QRATOR LABS

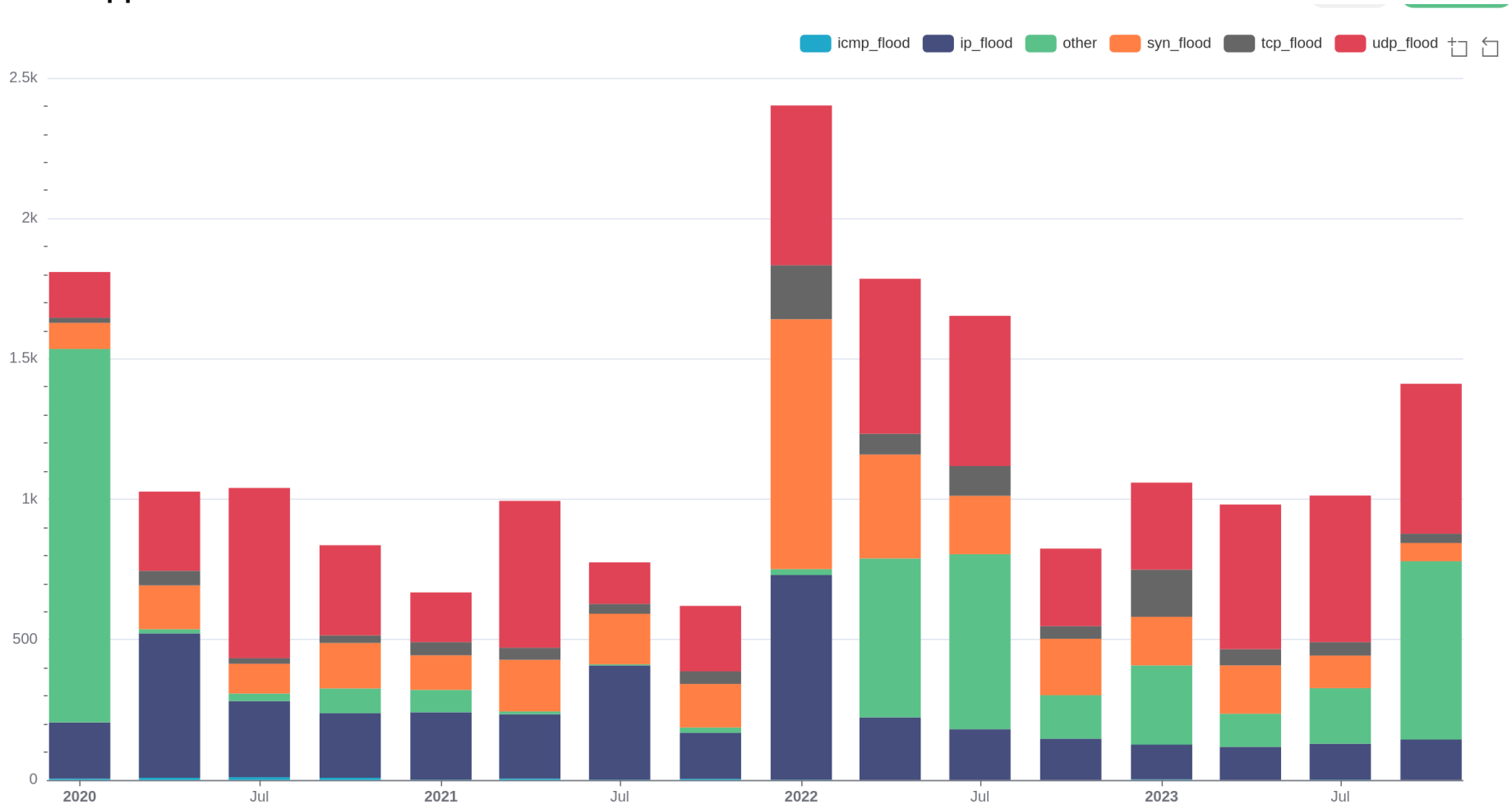
Как эффективно противодействовать DDoS-атакам

Новые тренды, кейсы использования сети фильтрации Qrator Labs и что ждет нас в 2024 году

О РЕЗУЛЬТАТАХ ИССЛЕДОВАНИЯ QRATOR LABS ЗА ТРЕТИЙ И ЧЕТВЕРТЫЙ КВАРТАЛ 2023:

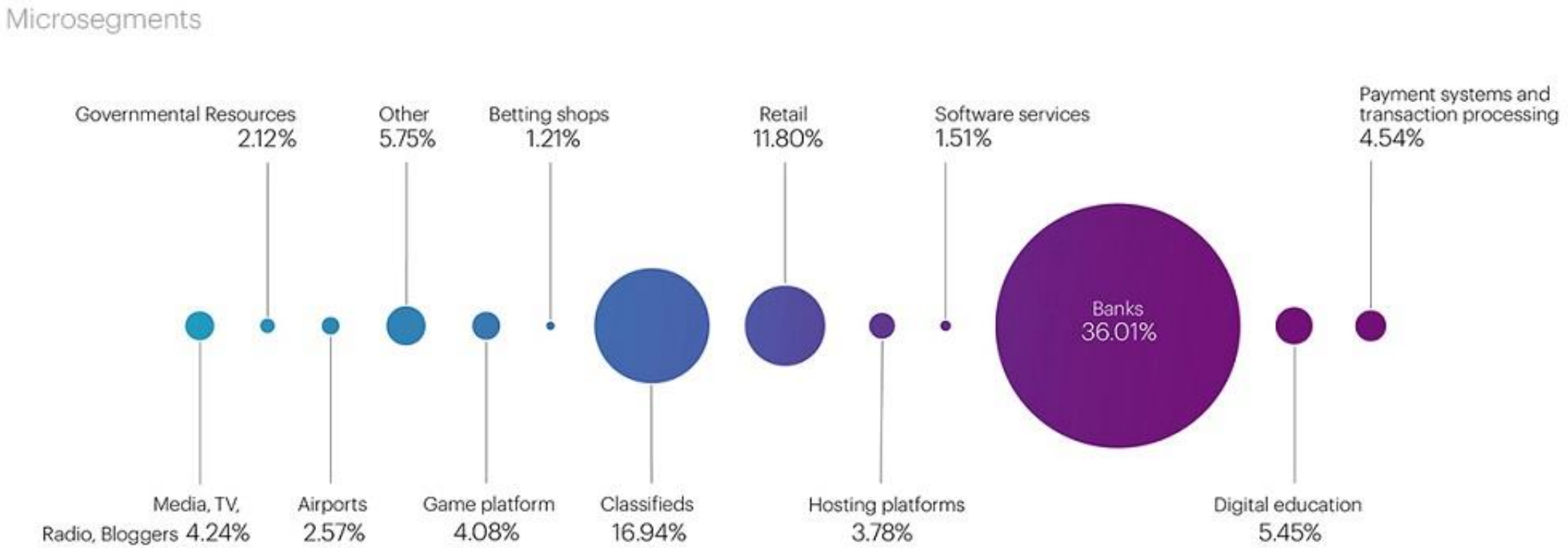
Динамика атак поквартально

Начиная с 2020 года



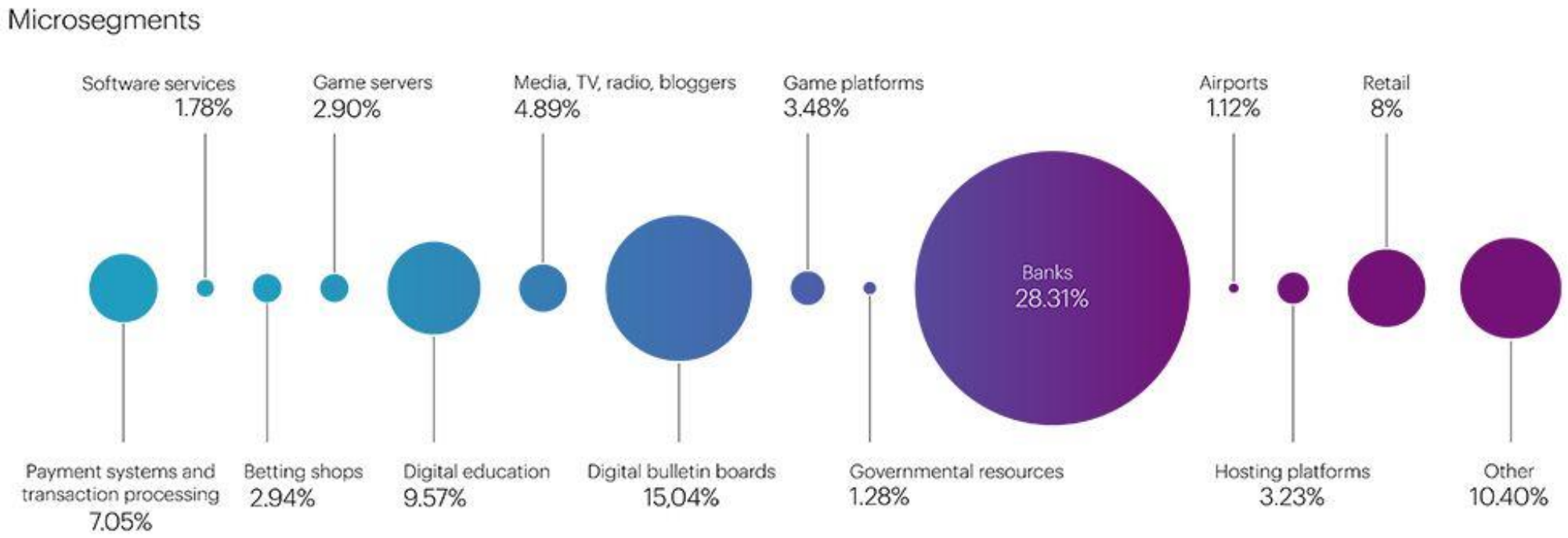
Распределение атак по индустриям

Q3 2023

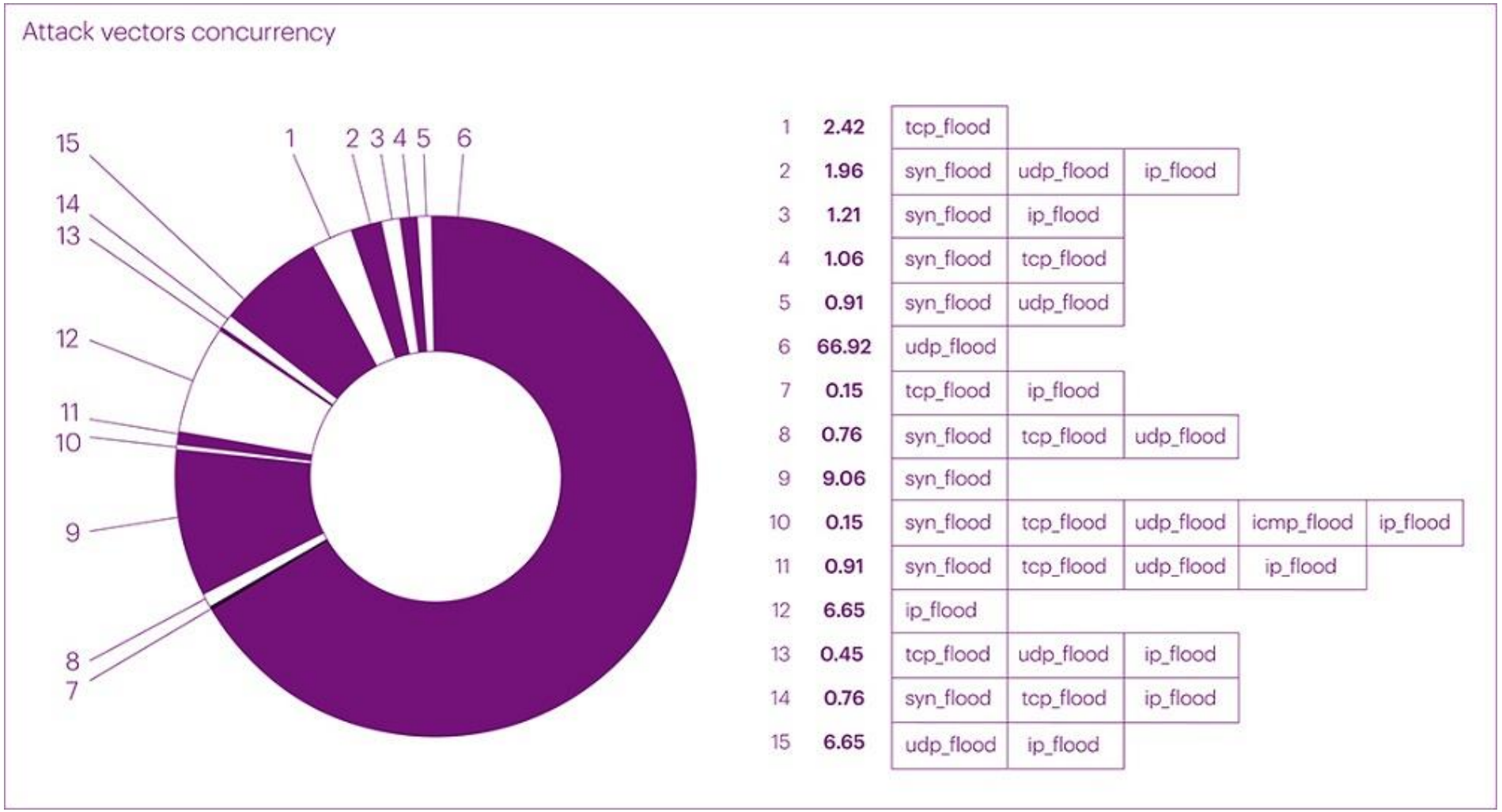


Распределение атак по индустриям

Q4 2023



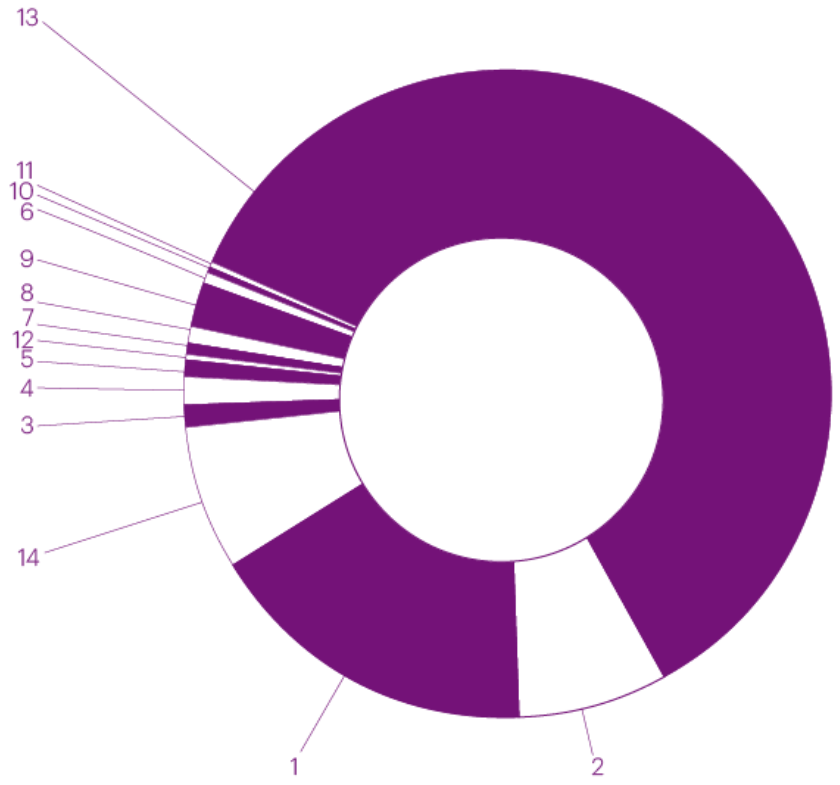
Векторы атак по типу – Q3 2023



1	2.42	tcp_flood				
2	1.96	syn_flood	udp_flood	ip_flood		
3	1.21	syn_flood	ip_flood			
4	1.06	syn_flood	tcp_flood			
5	0.91	syn_flood	udp_flood			
6	66.92	udp_flood				
7	0.15	tcp_flood	ip_flood			
8	0.76	syn_flood	tcp_flood	udp_flood		
9	9.06	syn_flood				
10	0.15	syn_flood	tcp_flood	udp_flood	icmp_flood	ip_flood
11	0.91	syn_flood	tcp_flood	udp_flood	ip_flood	
12	6.65	ip_flood				
13	0.45	tcp_flood	udp_flood	ip_flood		
14	0.76	syn_flood	tcp_flood	ip_flood		
15	6.65	udp_flood	ip_flood			

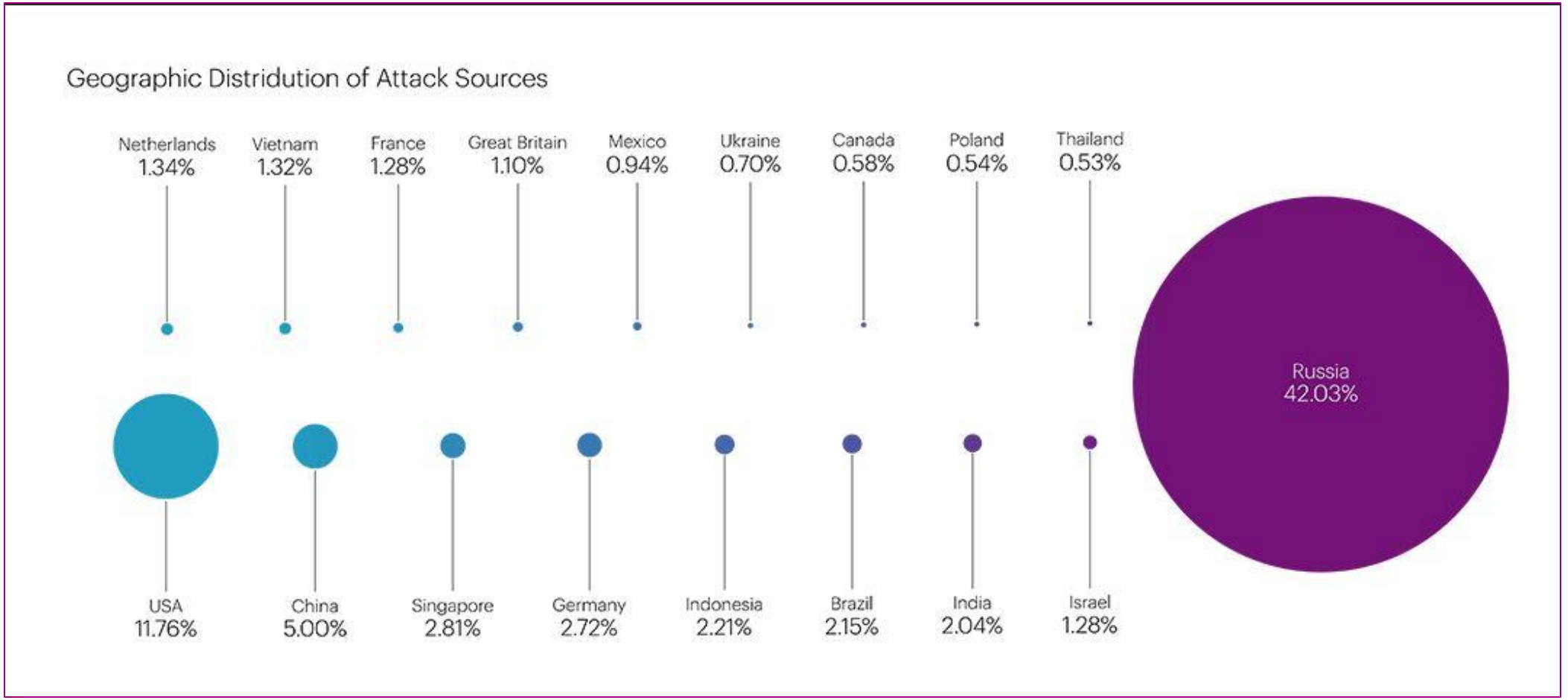
Векторы атак по типу – Q4 2023

Attack vectors concurrency



1	**16,86**	ip_flood			
2	**7,25**	syn_flood			
3	**0,98**	syn_flood	ip_flood		
4	**1,37**	syn_flood	tcp_flood		
5	**0,78**	syn_flood	tcp_flood	ip_flood	
6	**0,39**	syn_flood	tcp_flood	udp_flood	
7	**0,59**	syn_flood	tcp_flood	udp_flood	ip_flood
8	**0,78**	syn_flood	udp_flood	ip_flood	
9	**2,35**	tcp_flood			
10	**0,39**	tcp_flood	ip_flood		
11	**0,39**	tcp_flood	udp_flood		
12	**0,2**	tcp_flood	udp_flood	ip_flood	
13	**60,2**	udp_flood			
14	**7,45**	udp_flood	ip_flood		

География источников атак

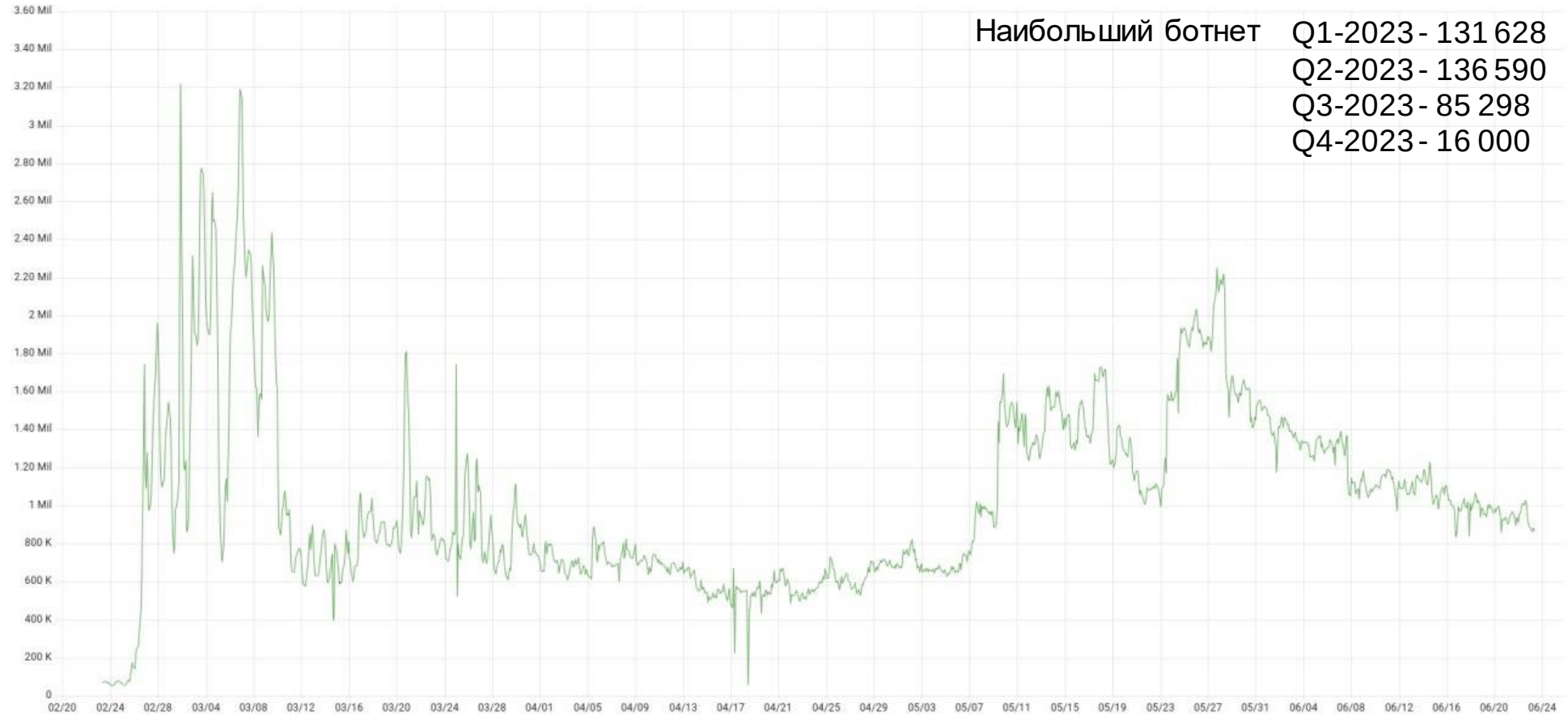


DDoS-атаки прикладного уровня, L7

Хактивизм — цифровое выражение социального протеста: дешево и не преследуется законом

- Повышение спроса на решение для защиты от ботов (Qrator Bot Protection)
- Поскольку хактивизм — DDoS-атаки часто идут в паре с попытками взлома которое требует подключения WAF

Если говорить про интенсивность атак L7 — то это размер черного списка

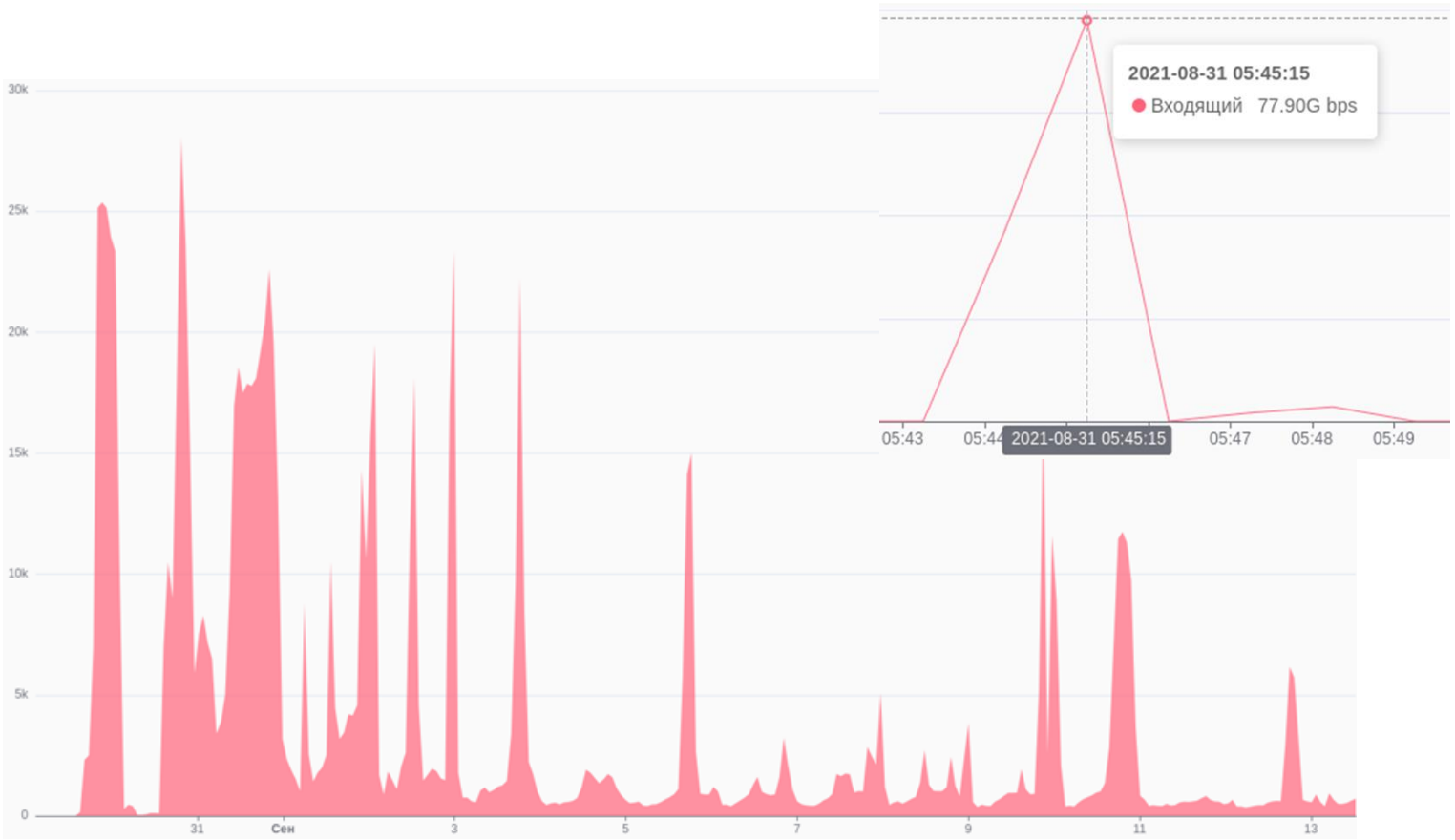


Наибольший ботнет
Q1-2023 - 131 628
Q2-2023 - 136 590
Q3-2023 - 85 298
Q4-2023 - 16 000

ИСТОРИИ ЗАЩИТЫ КОМПАНИЙ ОТ DDOS-АТАК

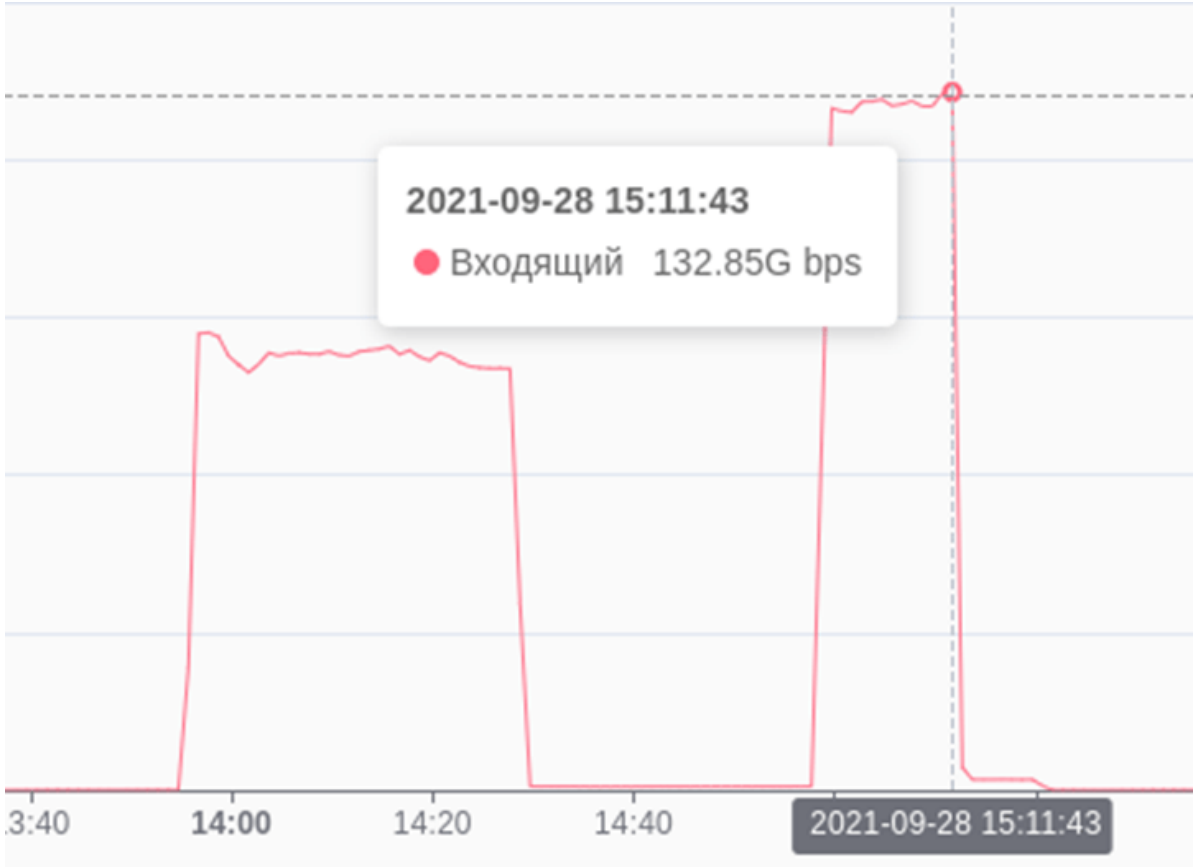
Как мы защищали "Тануки" от DDoS-атак "Мужского государства"

- С 29 августа по 13 сентября список заблокированных IP-адресов 15 раз превышал порог в 5 тысяч
- Не менее семи раз были предприняты попытки исчерпать канальную емкость атаками с амплификацией, самая мощная из которых составила более 77,9 Гбит/с
- 28 сентября произошла самая интенсивная атака за всё время «интернет-войны». Атака длилась 260 минут, во время неё было заблокировано 33,7 тысячи адресов, а интенсивность входящего трафика составила 132,85 Гбит/с в пике.



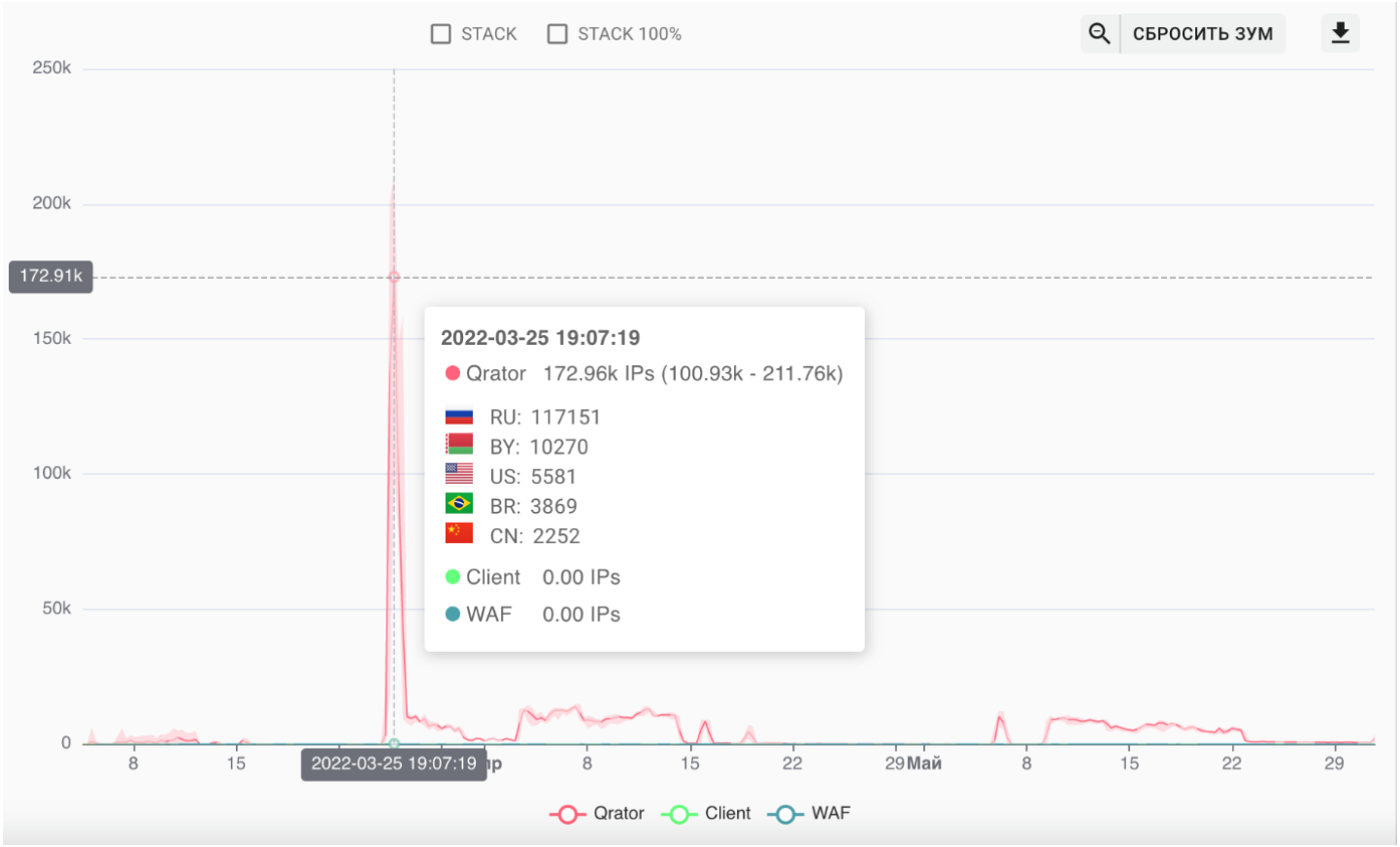
Как мы защищали "Тануки" от DDoS-атак "Мужского государства"

28 сентября произошла самая интенсивная атака за всё время «интернет-войны». Атака длилась 260 минут, во время неё было заблокировано 33,7 тысячи адресов, а интенсивность входящего трафика составила 132,85 Гбит/с в пике.



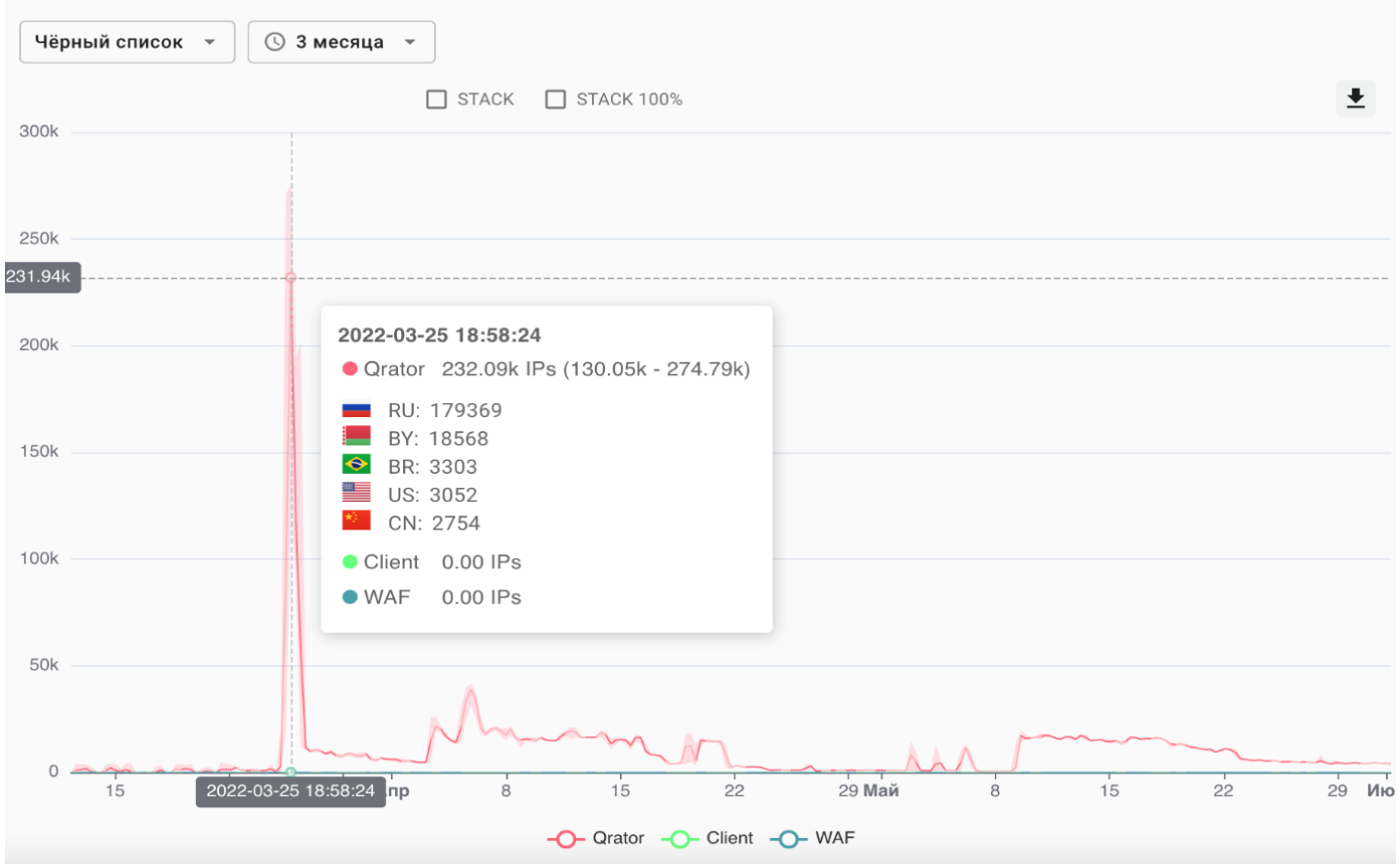
Атака на СДЭК

- С 5 марта атаки на уровне приложения (L7) на различные веб-ресурсы СДЭК фиксировались практически непрерывно.
- Пик наблюдался 25 марта, когда в ходе нападения было заблокировано почти 173 000 IP-адресов.
- Атака продолжалась вплоть до 19 апреля, но не увенчалась успехом



Атака на СДЭК

- В тот же период были зафиксированы атаки на на СДЭК Marketing, в пике более 230 000 адресов в черном списке.
- Большинство атак относится к проявлению так называемого хактивизма.
- Призывы атаковать ресурсы оператора были много раз замечены в различных пабликах и Телеграм-каналах.



О КОМПАНИИ QRATOR LABS

Сеть Qrator Labs

Преимущества и возможности

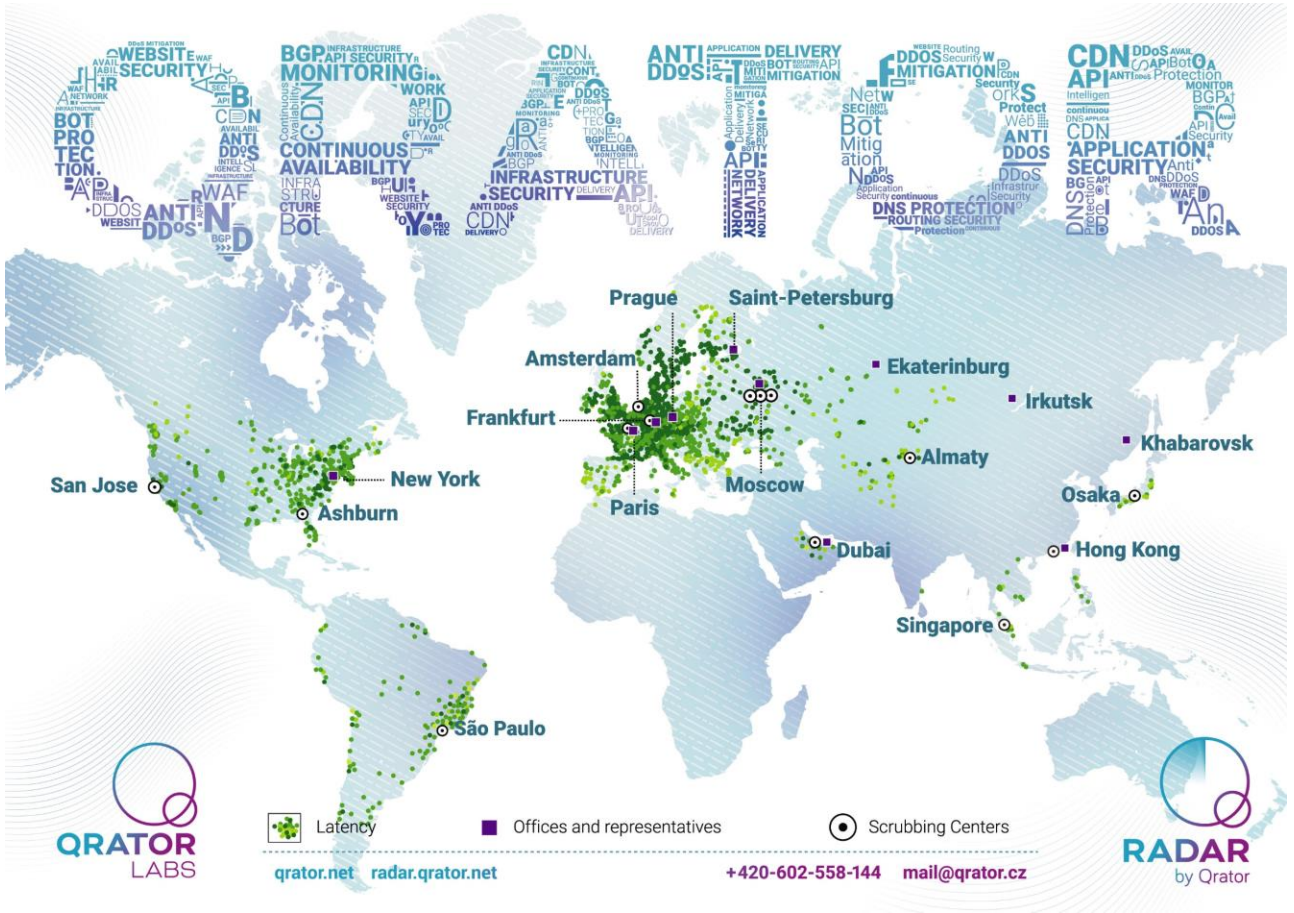
Более 15 центров очистки в мире
(на карте — «Scrubbing Centers»)
обеспечивают отличное покрытие
и связность

Прямая связь
с магистральными
провайдерами (Tier-1 ISPs)

Пропускная
способность сети —
свыше 4 Tb/s

Непрерывная
автоматическая фильтрация
трафика

Ответ на атаку: в среднем
менее 1 сек. При самом
сложном случае —
max. 3 мин.



Qrator.Anti-DDoS

Преимущества и возможности

- Нейтрализация атак на всех уровнях OSI, включая L7 (приложение)
- Уникальная платформа BGP- Anycast: надёжный, георасределённый отказоустойчивый сервис:

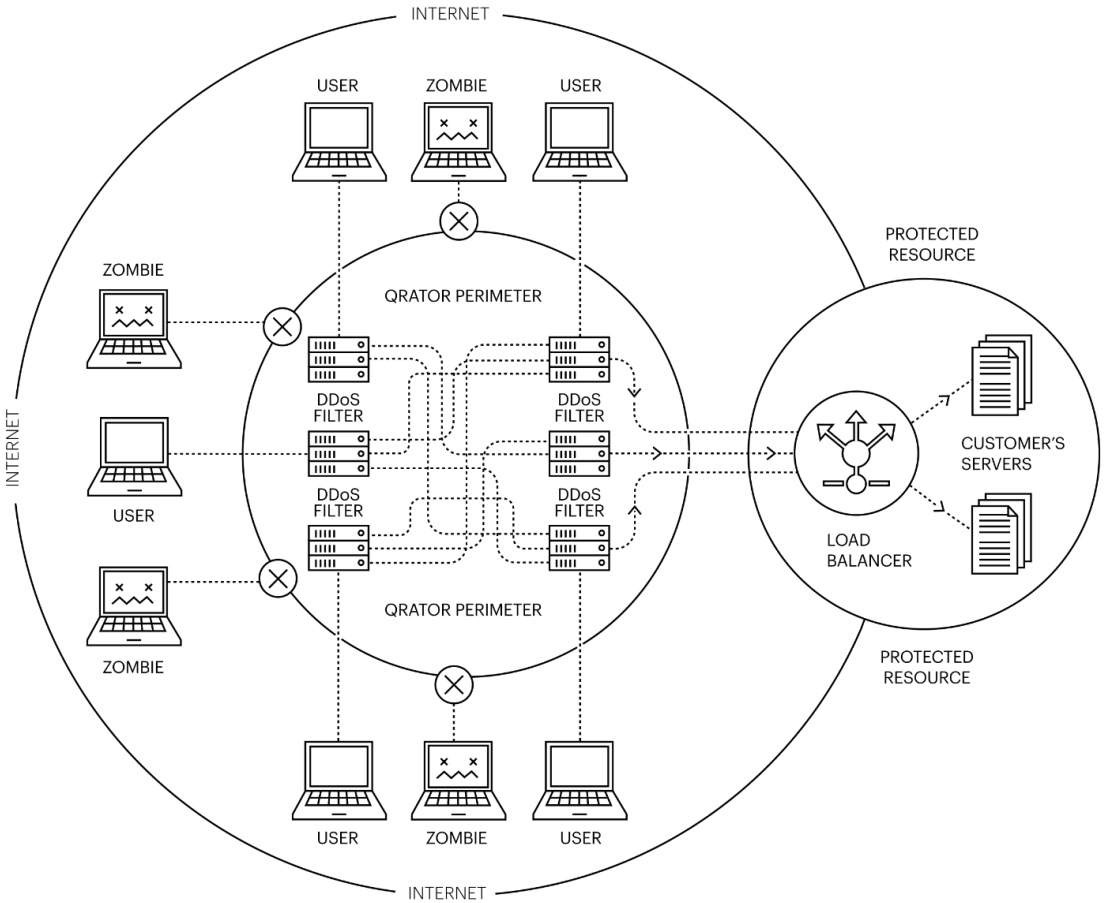
Подходит для мобильных приложений и API

Не используются технологии вроде CAPTCHA

Возможность настройки WAF в зависимости от нужд клиентов

Простая интеграция с приложением backend

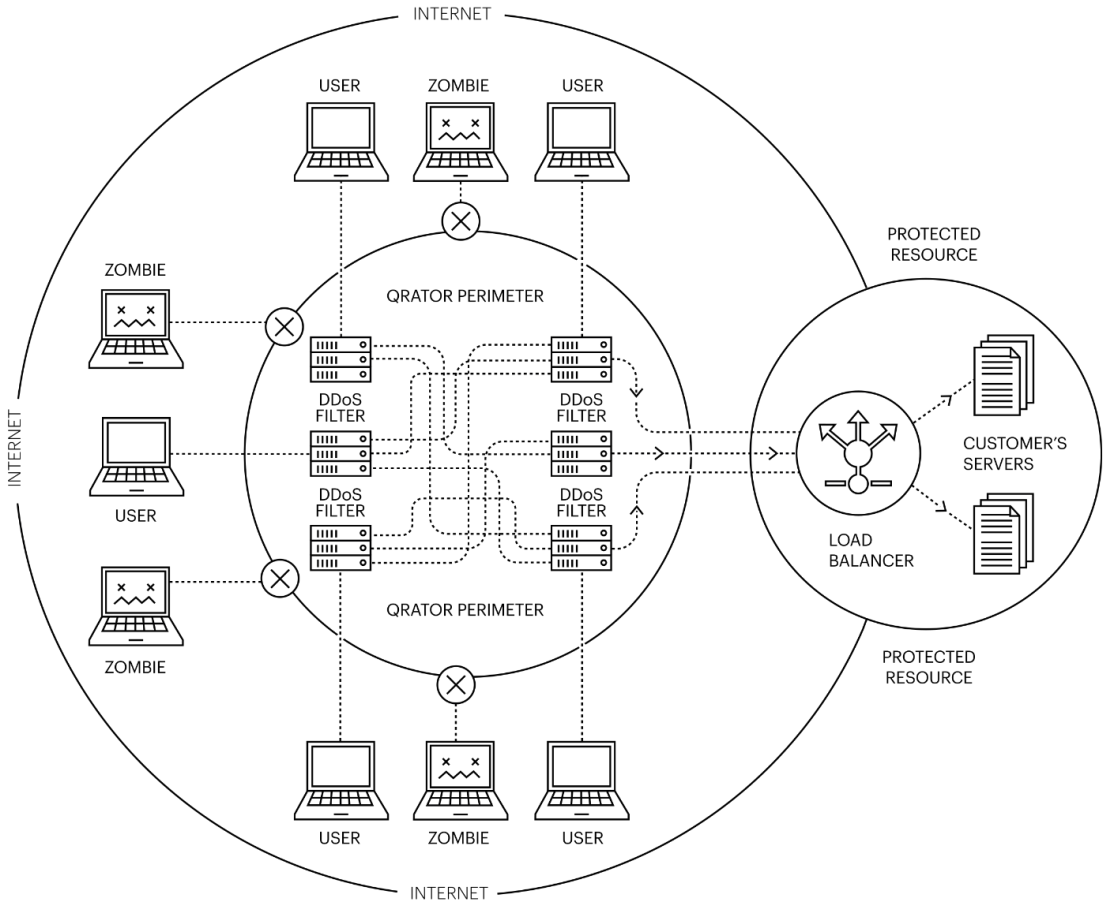
Qrator Bot Protection — для борьбы с парсерами и Брут-форс



Qrator.Anti-DDoS

Преимущества и возможности

- Фильтрация HTTPS трафика без раскрытия ключей шифрования, до L7 включительно
- Профессионалы техподдержки — 24/7 по всем каналам связи для всех часовых поясов мира
- Готовы нейтрализовать атаки «0-day»
- Встроенный мониторинг приложений
- Минимальное количество ложных срабатываний: 0% в спокойном режиме, во время атаки — не превышает 5%
- SLA до 99,95% - прописанный и гарантированный договором: Клиент не платит, если услуга не соответствует заявленному качеству

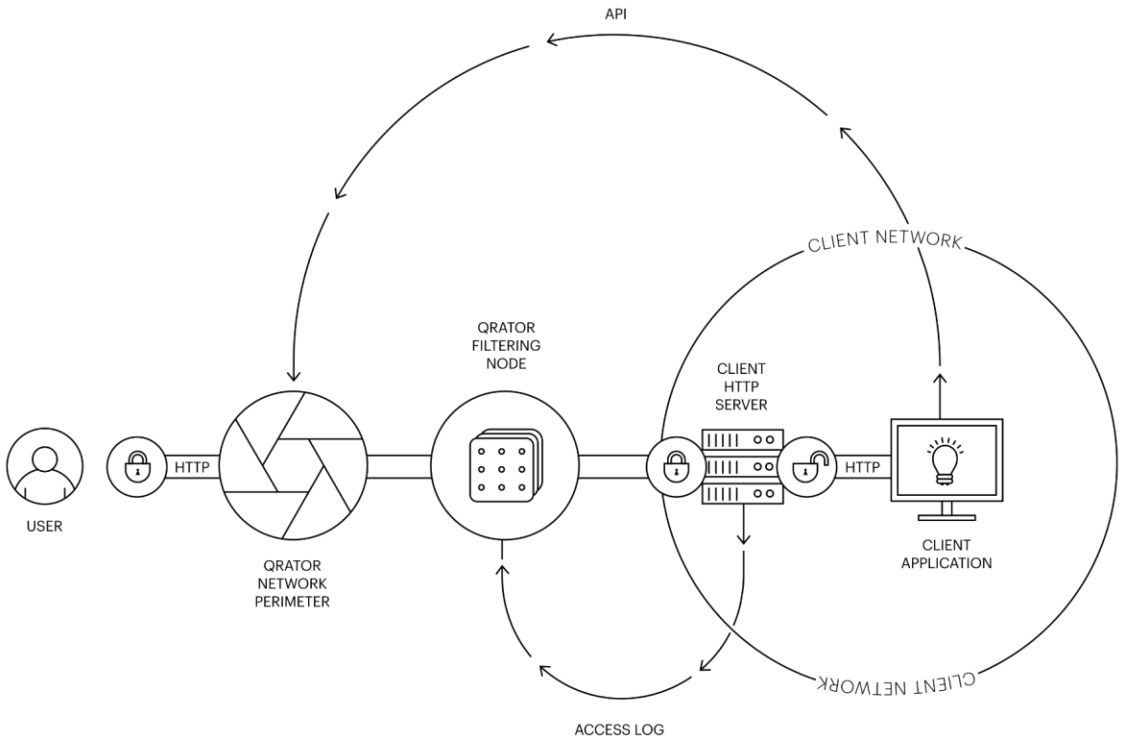


АНАЛИЗ ТРАФФИКА
БЕЗ РАСШИФРОВКИ SSL ТРАФИКА

Qrator.Anti-DDoS

Фильтрация HTTPS трафика без раскрытия ключей шифрования

- Полная конфиденциальность данных, проходящих через сеть Qrator Labs без нарушения политик безопасности заказчика
- Легитимный трафик передается на защищаемый сервер без дешифрования и без изменений, используются следующие технологии:

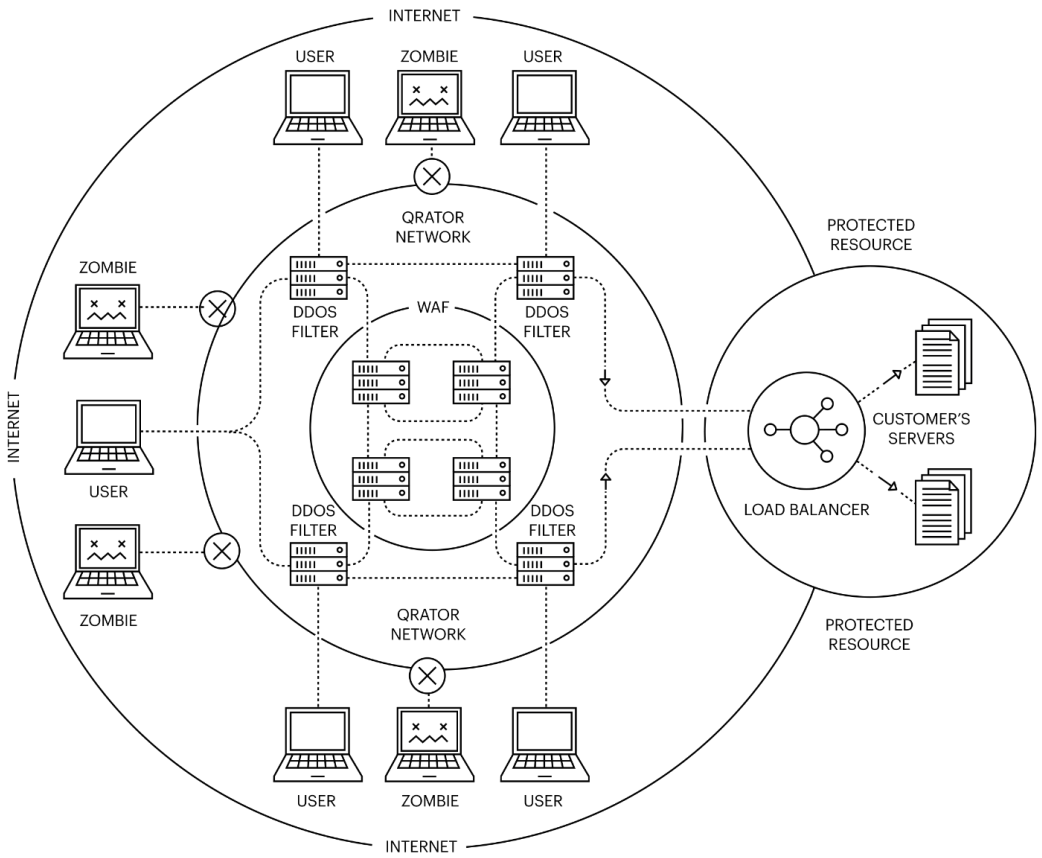


QLOG: Клиент может предоставлять в Qrator Labs журнал доступа защищаемого приложения в реальном времени посредством стандартного протокола syslog. Qrator Labs на основе алгоритмов поведенческого анализа будет автоматически формировать Белые и Черные списки

QRATOR.WAF

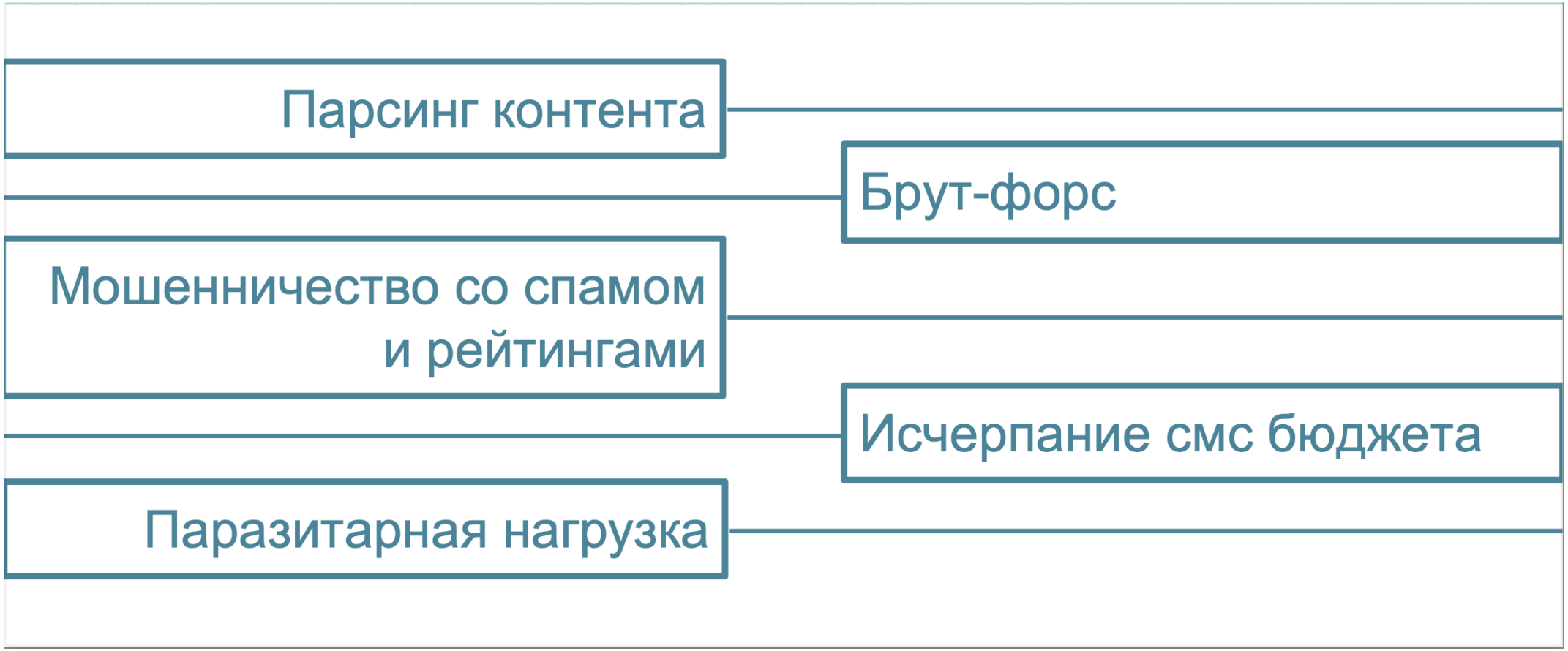
QRATOR.WAF

- Распределенное **облачное решение**;
- **Высокий уровень защиты** как от широко распространенных простых видов атак, так и от сложных направленных воздействий;
- Эффективный **механизм раннего подавления ложных срабатываний**;
- Уникальные **функции по анализу бизнес-логики** и действий пользователей;
- **Различные исполнения и тарифные планы** для обеспечения оптимальной стоимости владения;
- Максимально **широкий набор сценариев использования** среди аналогичных решений;
- **Гибкая настройка** с учетом особенностей защищаемых приложений;
- **Работа в режиме блокировки** с минимальным уровнем ложных срабатываний;
- **Соответствие требованиям** информационной безопасности.



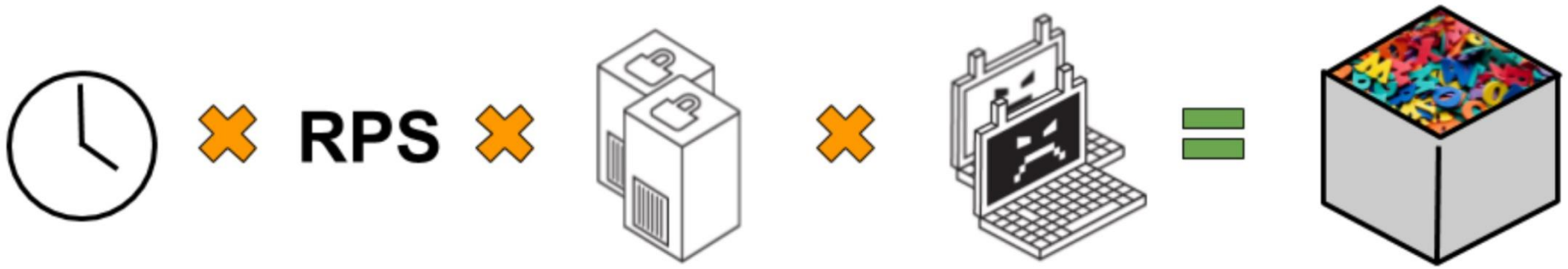
QRATOR BOT PROTECTION

Qrator Bot Protection



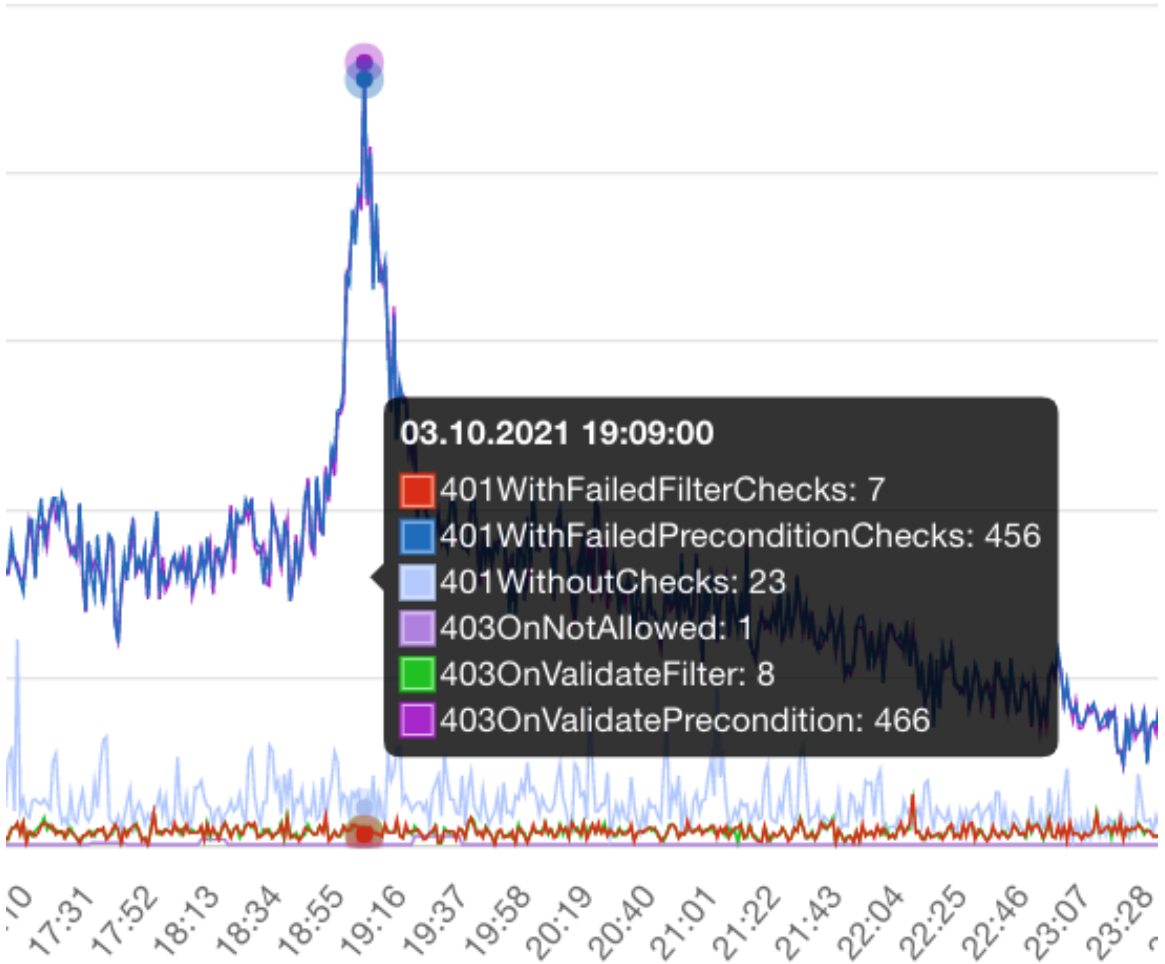
Qrator Bot Protection

Арифметика скрэпинга



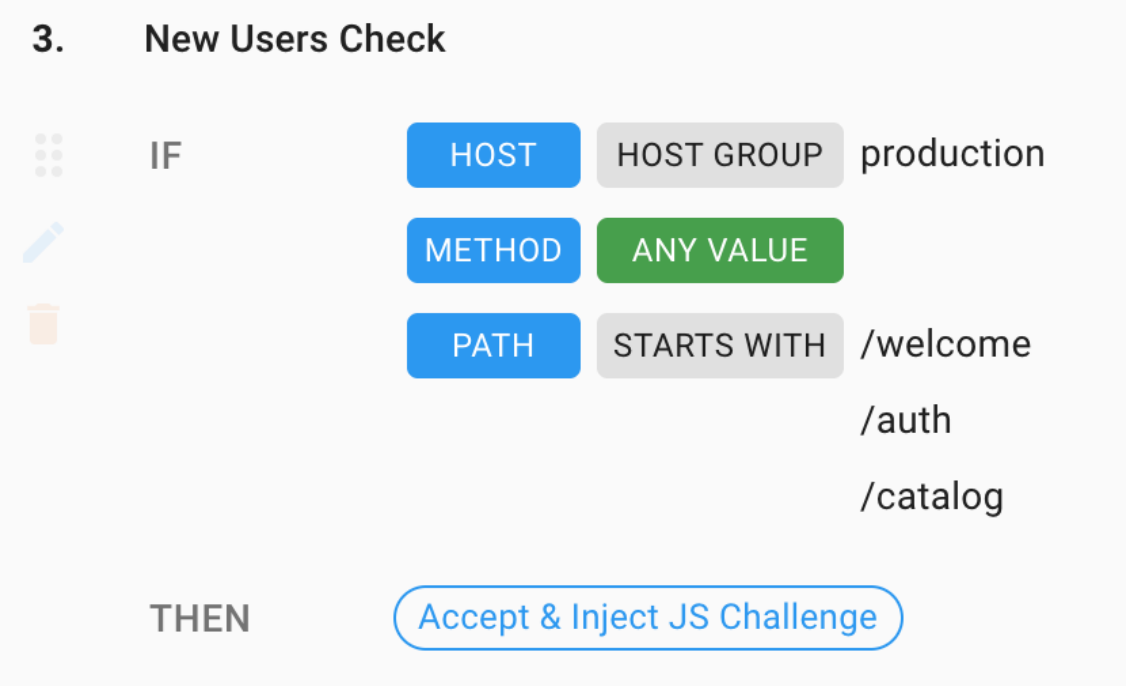
Qrator Bot Protection

- Немедленное обнаружение и устранение вредоносных ботов
- Блокировка ботов с первого запроса
- Никаких страниц ожидания и CAPTCHA
- Легкий, с низкими накладными расходами, прозрачный подход
- Возможность интеграции с мобильными приложениями

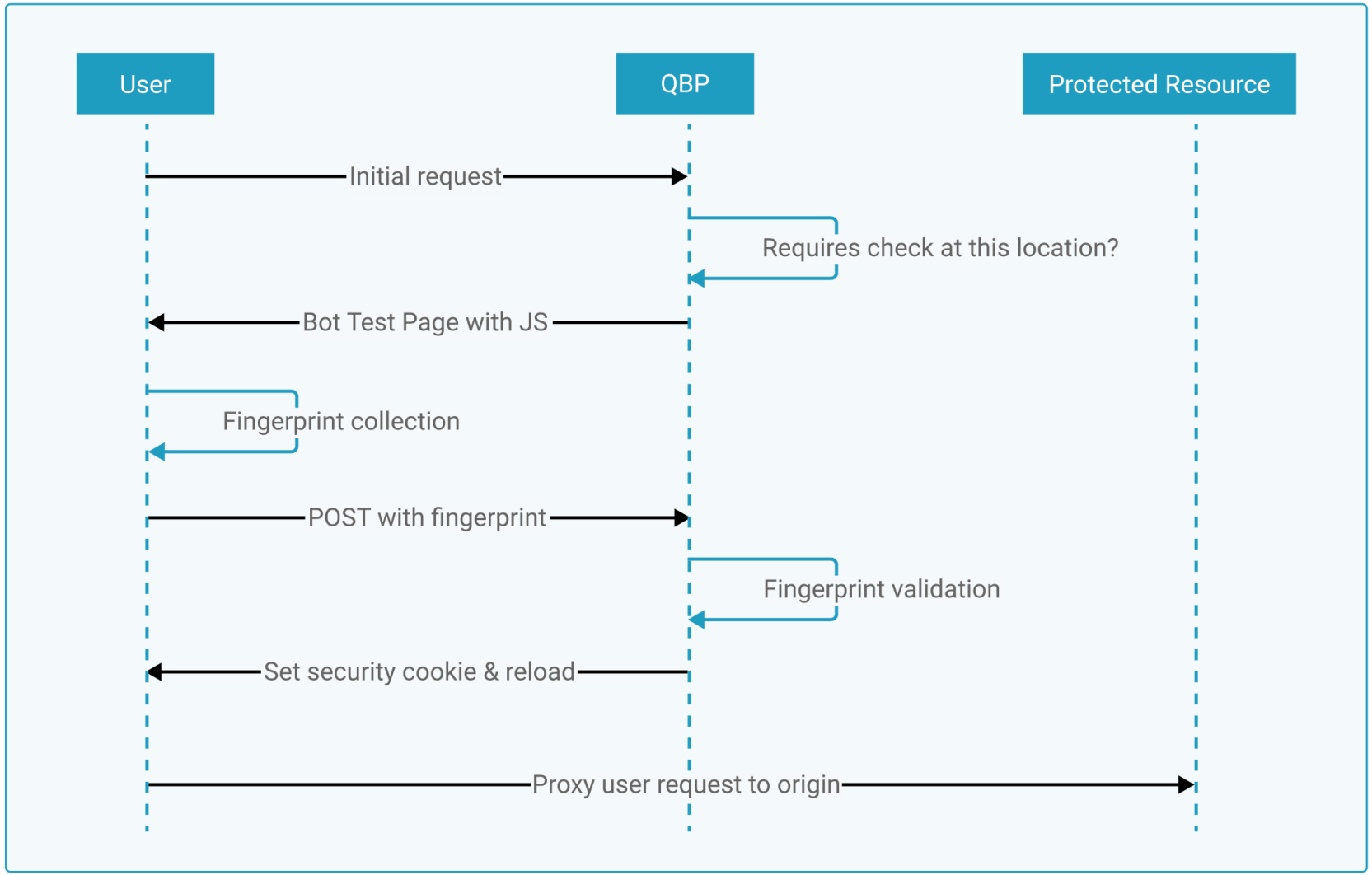


Qrator Bot Protection

- Фингерпринтинг устройства
- Обнаружение несанкционированного доступа
- Проверка браузера на основе JS
- Анализ репутации пользователей
- Поведенческий анализ



Qrator Bot Protection



Qrator Bot Protection