Технические аспекты блокировки интернета в России. Проблемы и перспективы

Филипп Кулин (Дремучий лес)

v1.0.4

HighLoad++

Профессиональная конференция разработчиков высоконагруженных систем

Сплошной клубок проблем

- Сопутствующий ущерб
- Волатильность нормативов и практик
- Трудность диагностики
- Непредсказуемость
- Невозможность рассчитать риски
- Неприемлемое время обратной связи
- Безысходность

Группы риска

- Владельцы сайтов и сервисов
- Пользователи сервисов
- Хостеры и провайдеры

Начнем, пожалуй

Как это работает

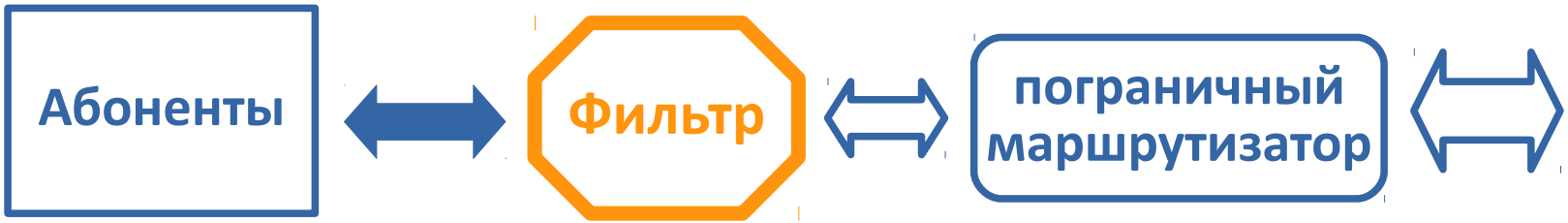
- Решение ФОИВ или суда о запрете
- Внесение в реестр Роскомнадзором
- Решение Роскомнадзора о блокировке, внесение в «выгрузку»
- Получение провайдером «выгрузки»
- Осуществление провайдером ограничения
- Проверка провайдеров

Как выглядит схема фильтрации

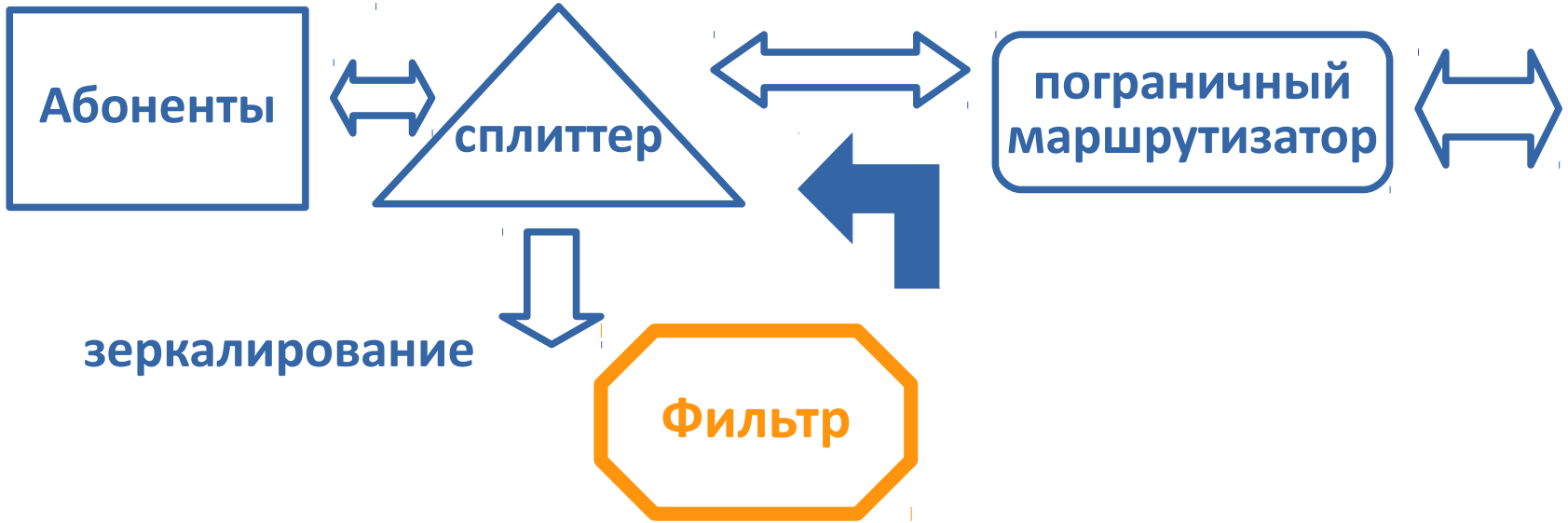
Чем фильтруют

- Фильтрованный трафик вышестоящего провайдера
- Специальные комплексные коммерческие решения
- Свободно распространяемые решения с открытым исходным кодом
- Свой «колхоз»

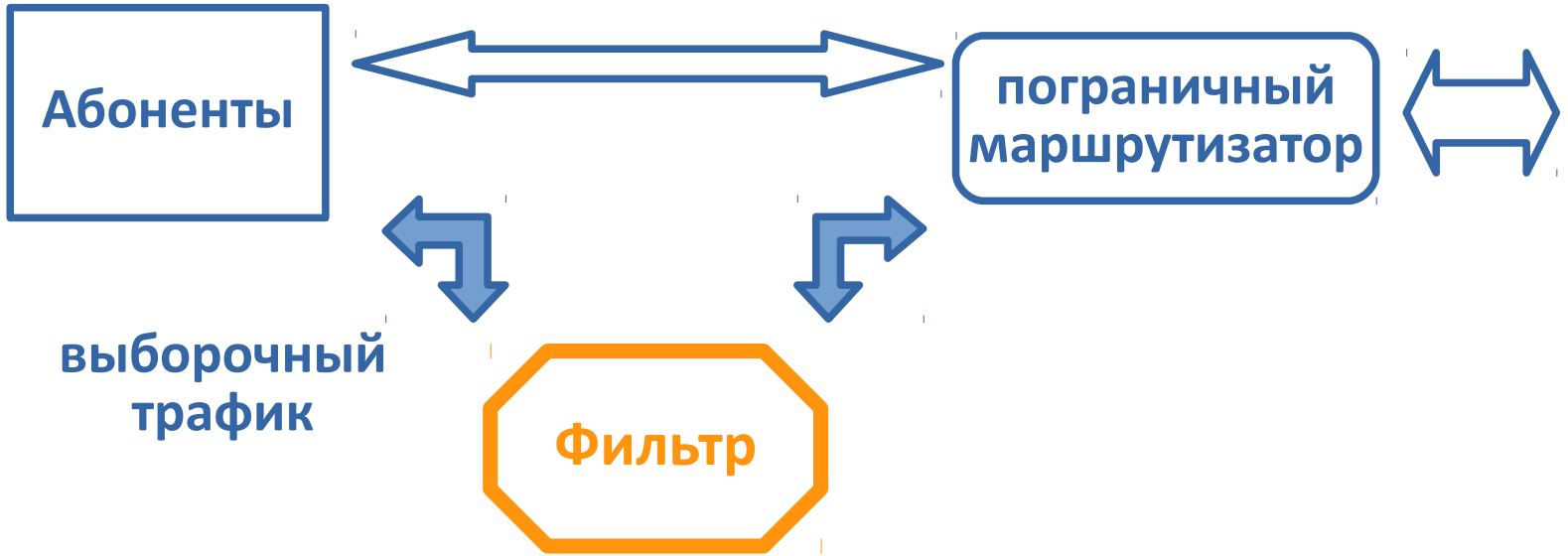
Фильтр в разрыв



Работа на опережение



Выборочная маршрутизация



Распространённая практика

Выборочная маршрутизация

+ Наборы IP-адресов для фильтрации агрегируются в большую сторону

+ Комбинация с DNS-фильтром

Разберем проблемы поэтапно

Принятие решения о блокировке

- Адресат уведомления не точен, уведомления теряются
- Открытой информации нет
- Сроки взаимодействия не соблюдаются
- Протоколы и тексты решений не предоставляются

Время применения «выгрузки»

- Сутки (и блокировка, и разблокировка)
  - например, ночные обновления коммутаторов
- Незамедлительно
  - в течение часа по устной договорённости

Что внутри «выгрузки»

Всегда: тип блокировки и реквизиты решения

- URL(s) + домен + IP-адрес(а)
- Домен + IP-адрес(а)
- Домен с маской (*.example.com) + IP-адрес(а)
- IP-адрес(а)

Статистика «выгрузки»

записей:	123 452
тип «по URL»:	47 027 (38.1%)
тип «по домену»:	67 807 (54.9%)
тип «по маске»:	6 400 (5.2%)
тип «по IP-адресу»:	2 218 (1.8%)
уникальных URL:	52 621
IP-адресов «по IP»:	44 443
блоков IP-адресов:	60
охвачено IP «по IP»:	3 678 864

размер в архиве:	7 MB
размер «выгрузки»:	40 MB
в день:	~ 70

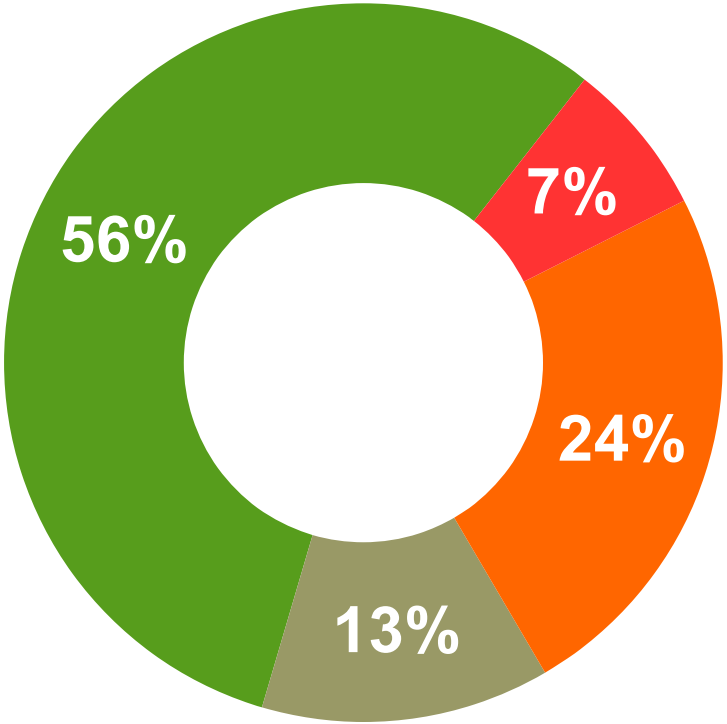
Токсичность «выгрузки»

- Избыточность
- URL с фрагментами (#) и сессиями
- Неправильные URL и домены
- Актуальность IP-адресов

Актуальность «выгрузки»

IP-адреса в «выгрузке»
и в реальности:

- Совпадают
- Частично
- Различаются
- Отсутствуют



Проверка блокировок

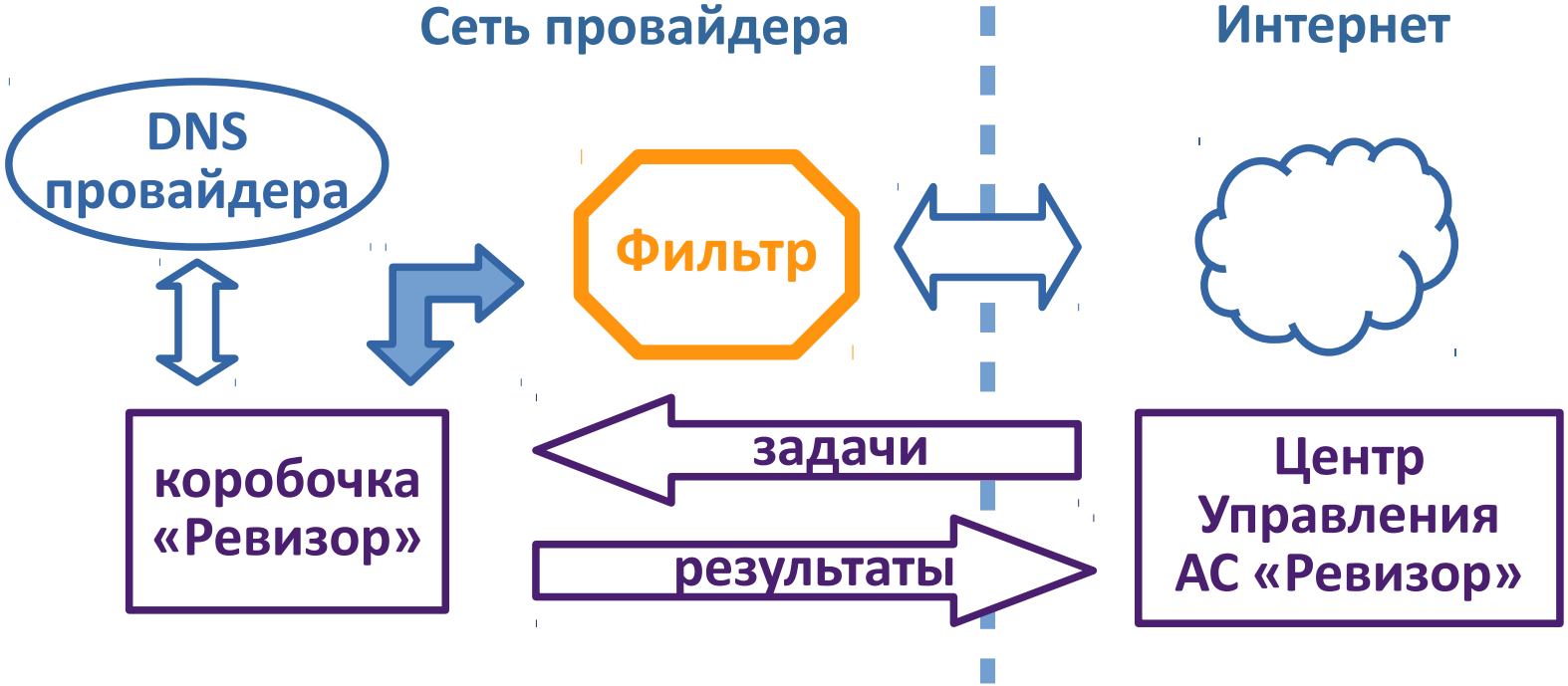
Вся история реализации блокировок в России – это история проверок

До реестра запрещенных сайтов существовал список экстремистских материалов Минюста и прокурорские проверки блокировок по этому списку

Виды проверок

- Выездные проверки
- АС «Ревизор»

Схема АС «Ревизор»



Проблемы проверки

- СПЕКТР-2017, доклад Вэклича А.А. (ФГУП ГРЧЦ)
- Это фильтр провайдера или ресурса?
- Показатель блокировки для HTTPS, домена, IP-адреса
- Показатель блокировки для других протоколов
- Как проверить домен по маске?

Методика работы АС «Ревизор»

Что делать без методики

- Экзистенциальный опыт
- Эмпирический путь
- Чатик в Телеграм
- Норматив «способы и методы»

Методика работы с «выгрузкой»

- по URL
  - HTTP фильтр по заголовкам
  - HTTPS фильтр как «домен»
- по домену
  - HTTP фильтр по заголовку Host
  - HTTPS фильтр DNS или SNI или IP-адреса
  - Остальное как «IP-адрес»
- по домену с маской
  - Как домен с учетом шаблона в домене
- по IP-адресу и блоку IP-адресов

Проблемы фильтрации

Добросовестные участники интернета:

- Нет умысла
- Не нарушает законодательство

Какой DNS? Почему DNS?

- А причем тут DNS? Добросовестные участники
- Перехватывать весь DNS трафик? SLA
- Создавать свою систему подмены ответов?
- DNSCrypt, DoT, DoH

Что делать с доменами по маске

- HTTP/HTTPS сканировать всю полосу
- Что делать с остальными протоколами?
- А проверки всё равно нет

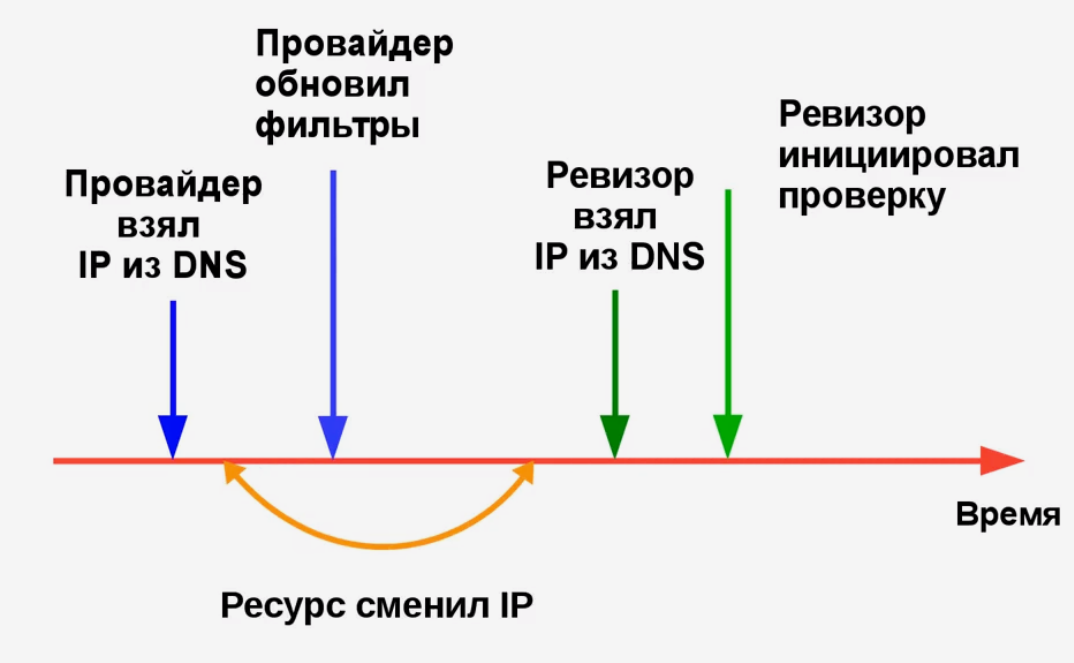
Что делать если на порту 443...

- Нет SNI
- ESNI
- QUIC, DNSCrypt, VPN, MTProto-proxy

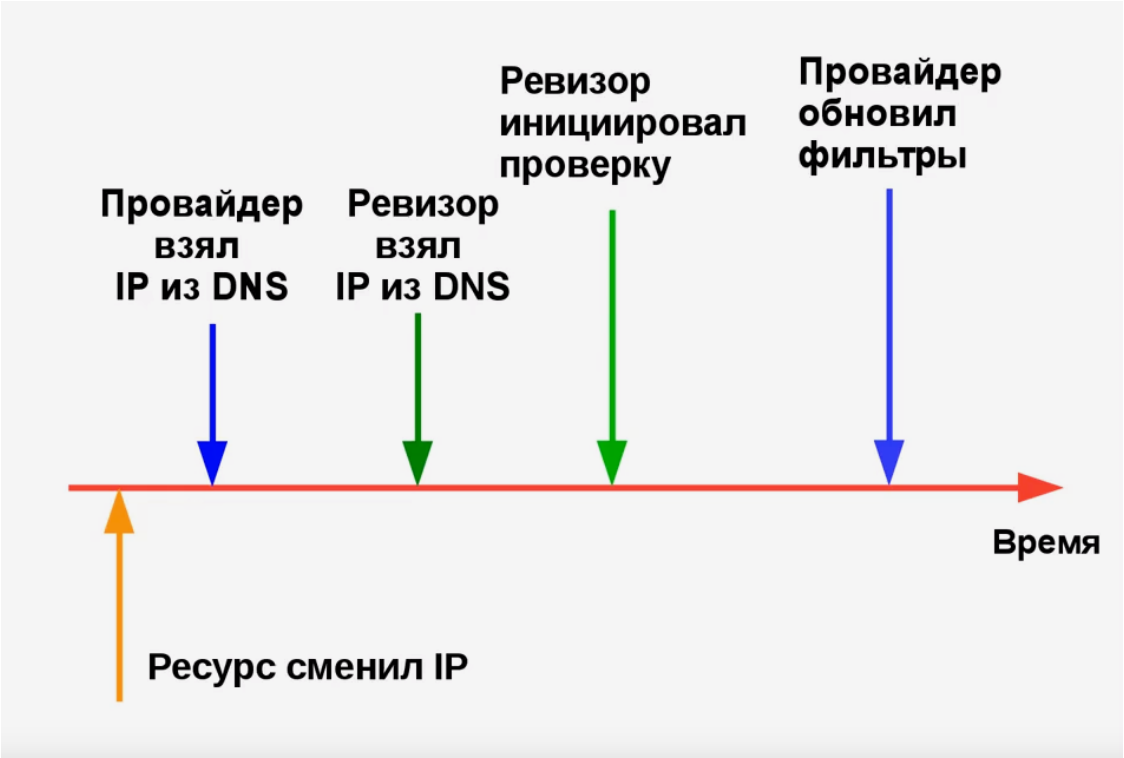
Резолвинг домена

- В нормативе нет, но «вы же понимаете»
- Возможность выборочной фильтрации

Проблема фаз при проверке



Проблема фаз при проверке



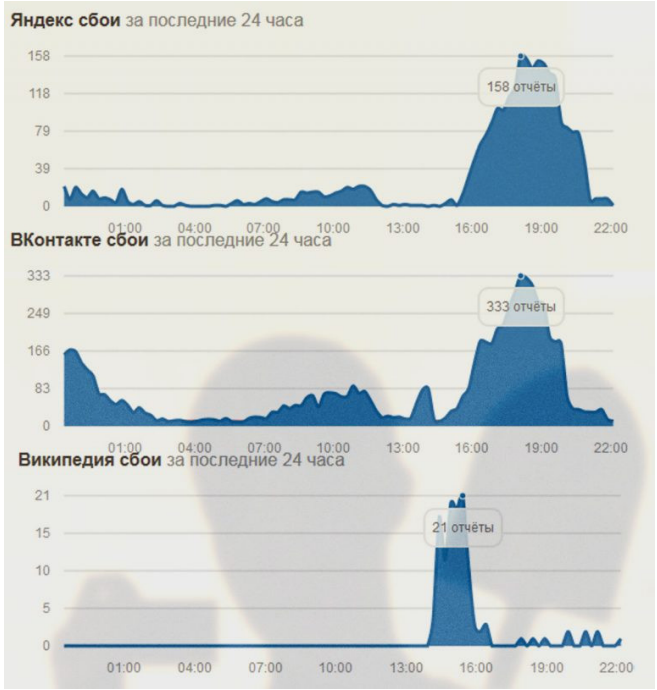
Этот непростой резолвинг

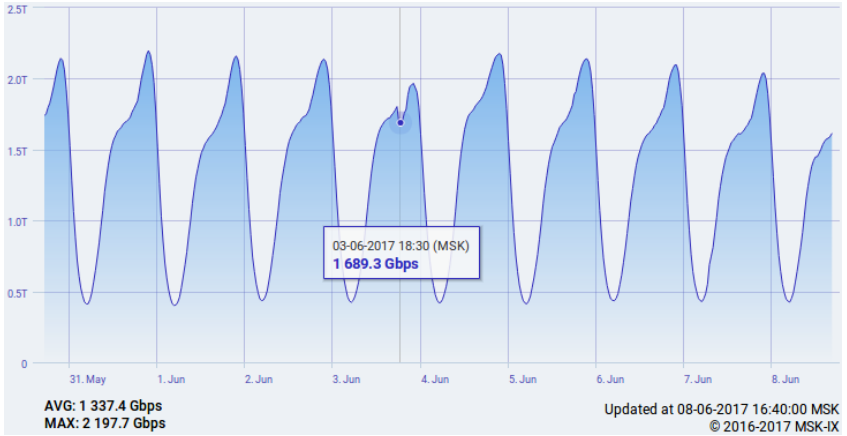
- Балансинг
- Геотаргетинг
- Миграция сервисов, в том числе и умышленная

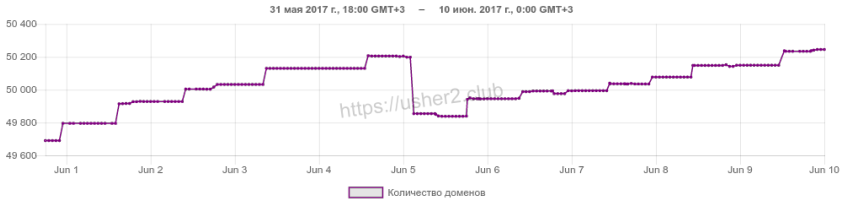
«Протухшие» домены

- У домена закончился срок регистрации, но он остаётся в выгрузке
- Новый владелец домена получает контроль над частью «выгрузки»
- Сейчас «протухших» доменов в «выгрузке» около 200, но мы не знаем, сколько уже купленных

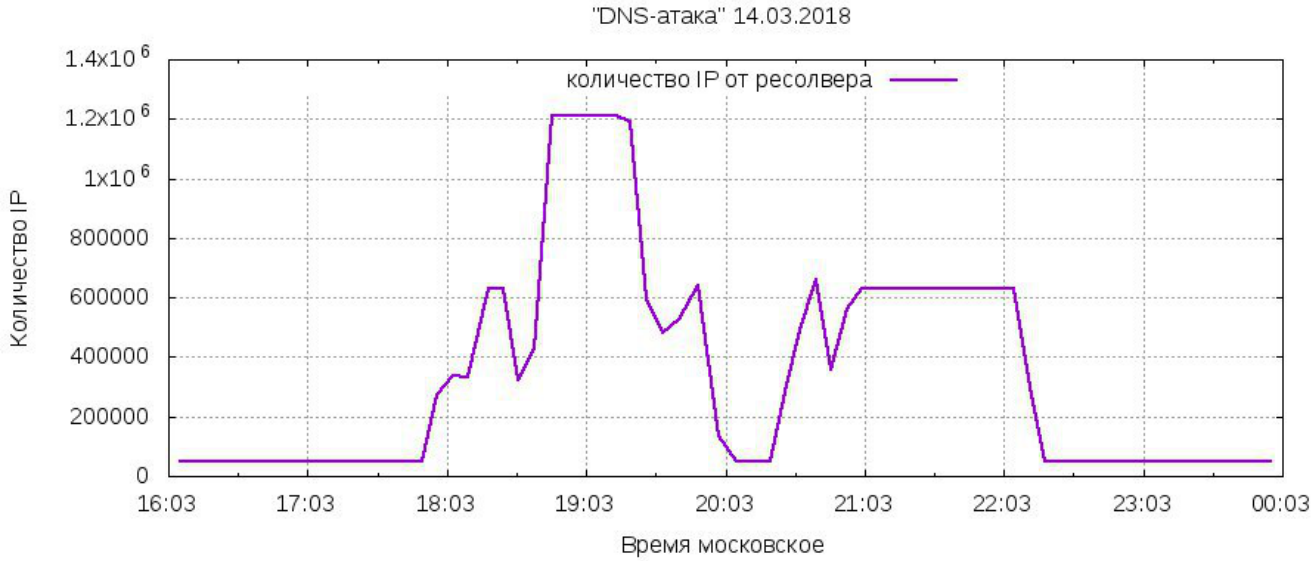
«DNS-атака» летом 2017



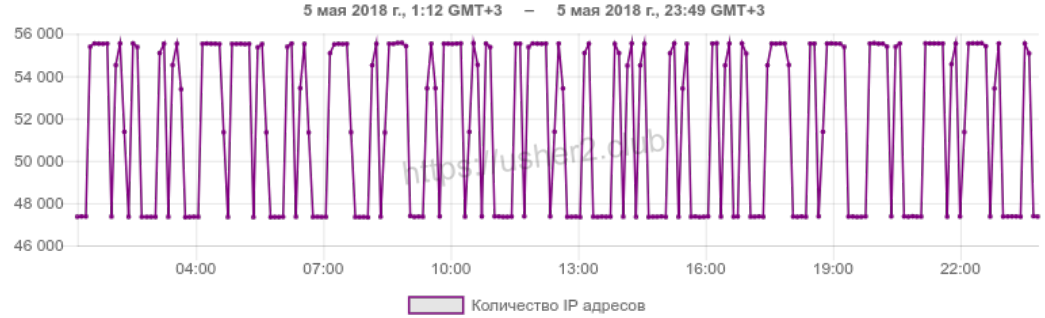


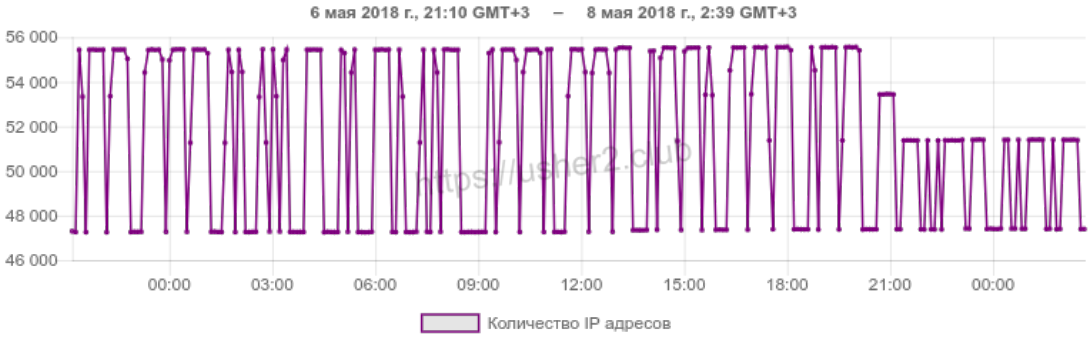


Авария ТТК 14 марта 2018



Послание на графике в мае 2018





Кстати об авариях и сбоях

Проблемы обслуживания

- Оборудование и программы фильтрации не хотят ходить строем
- Нагрузка и QoS
- Motobratan.ru летом 2017

Регламент техобслуживания

- Не работает сервис «выгрузок»
- Авария на каналах связи
- Поломка фильтров
- Профилактика фильтров

Фантазии

Белые списки

- Критерии включения
- Система взаимодействия
- В облаках – заявка на каждую виртуалку?
- Бедный CI/CD

Этот чудный и волшебный DPI

- Производительность
- Хранение состояний
- Сбои

Единый DNS для резолвинга

- Трудоёмкая задача
- Не решает проблему фаз при проверке
- Легче держать «выгрузку» актуальной

Можно ли заблокировать Telegram?

Да. При помощи изменения нормативной базы, волшебных DPI и пренебрегая сопутствующим ущербом

Надеюсь мне удалось дать общее представление о технической составляющей блокировок интернета в России

ВОПРОСЫ

Филипп Кулин

https://usher2.club