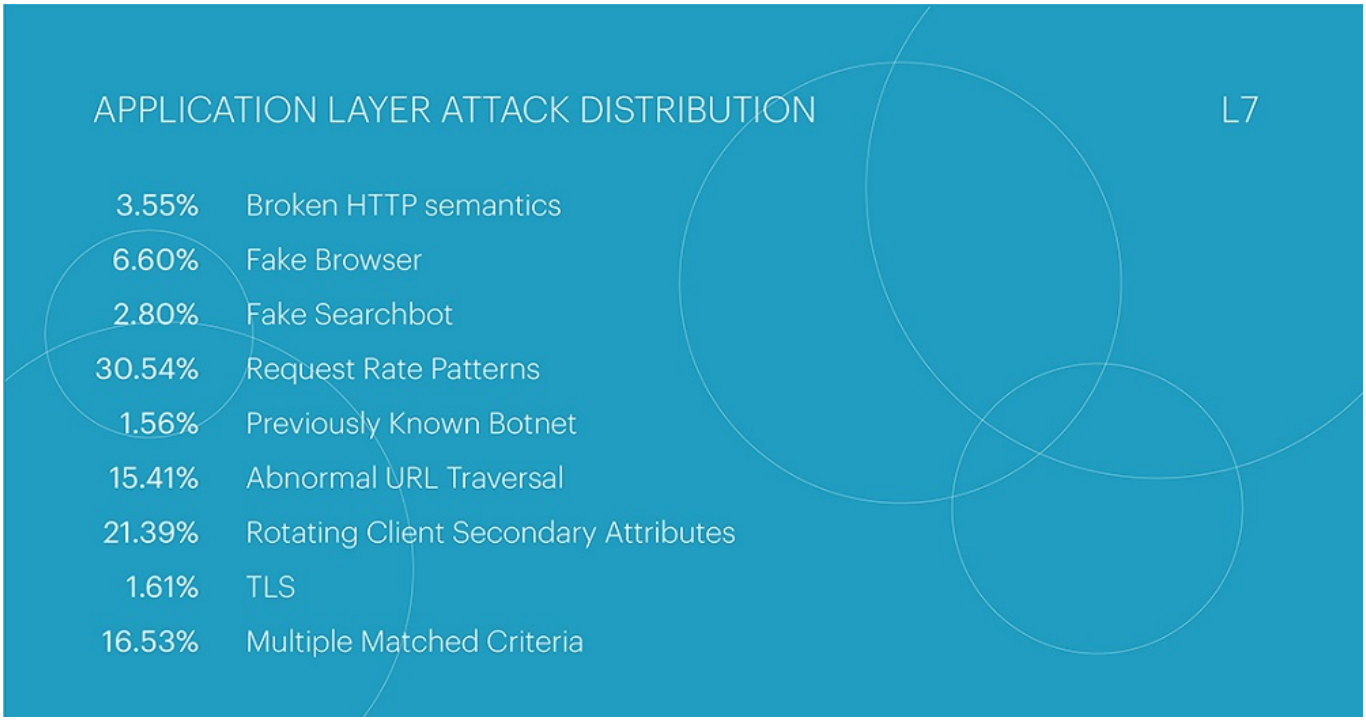
Генерация большого количества запросов от небольшого количества устройств возможна, если зараженное устройство достаточно мощное для этой цели. Например, можно арендовать или заразить IP-адрес с выделенным сервером или виртуальный сервер, с которого можно генерировать от нескольких сотен до нескольких тысяч запросов. Атаки такого рода относительно легко обнаруживаются и нейтрализуются поставщиками облачной защиты, которые анализируют трафик на уровне приложений (L7).

С появлением новой версии протокола HTTP/2 стало возможным генерировать сотни запросов в рамках одной TCP-сессии, одновременно нацеливаясь на разные элементы атакуемого ресурса. Новый протокол практически не имеет ограничений на количество запросов в рамках одного сеанса TCP, позволяя злоумышленникам оставаться

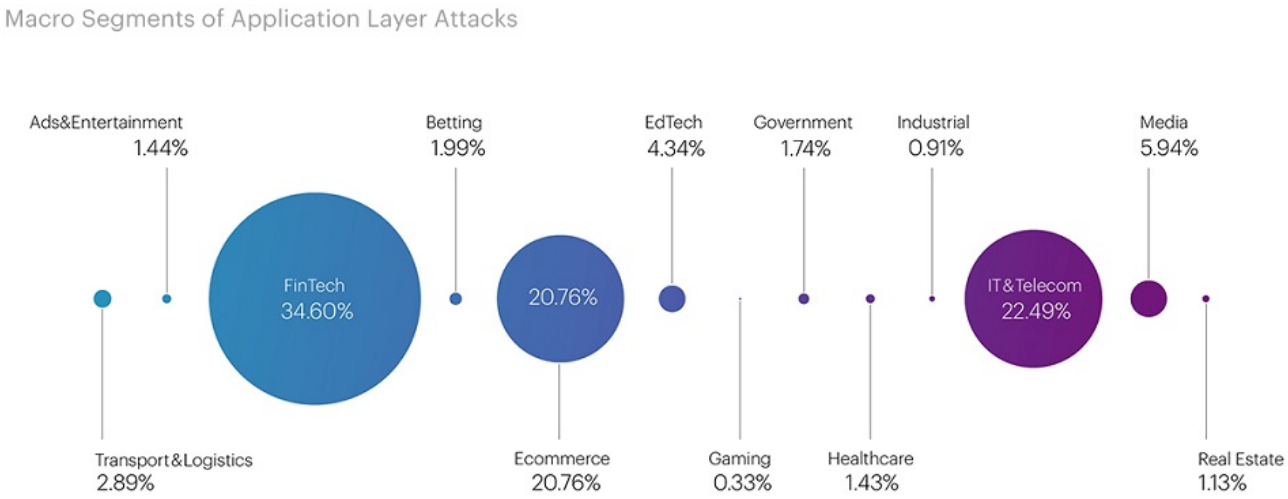
Кроме того, с помощью атак L7 злоумышленники могут принудительно масштабировать ресурсы жертвы по горизонтали, тем самым значительно увеличивая счет за облачные ресурсы. Такие атаки часто организуются против компаний, арендующих серверы в облаке.
По формальным критериям ресурсы жертвы не ухудшаются во время атаки, поскольку по мере увеличения объемов трафика сервер мгновенно масштабируется. Однако в конце месяца это может обернуться значительными финансовыми потерями для заказчика, поскольку стоимость использования ресурсов в облаке может увеличить счет в несколько раз.

Распространение атак L7

В списке самых популярных классов атак произошла смена руководства. Шаблоны частоты запросов, которые являются индикаторами поведения, отличающегося от ожидаемого законного поведения пользователей с точки зрения частоты запросов, составили 30,54% всех атак. Смена руководства не приводит к значительному увеличению класса шаблонов частоты запросов, поскольку его доля увеличилась лишь на 4,72% по сравнению с предыдущим кварталом. Причиной этого является значительное снижение доли класса вторичных атрибутов Rotating Client, который состоит из необычного набора заголовков в запросах. Лидер предыдущего квартала сейчас занимает вторую позицию с показателем 21,39%, что на 11,58% ниже, чем в предыдущем квартале. В тройку лидеров вошли многоклассовые атаки, которые объединяют два или более классов атак, - 16,53%. Их доля увеличилась на 4% по сравнению с предыдущим кварталом.



место с 22,49% всех атак (на третьей позиции рейтинга за второй квартал - 13,08%). Сегмент электронной коммерции замкнул тройку самых целевых сегментов на этом уровне с показателем 20,76% (лидер во втором квартале с показателем 33,04%).



При изучении микросегментов становятся очевидными отличия от атак на уровне инфраструктуры (L3-L4). В то время как злоумышленники часто нацеливались на банки на сетевом и транспортном уровнях, на уровне приложений фокус атак сместился на платежные системы, которые заняли первое место с 17,17% всех атак. В тройку лидеров атак L7 также вошли программные сервисы (14,55%) и розничная торговля (9,25%). Напротив, на L3-L4 объявления заняли второе место, а розничная торговля - третье.

Среди наиболее часто используемых классов атак на платежные системы наиболее распространенными были шаблоны частоты запросов (34,17%), за ними следовали многоклассовые атаки (18,85%) и неправильный обход URL-адресов (16,67%) (четвертый по популярности класс атак в третьем квартале составил 15,41%). Шаблоны частоты запросов чаще всего используются злоумышленниками из-за их простоты. В этом сегменте класс вторичных атрибутов ротируемого клиента занимал лишь четвертую позицию с показателем 13,7%, тогда как в предыдущем квартале это место занимал класс Fake Browser (11% во втором квартале).

Кроме того, стоит отметить, что сегменты банковского обслуживания (8,10%) и розничной торговли продуктами питания (7,85%) не остались без внимания злоумышленников. На совокупную долю пяти наиболее целевых сегментов приходится более половины, а именно 56,92%, всех атак на уровне приложений.

L3-L4		L7	
Рейтинг (в порядке убывания)	**Поделиться**	**Рейтинг (в порядке**	**Поделиться**

Финансовый сектор: Банки	36,01%	сектор: Платежные системы	17,17%
Электронная коммерция: Объявления	16,94%	IT и Телеком: программные услуги	14,55%
Электронная коммерция: Розничная торговля	11,80%	Электронная коммерция: Розничная торговля	9,25%
Образовательные технологии: онлайн-образование	5,45%	Финансовый сектор: Банки	8,10%
Финансовый сектор: Платежные системы	4,54%	Электронная коммерция: Розничная торговля продуктами питания	7,85%

Рейтинг атак с наибольшим количеством запросов в секунду (RPS) в третьем квартале был составлен на основе динамики количества запросов. Этот класс использовался при атаке на сегмент Classified s, достигнув пиковой частоты 978,4 тыс. запросов в секунду. Этот сегмент не попал ни в один из рейтингов атак на уровне приложений, но мы зафиксировали самую высокую частоту запросов за все первые девять месяцев 2023 года. Это превышает показатель второго квартала более чем на 633%. Атака длилась всего одну минуту и была частью многоклассовой серии атак на этот сегмент с 24 по 30 сентября. Всего в рамках этой серии было совершено 18 атак на один домен.

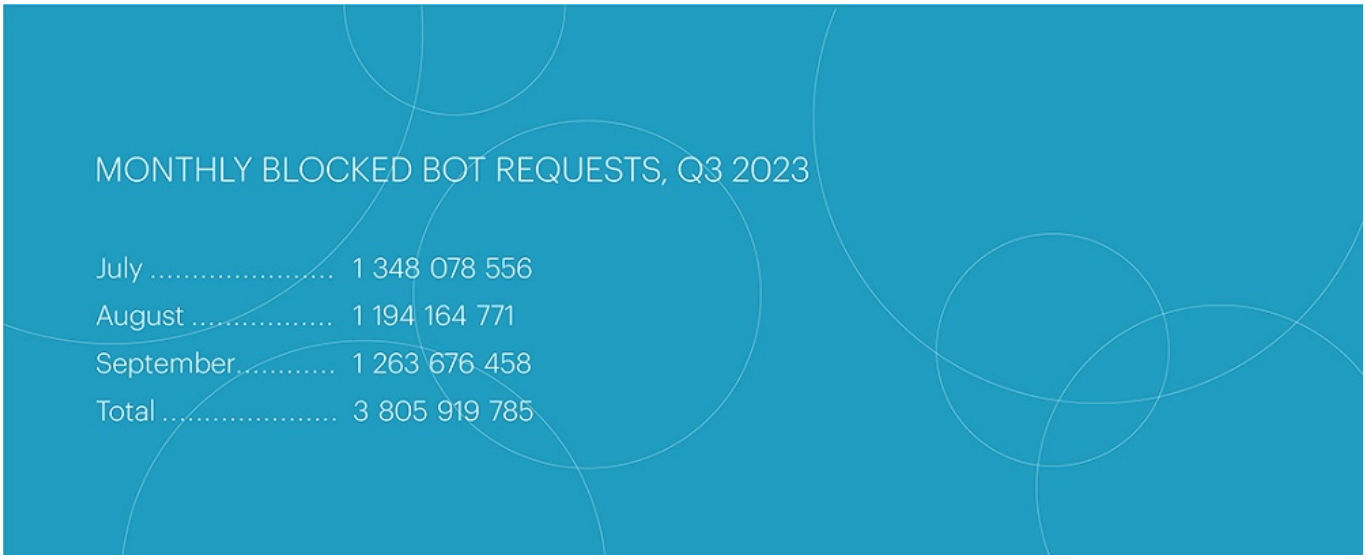
Хотя эти атаки не были продолжительными, достигнув максимума всего в 2,5 минуты, аналогично атакам на уровнях L3-L4, есть признаки коммерческой (заказной) DDoS-атаки, как упоминалось ранее. В дополнение к вышеупомянутому классу, в атаке также использовались классы "Поддельный браузер", "Изменяемые вторичные атрибуты клиента" и "Неправильный обход URL". Примечательно, что ботнет, использованный для атаки, состоял всего из 3246 устройств. Среднее количество устройств во всех ботнетах, задействованных в этой серии атак, составило всего 17 092 устройства.
Вторая по интенсивности атака была зафиксирована в сегменте хостинга, достигнув 445,7 тыс. запросов в секунду и длившись 2 минуты. Замыкает тройку лидеров атака с

Самая продолжительная атака на уровне приложений была зафиксирована в сегменте электронной коммерции (розничная торговля). Атака с интенсивностью всего 527 запросов в секунду длилась более трех дней (73,06 часа). Вторая по продолжительности атака пришлась на сегмент программных услуг (IT и телеком) продолжительностью 10,35 часа, а третья - на сегмент онлайн-образования продолжительностью 10,15 часа. Во всех трех случаях атаки были многоклассовыми (с использованием двух или более классов атак).

Средняя продолжительность атак на уровне приложений в третьем квартале составила примерно 20 минут при средней интенсивности 4,9 тысячи запросов в секунду.

Статистика защиты от ботов

По сравнению со вторым кварталом количество бот-атак сократилось на 10%, составив 3 805 919 785. Пиковые значения в третьем квартале были ниже, и не было зафиксировано рекордных по объему и продолжительности массовых атак ботов, которые значительно выделялись бы на фоне повседневной активности. Самым активным месяцем в третьем квартале был июль, с наибольшим количеством атак: 1,35 миллиарда заблокированных запросов ботов.

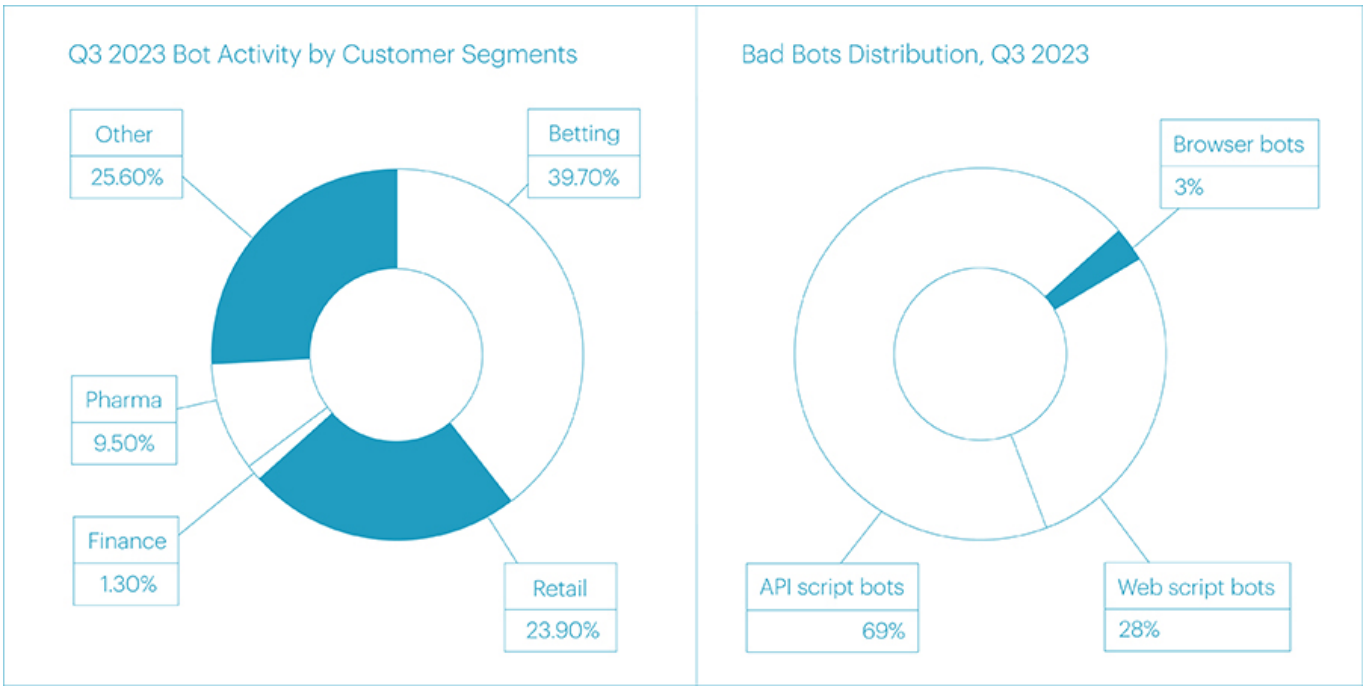


Сегменты беттинга и онлайн-ритейла остаются на вершине списка атакующих третий квартал подряд. В третьем квартале их доли составили 39,7% и 23,9% соответственно. Третью и четвертую позиции, как и в предыдущем периоде, заняли фармацевтические препараты (9,5%) и финансовые организации (1,3%).

Количество фоновых инцидентов и инцидентов с ботами в сегменте онлайн-аптек почти удвоилось по сравнению со вторым кварталом 2023 года. Серьезные ботнеты, которые ранее были нацелены на розничные и развлекательные ресурсы, такие как

Крупнейшая бот-атака произошла в секторе ставок 24 сентября. В тот день была зафиксирована 24 255 701 атака, что, однако, почти на 10 миллионов меньше, чем пиковая атака в том же сегменте во втором квартале. Самая быстрая атака, как и в предыдущем периоде, произошла в тот же день, 24 сентября, в сегменте электронной коммерции. Скорость атаки достигла 43 644 запросов ботов в секунду (RPS), что в 3,5 раза выше самой быстрой атаки во втором квартале, также произошедшей в сегменте электронной коммерции.

Продолжительность атак ботов увеличилась, но количество резких скачков сократилось. Основной причиной активности ботов теперь является фоновый режим: атаки, которые создают непрерывную нагрузку на ресурсы цели 24/7 без резких колебаний. Хорошей иллюстрацией этого является то, что рекордные значения нагрузки в день и единичные случаи атак ботов сейчас намного ниже, чем в предыдущем квартале. Например, крупнейшая атака в текущем квартале была на 30% слабее показателей предыдущего периода, но общее количество запросов ботов было всего на 10% ниже. Это указывает на то, что большая часть усилий была перенесена на фоновую загрузку.



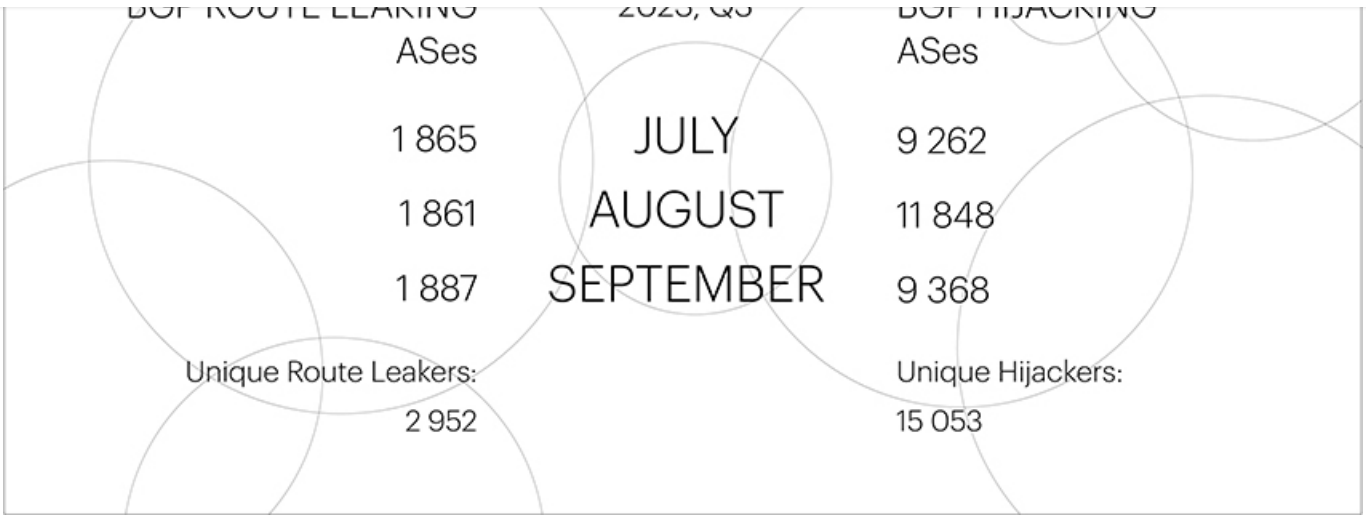
Наиболее используемыми методами распространения ботов стали API-скрипты (69%), веб-скрипты (28%) и браузеры (3%). Среднее ежедневное количество запросов ботов на этот раз составило 41 823 294, что почти на 5 миллионов запросов меньше по сравнению с предыдущим периодом.

Теперь их организаторы быстрее пресекают атаки ботов, когда они сталкиваются с контрмерами со стороны систем защиты от ботов. В то время как во втором квартале часто случалось, что после нейтрализации атаки она могла затянуться еще на неделю и

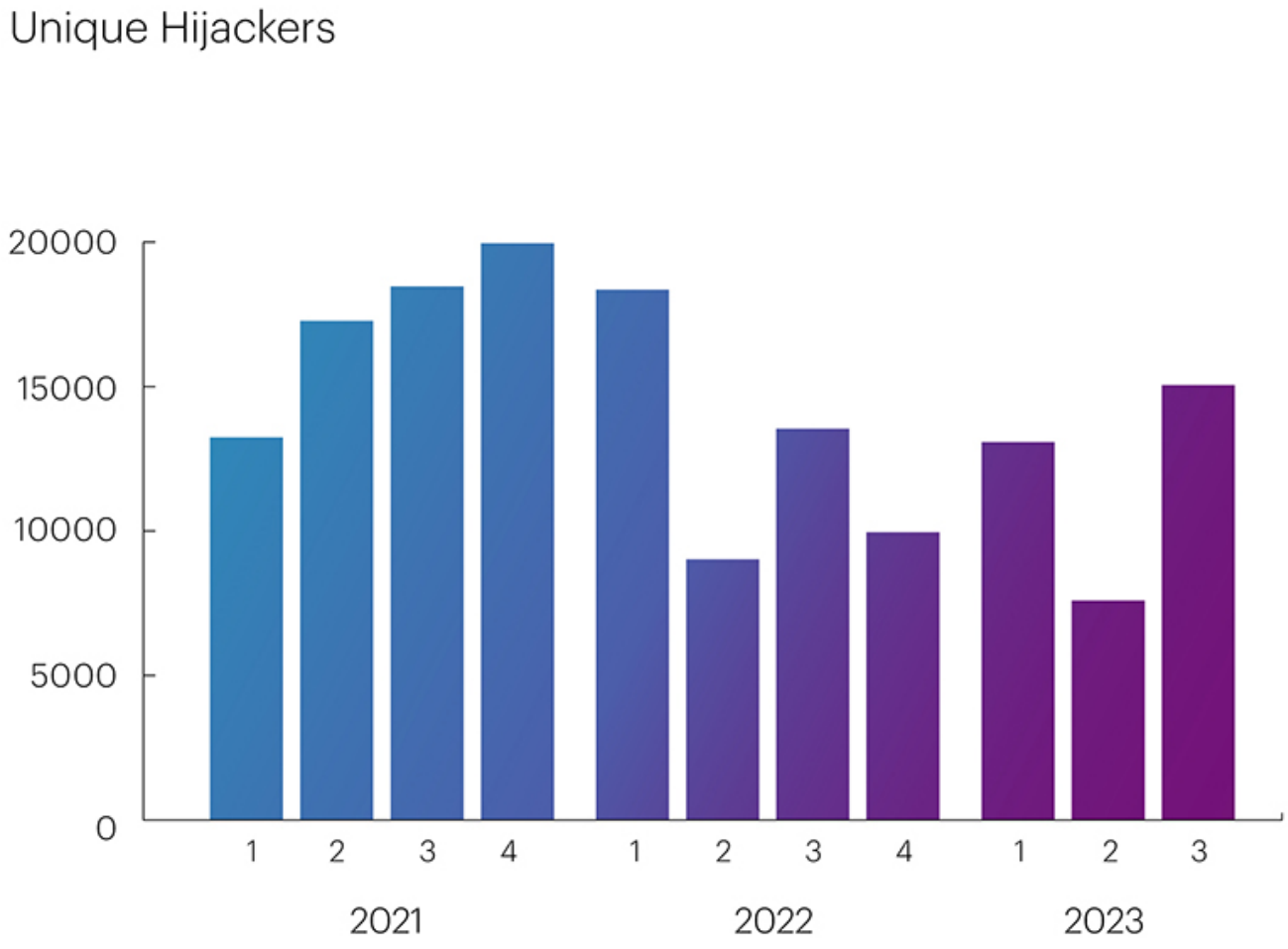
Популярность новых инструментов для очистки и автоматизации браузера (новый Chrome headless) в настоящее время ниже, чем ожидалось. Они не выделяются массовыми скачками и не выделяются в общем ландшафте атак. Однако это может быть затишьем перед бурей. Мы ожидаем широкого использования ранее незамеченных векторов активности ботов в четвертом квартале, особенно во время Черной пятницы.

Инциденты BGP

Количество уникальных автономных систем, задействованных в утечках маршрутов, в третьем квартале осталось примерно на том же уровне, что и в предыдущем периоде. Однако количество уникальных автономных систем, осуществляющих перехваты BGP, увеличилось почти в два раза, с 7 595 до 15 053.



Несмотря на увеличение числа попыток взлома BGP в третьем квартале, наблюдается четкая тенденция к сокращению их количества в годовом исчислении.



Пик количества взломщиков BGP пришелся на четвертый квартал 2021 года и первый квартал 2022 года, достигнув 19 960 и 18 352 человек соответственно, после чего их численность начала снижаться, достигнув минимальных значений во втором квартале этого года - 7 595.

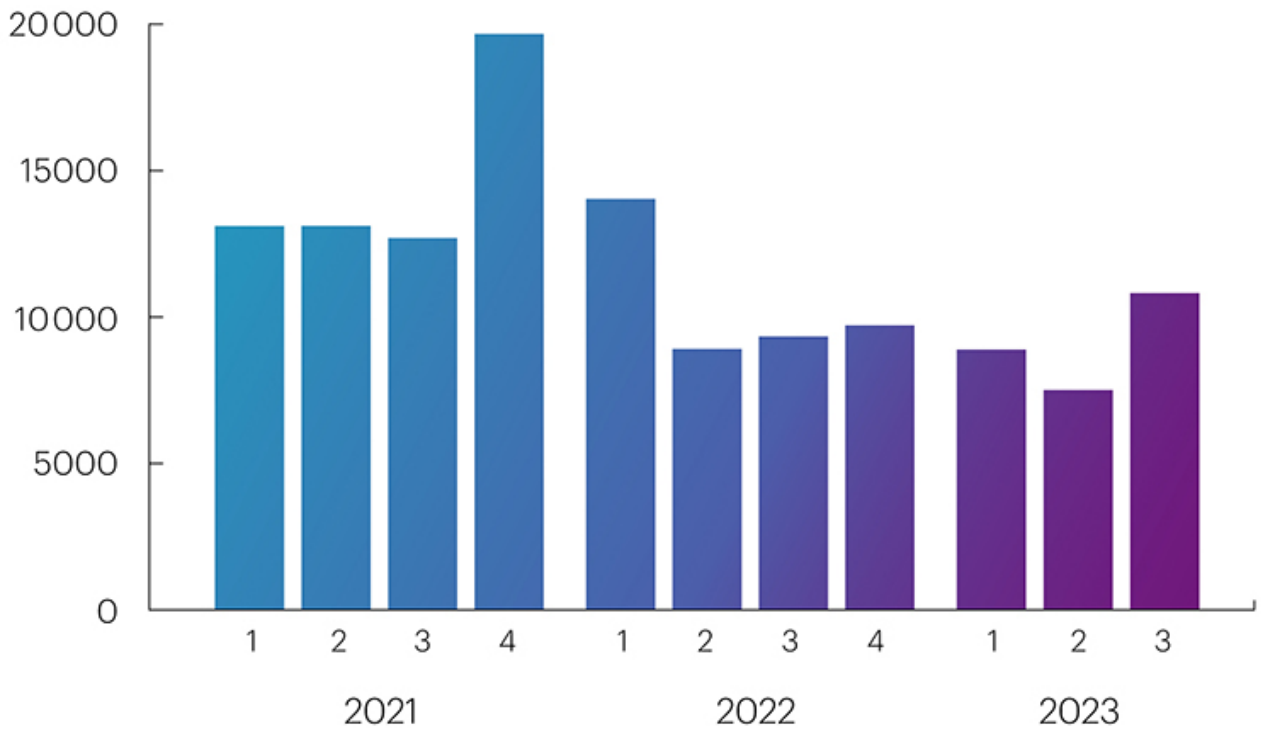
Сокращение в первую очередь связано с широким внедрением проверки на основе ROA в RPKI. С одной стороны, количество записей ROA в репозиториях RPKI увеличивается, и

пользователей от попадания в автономные системы с недопустимыми объявлениями. Следовательно, с точки зрения нашей системы мониторинга, это приводит к снижению видимости автономных систем, занимающихся перехватом BGP.

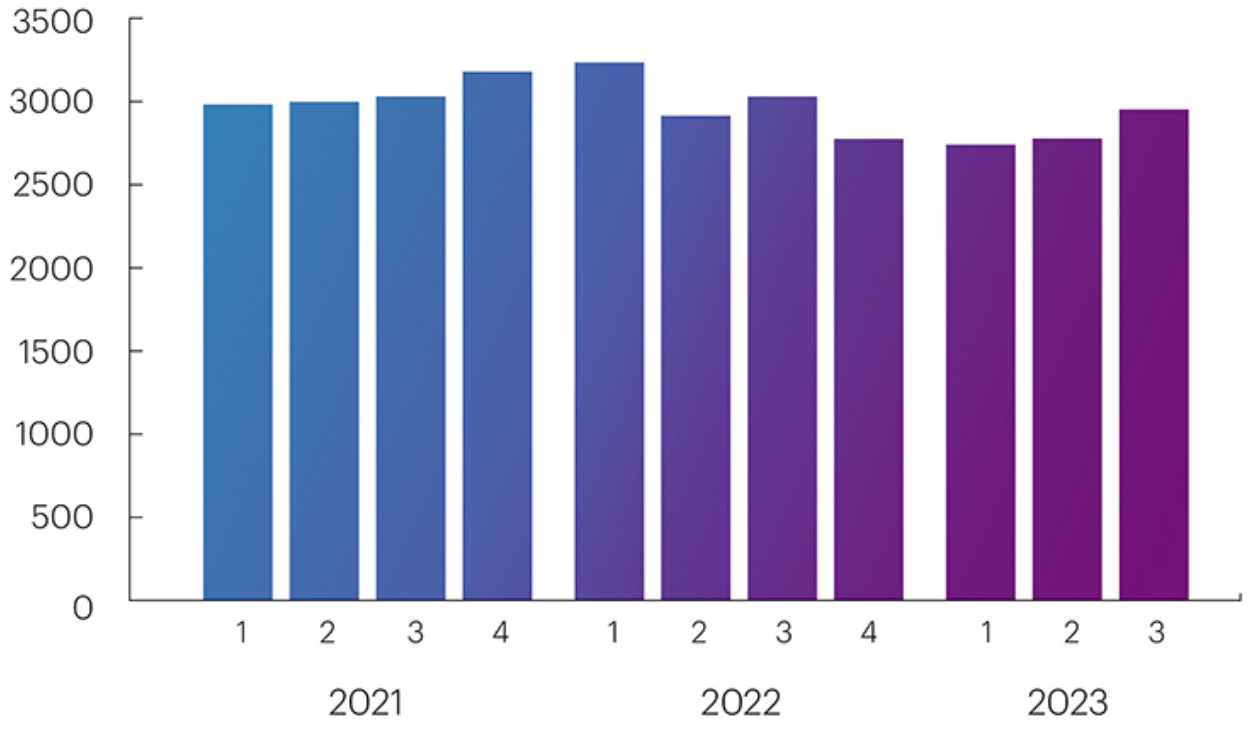
Однако третий квартал этого года стал исключением из правил, поскольку возросшие показатели резко контрастировали с общим снижением числа взломщиков BGP.

Qrator.Команда Radar провела исследование этого необычного всплеска, в ходе которого они выявили автоматическое объявление префиксов IPv6 автономными системами в диапазоне APNIC (в виде номеров от 142067 до 146745), которые обычно принимают минимальное участие в глобальной маршрутизации. Эти объявления привели к нетипичному увеличению количества уникальных ASN примерно на 4000 каждый месяц.

Причиной этого стали действия Китайской образовательной и исследовательской сети (CERN), образовательной и исследовательской сети в Китае, которые, вероятно, были направлены на развитие китайского интернета следующего поколения (CNGI), основанного на использовании IPv6. Однако, с точки зрения глобальной маршрутизации, объявление префиксов от имени сторонних ASE не считается хорошей практикой. После фильтрации данных за третий квартал и исключения перехвата адресного пространства китайской сетью был получен более четкий график, показывающий, что количество уникальных взломщиков BGP действительно уменьшалось по сравнению с серией



К сожалению, механизм RPKI ROA не позволяет предотвращать утечки маршрутов, и тенденция к сокращению числа взломщиков BGP-каналов практически не заметна для участников утечки маршрутов BGP. Их количество меняется очень незначительно от квартала к кварталу.



Чтобы уменьшить количество ASE, вызывающих утечки маршрутов, необходимо реализовать механизм защиты ASPA, основанный на проверке AS_PATH. Этот механизм, как и RPKI ROA, работает на хорошо отлаженной инфраструктуре RPKI и может устранять большинство BGP-инцидентов.

Глобальные инциденты BGP

У Qrator.Radar team есть набор конкретных пороговых значений, которые отличают глобальные инциденты от всех остальных. К ним относятся количество затронутых префиксов, автономные системы и степень распространения аномалий в таблицах маршрутизации.
В отличие от предыдущего периода, в третьем квартале 2023 года увеличилось количество утечек по глобальным маршрутам.

Глобальные утечки маршрутов BGP	**Глобальные перехваты BGP**
Июль: 3 Август: 2 Сентябрь: 1	Июль: 0 Август: 1 Сентябрь: 0

Подробный анализ распространения и влияния на трафик двух обнаруженных нами инцидентов, произошедших 28 и 29 августа, был проведен нашим коллегой Дугом

Основные выводы:

1. UDP-флудинг продолжал набирать обороты, установив новый рекорд в 66,92% от общего числа атак в смешанных значениях и 64,13% в абсолютных цифрах.
2. Комплексные (смешанные) атаки отличались наибольшей продолжительностью и пропускной способностью.
3. Третий год подряд мы наблюдаем сезонное снижение общего количества атак в третьем квартале. В этом году показатель снизился на 13,46%, что еще раз указывает на сдвиг в поведении злоумышленников в сторону UDP.
4. Самая продолжительная атака была зафиксирована в конце августа, нацеленная на сегмент транспорта и логистики (аэропорты) и продолжавшаяся почти три дня (71 час 58 минут).
5. В третьем квартале, как и в предыдущем квартале, Финансовый сектор пострадал от атак больше всего - 42,06%.
6. Наиболее нацеленными микросегментами были банки, рекламные объявления и розничная торговля, что можно объяснить подготовкой и началом осеннего сезона.
7. Коммерческие атаки в этом году вновь набирают популярность из-за расширения каналов связи, перехода на новые протоколы для оптимизации удаленных офисов, а также простоты и низкой стоимости организации.
8. Для обхода геоблокировки злоумышленники стали активнее использовать локальные источники трафика, максимально приближенные к региону проживания своих жертв, что привело к увеличению общего количества заблокированных IP-адресов на 116,42% по сравнению со вторым кварталом.
9. Количество атак L7 продолжает снижаться (снизившись еще на 26,67%), при этом атаки становятся очень целенаправленными, а не массовыми.
10. Большинство атак уровня L7 были нацелены на сегмент финансовых технологий (34,60%). Второе место занял сегмент IT и телекома (22,49% всех атак), в то время как электронная коммерция заняла третье место (20,76%).
11. По сравнению со вторым кварталом количество бот-атак сократилось на 10%. Самым активным месяцем в третьем квартале был июль, с наибольшим количеством атак: 1,35 миллиарда заблокированных запросов ботов.
12. Сегменты беттинга и онлайн-ритейла третий квартал подряд остаются на первых местах по количеству инцидентов с ботами.
13. Несмотря на то, что количество уникальных взломов автономных систем BGP увеличилось почти в 2 раза в третьем квартале, наблюдается четкая тенденция к их ежегодному снижению.
14. Внедрение проверки на основе RPKI ROA продолжает оказывать значительное влияние на сокращение числа взломщиков BGP.

Другие выводы:

2. Количество крупнейших ботнетов сократилось почти вдвое по сравнению со вторым кварталом, составив 85 298 устройств.
3. В третьем квартале по атакам с наибольшим количеством запросов в секунду (RPS) лидировал класс Request Rate Patterns, использованный при атаке на сегмент объявлений с пиковой частотой 978,4 тыс. запросов в секунду.
4. Самая продолжительная атака на уровне приложений наблюдалась в розничном сегменте, длившаяся более трех дней (73,06 часа) с интенсивностью всего 527 запросов в секунду. Вторая по продолжительности атака была направлена на сегмент программных услуг (IT и телеком) в 10.35, а третье место занял сегмент онлайн-образования в 10.15. Все три атаки были многоклассовыми.
5. Продолжительность атак ботов увеличилась, но количество резких скачков сократилось. Основная активность ботов теперь достигается в фоновом режиме: атаки, которые создают непрерывную нагрузку на ресурсы цели 24/7 без резких колебаний.
6. В третьем квартале произошел всплеск числа взломщиков BGP из-за действий Китайской сети образования и исследований (CERN), вероятно, направленных на развитие китайского интернета следующего поколения (CNGI), основанного на использовании IPv6.
7. Количество утечек маршрутов меняется очень незначительно от квартала к кварталу. Чтобы уменьшить количество ASE (автономных систем), вызывающих утечки маршрутов, необходимо реализовать механизм защиты ASPA, основанный на проверке AS_PATH.

Примечания

Боты с веб-скриптами: скриптовые процедуры, которые делают прямые запросы на загрузку веб-страниц и анализируют содержимое страницы на предмет определенных данных без использования браузера или внешнего приложения.

Боты-скрипты API: скриптовые процедуры, которые выполняют прямые вызовы API к серверной части веб-или мобильного приложения для загрузки необходимых данных, игнорируя внешний интерфейс.

Браузерные боты: платформы автоматизации высокого уровня, которые работают с автономными или модифицированными веб-браузерами и максимально приближены к человеческому опыту использования.