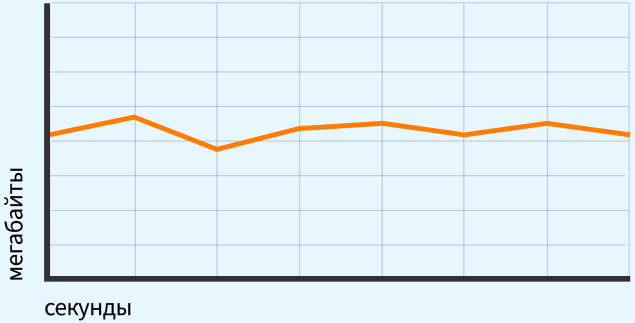
Будь готов!
Несколько примеров
Реальных атак

30

провайдеров опрашивает агентство, чтобы найти нужный билет

60

раз в секунду агентство опрашивает провайдеров



до 5мб

может занимать ответ провайдера

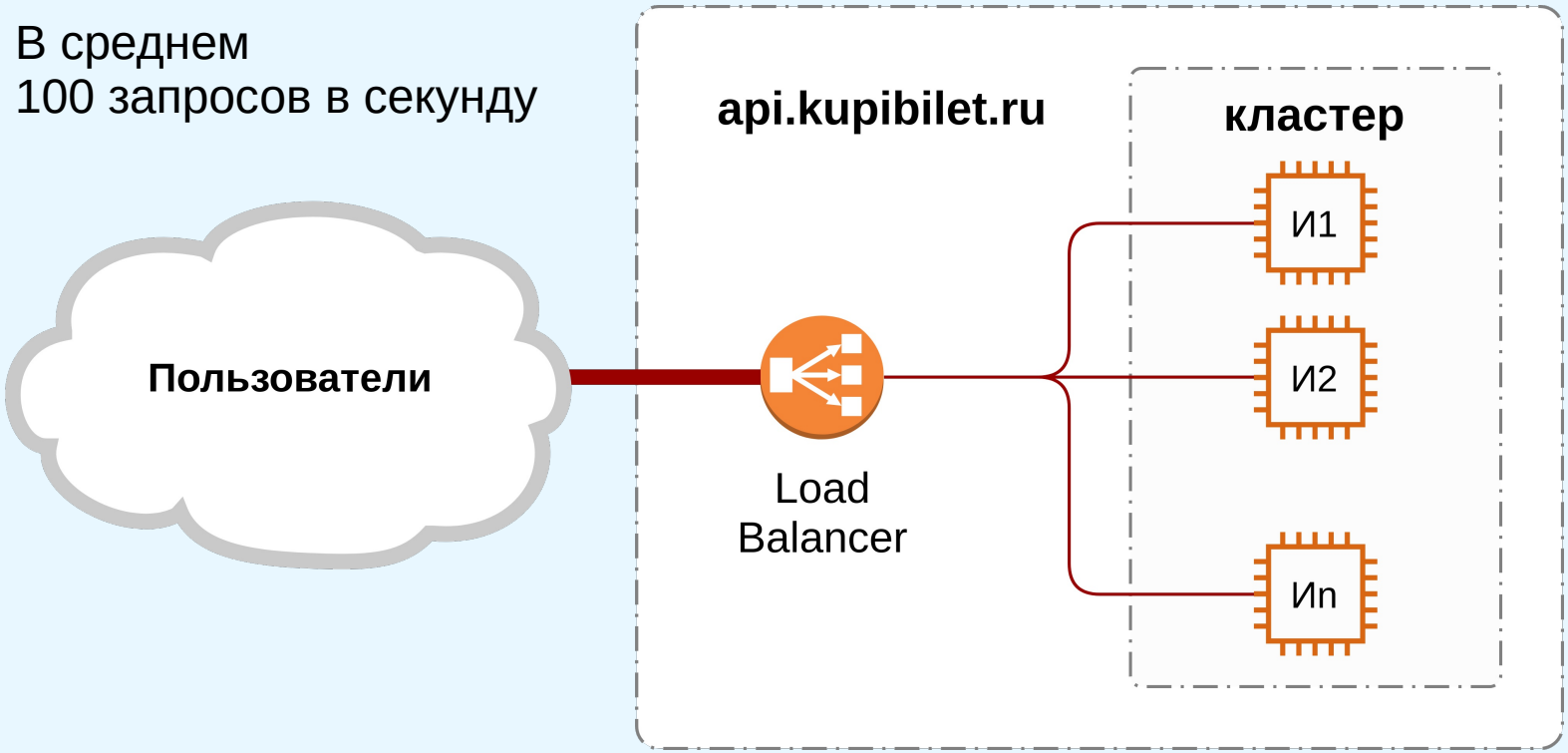
Смарт маршруты – это

- более 700 авиакомпаний
- 100 млрд. билетов
- на 30% дешевле
- выдача за 2 сек.

Что защищаем

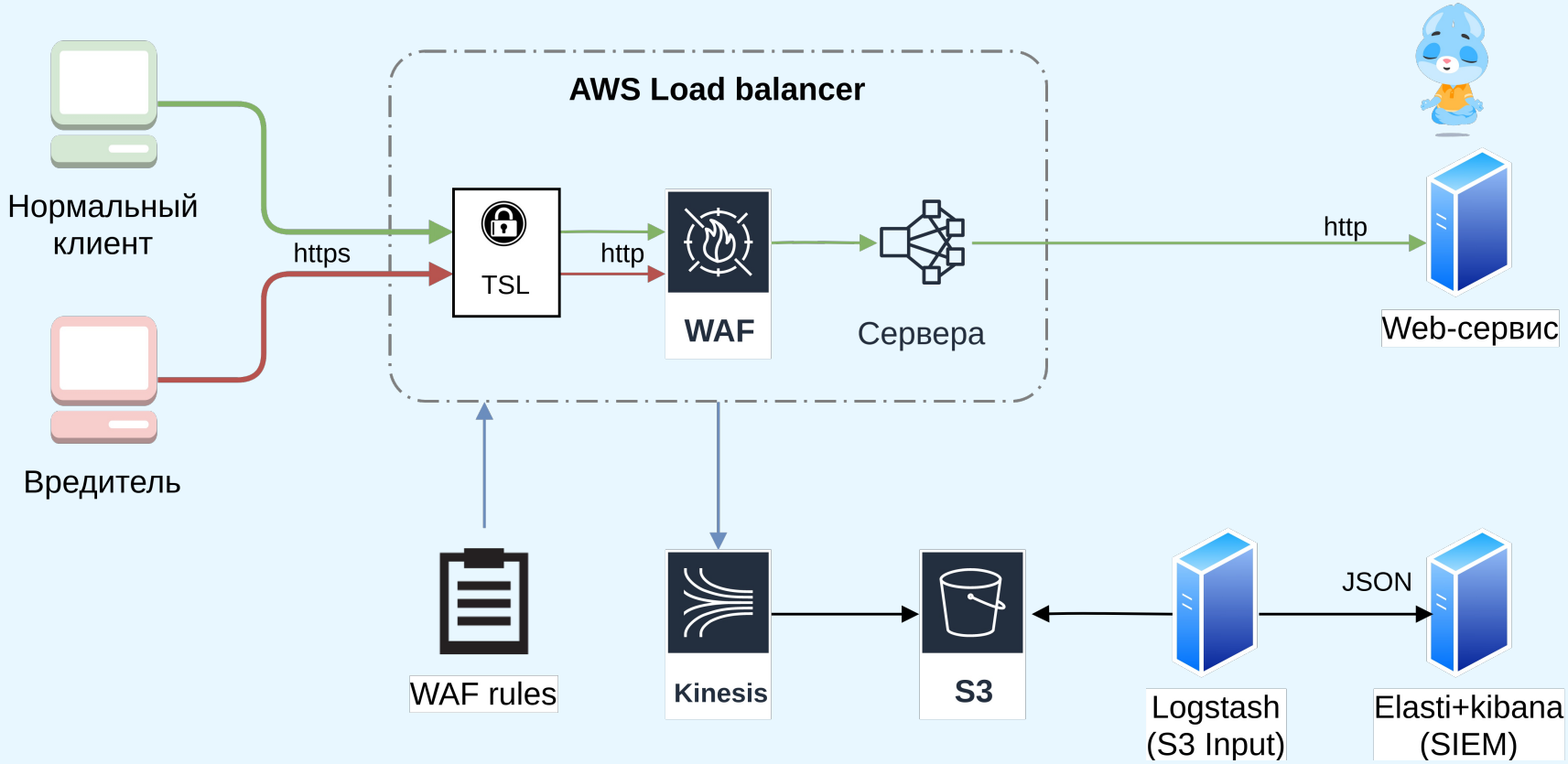
KUPIBILET

В среднем
100 запросов в секунду



Архитектура

KUPIBILET



Пример 1. Описание

Первая атака, зафиксированная
после включения WAF:

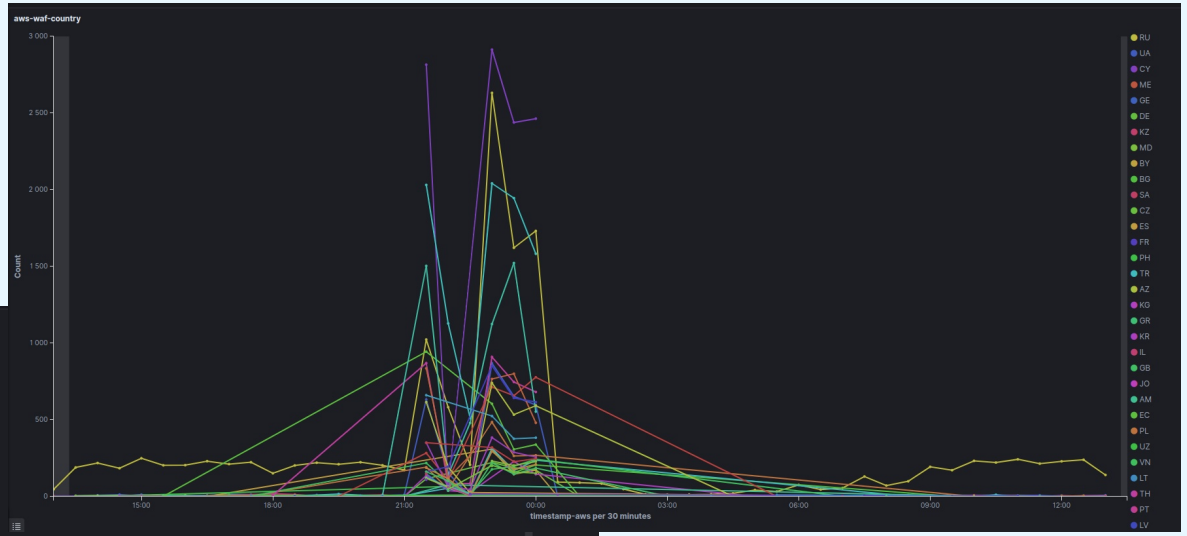
Брут с отправкой максимально возможного количества запросов с каждого атакующего устройства.

Во время атаки WAF только фиксировал происходящее.

Пример 1. На практике

KUPIBILET

Длительность: 4 часа



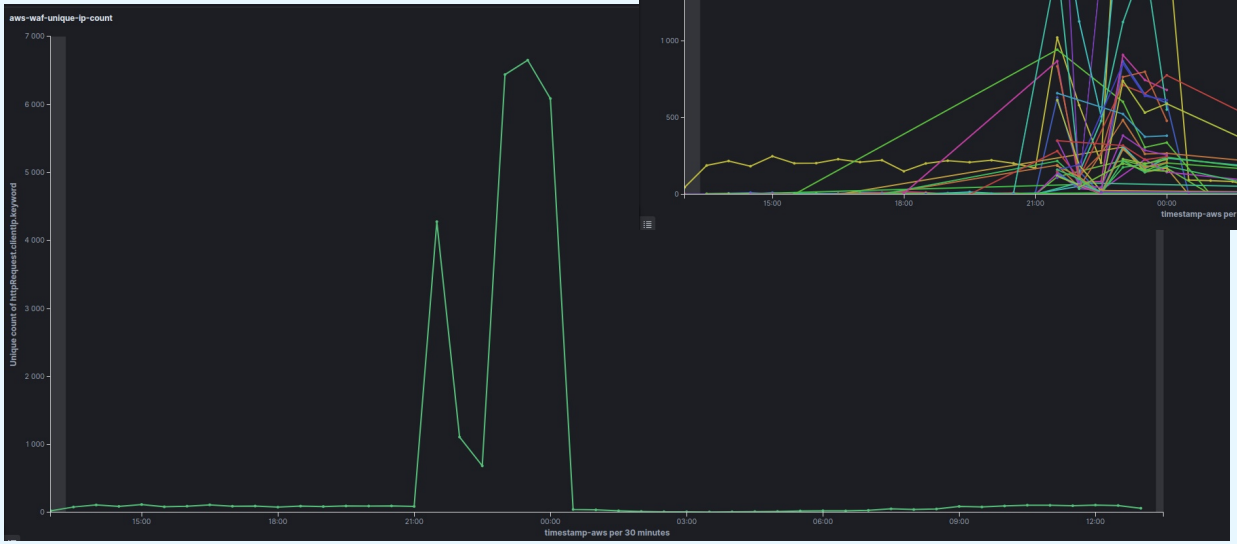


График отображает количество запросов к форме входа за 30 минут

Пример 2. Адаптация

Адаптация под лимиты.

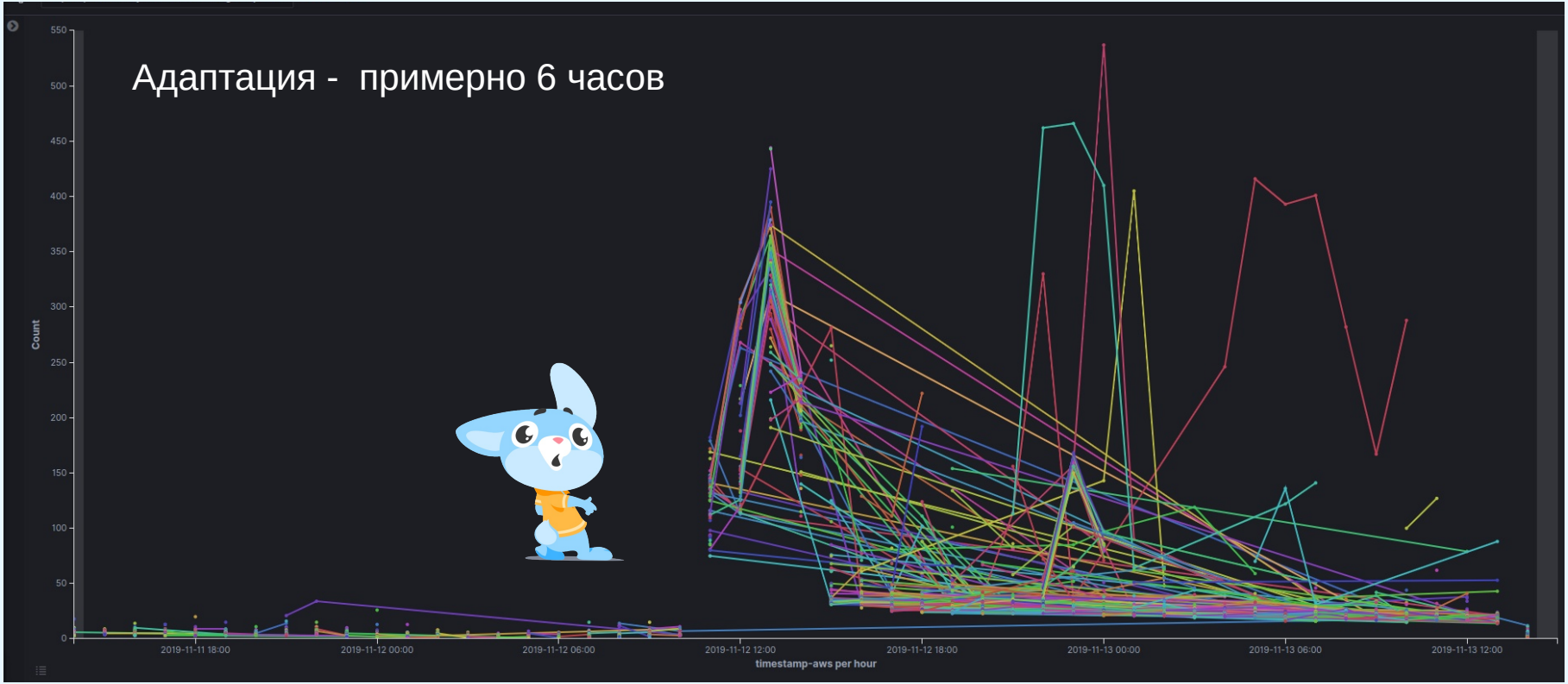
После первой атаки были активированы ограничения на количество запросов к форме входа.

Время адаптации атакующих к новым ограничениям — примерно **6 часов**

Пример 2. На практике

KUPIBILET

Лимит частотного правила: 200 запросов за 5 минут. Продолжительность: 24 часа



Пример 3. Боты

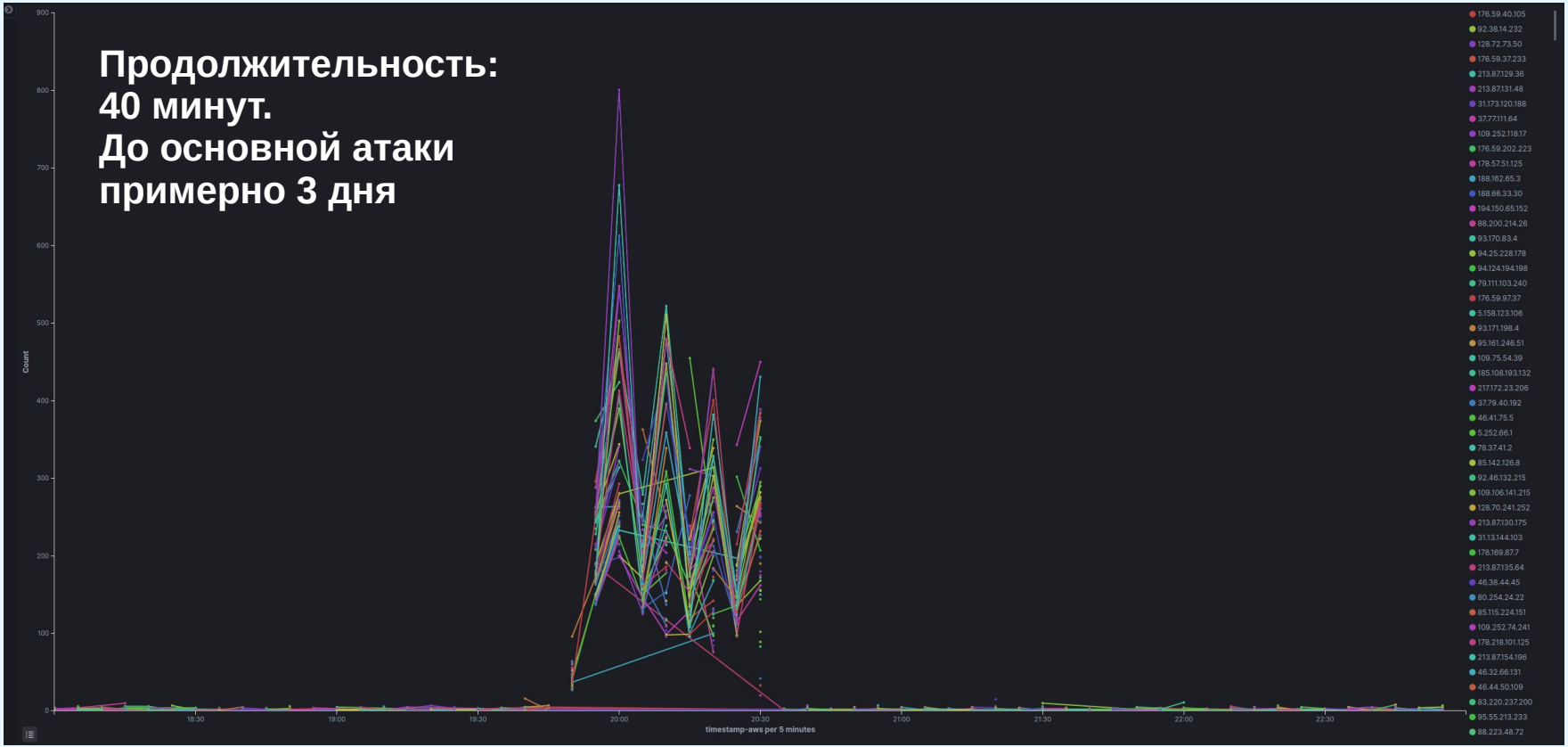
Моделирование поведения пользователя

Были существенно снижены лимиты количество обращений к форме входа. Теперь максимальное количество запросов равнялось удвоенному среднему количеству запросов.

Во время атаки количество обращений к форме входа не превышало среднее количество обращений с легитимного устройства.

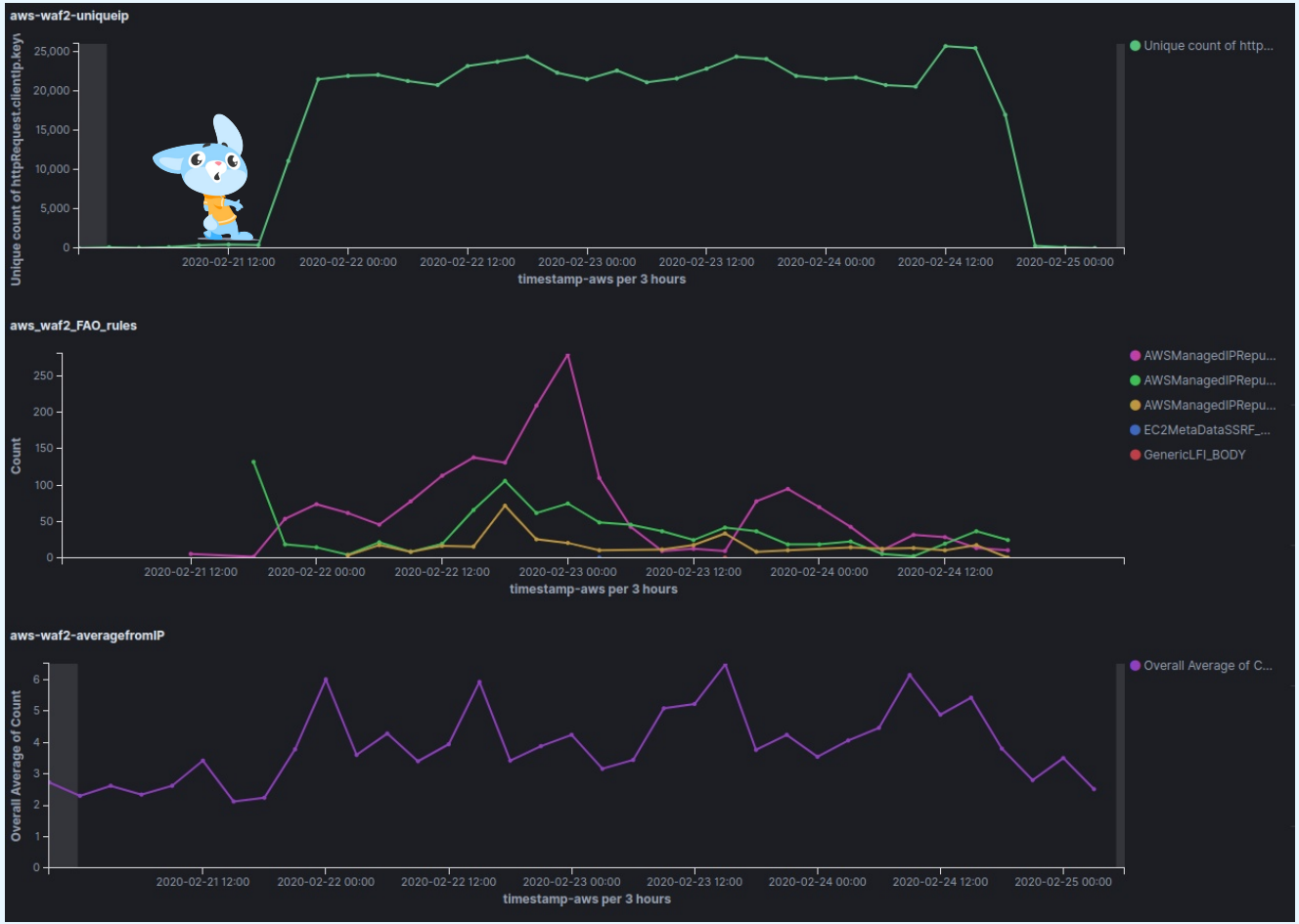
Пример 3. Разведка

KUPIBILET



Пример 3. Основная фаза атаки

KUPIBILET



Продолжительность: Примерно **3 дня.** Количество устройств увеличилось **в 50 раз**. Всего использовалось примерно **3 млн ботов**.

Репутационные правила **не сработали**, значит атака шла с живых устройств.

Среднее количество запросов с одного устройства **не изменилось**

Пример 4. Бесполезная полезная нагрузка

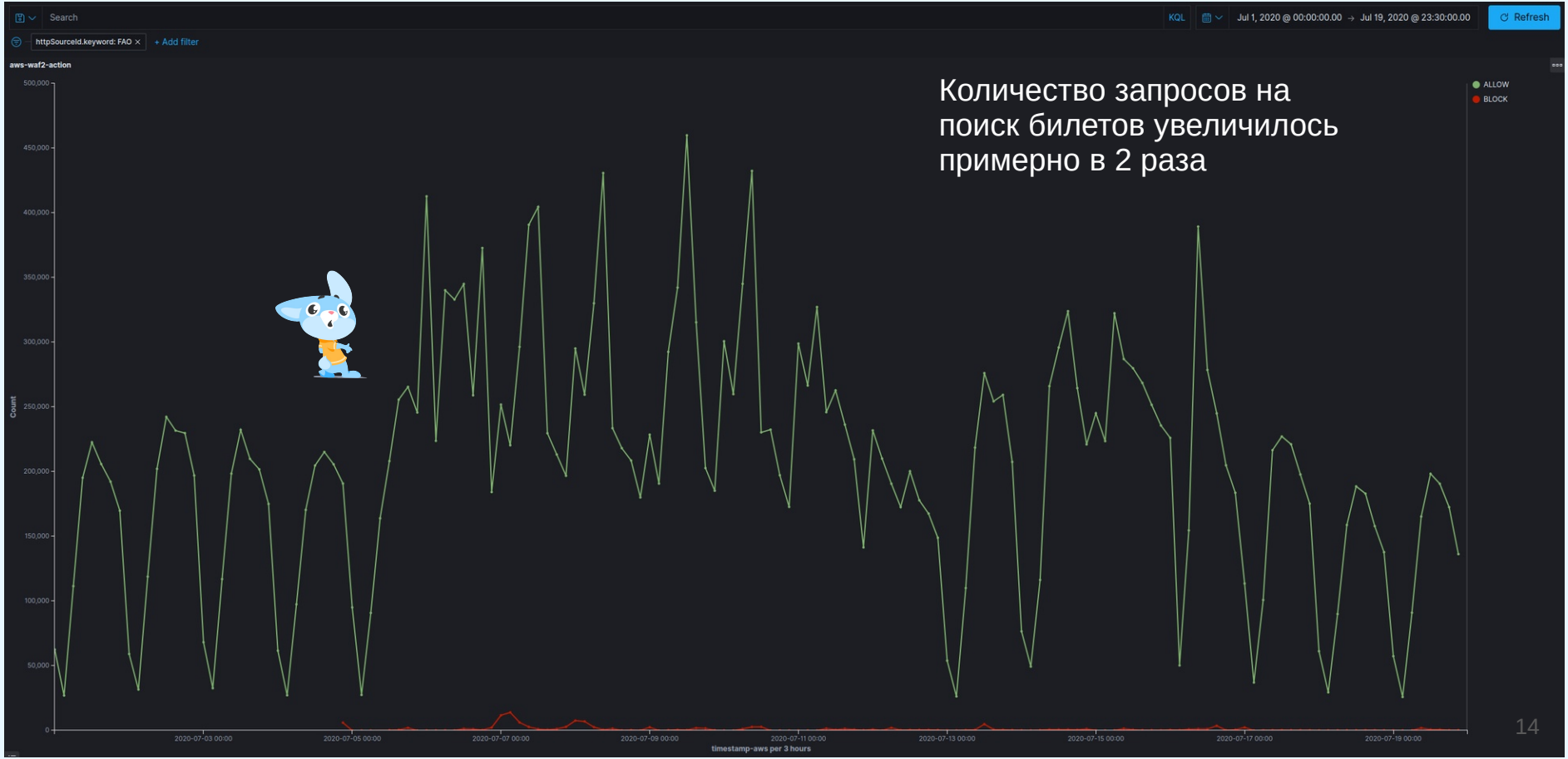
KUPIBILET

Для защиты от ботов нужно использовать системы, построенные на анализе поведения пользователей. Необходимо определить нормальное поведение пользователя вашего ресурса.
Пользователи, которые ведут себя нормально, пользуются сервисом без ограничений.
Остальные регулярно проверяются и блокируются.

Целью использования ботов могут быть не только аккаунты ваших пользователей, но и ваш контент.

Пример 4. На практике

KUPIBILET



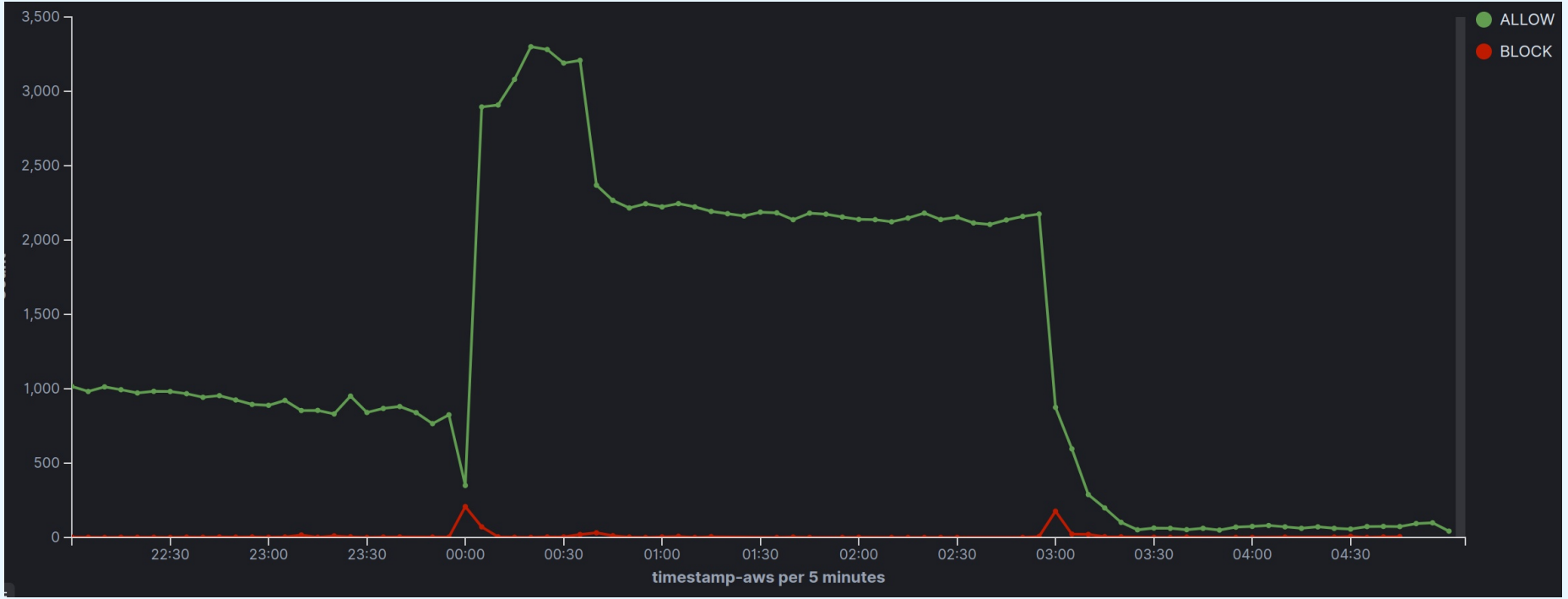
Количество запросов на поиск билетов увеличилось примерно в 2 раза

Пример 4. Поведение

KUPIBILET

Пример 4. Типовой сценарий

KUPIBILET



Пример 4. Итоги

Информация о билетах, с большой вероятностью, использовалась на различных фишинговых сайтах.

Ежемесячно детектируем от 1 до 5 фишинговых сайтов, которые пытаются использовать наш контент для обмана пользователей.

Результаты атаки:
Продолжительность — примерно 7 дней
Затраты на ресурсы — примерно $1000
Репутационный ущерб — заблокировали заблокировали поисковые запросы примерно 50 легитимных пользователей

Возможно, где-то кого-то обманули ...

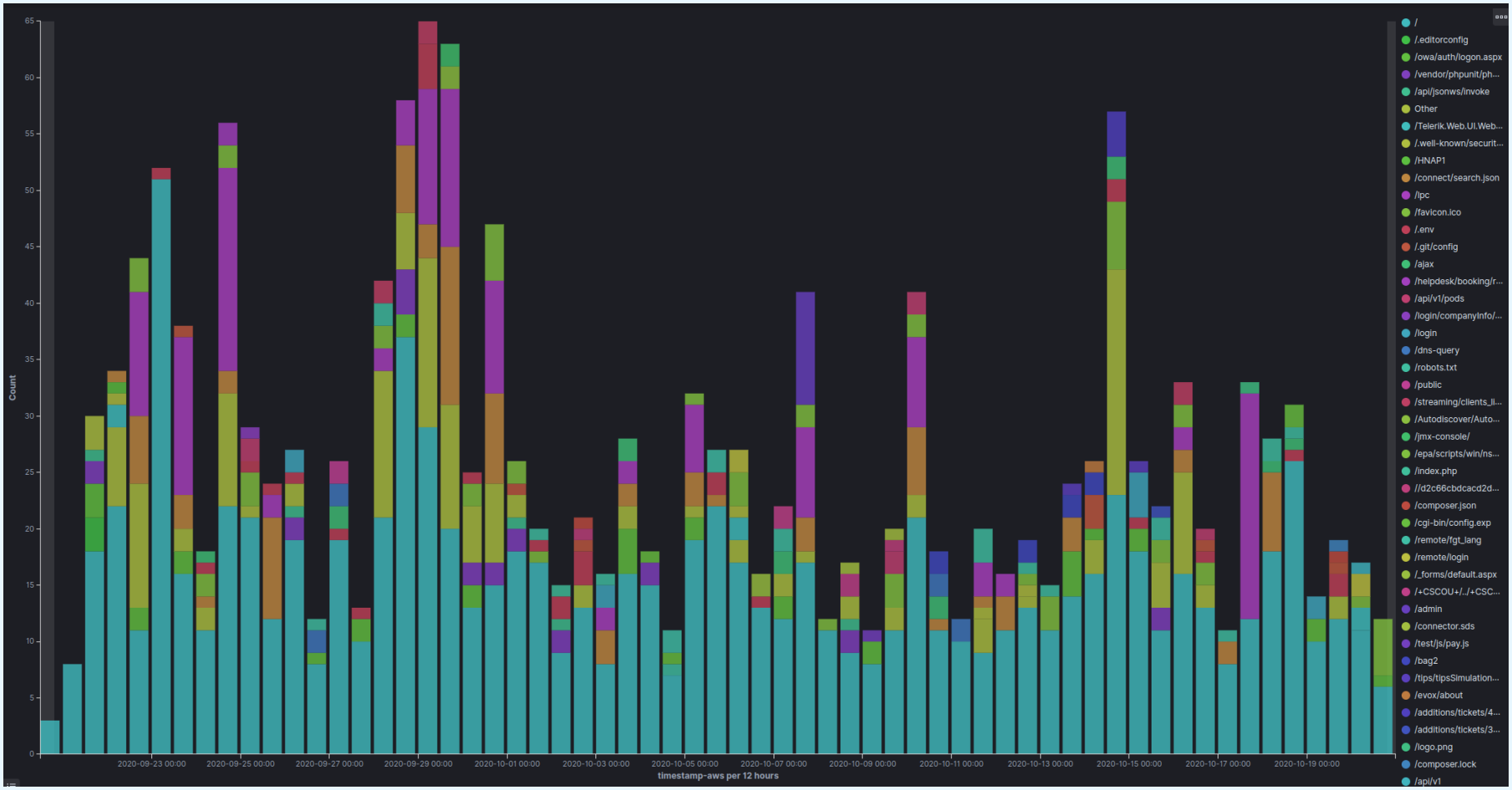
Пример 5. Фоновый шум

На примере ресурса, для которого определен белый список источников запросов и URI.

В среднем 2,5 запроса в час — бесполезная нагрузка от исследователей безопасности, которые пытаются выявить уязвимости.

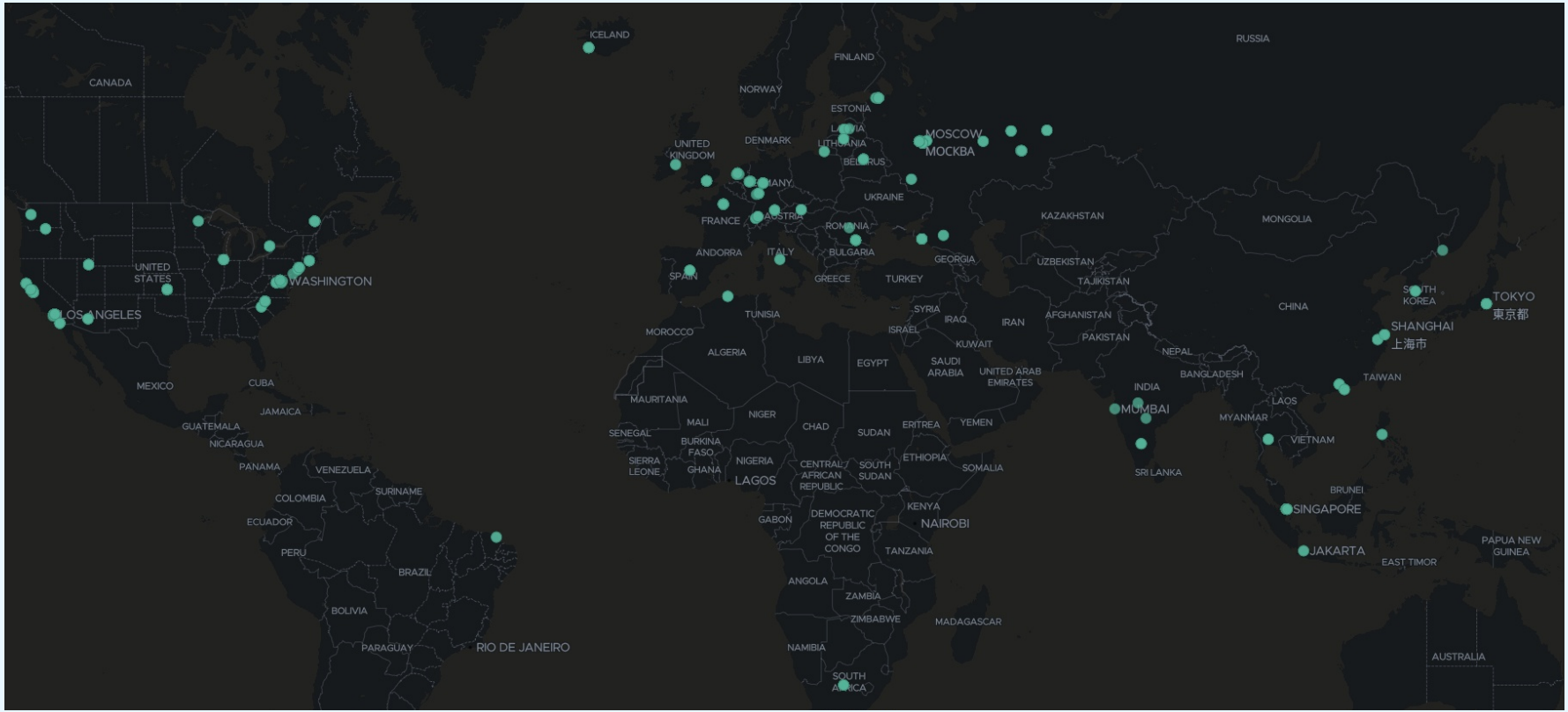
Пример 5. Фоновый шум

KUPIBILET



Пример 5. Источники

KUPIBILET



Выводы

1. Необходимо контролировать то, что происходит на вашем интернет-ресурсе.
2. Обработка каждого запроса требует определенных ресурсов.
3. Атакующие очень оперативно адаптируются к новым механизмам защиты.
4. Атакующие экономят свои ресурсы. Как только количество заблокированных запросов превышает некий определенный порог, атака прекращается (добавить пример).

Рекомендации

1. Используйте механизмы от типовых атак (OWASP Top10)
2. Ограничивайте максимальное количество запросов с одного устройства к определенному функционалу.
3. Анализируйте поведение пользователей и выявляйте аномалии.
4. Выполняйте проверку устройств, которые приходят на Ваш Интернет-Ресурс. Если устройство подозрительно, то необходимо выполнять дополнительные проверки пользователя.
5. Выявлять атаку следует по косвенным признакам, а блокировать по прямым (ip-адрес или некий секрет)
6. Для защиты от ботов можно использовать ловушки.

Важно помнить, что нет абсолютных механизмов защиты. Все применяемые меры направлены на увеличение стоимости атаки вашего ресурса.

Thank you

Беляков Игорь
Belyakov.Igor@kupibilet.ru
+7 921 3089713

KUPIBILET