Безопасность DNS

Филипп Кулин

Saint HighLoad++

Откиньтесь на спинку кресла

- Эта презентация сделана с помощью LaTeX
- Я расскажу страшную сказку
- Я попытаюсь сделать акцент на точку зрения роботов
- Несмотря на обыденность, тема DNS очень специфична
- Без сомнения, мы рассмотрим и какие-то решения

HL++ 2021 Saint HighLoad++

DNS — всему голова

- Пользователи сети
- API, CDN
- Kubernetes, автообнаружение и конфигурация сервисов
- Невообразимое количество всего

HL 2021 Saint HighLoad++

Где-то под сценой...

- MySQL определяет домен для подключившегося IP
- Apache определяет домен для подключившегося IP
  даже если `HostnameLookups Off`, но есть `Require`
- Microsoft Windows постоянно шлет DNS Update в сеть
- Запустите tcpdump/WireShark

HL 2021 Saint HighLoad++

DNS — это просто?

Три каверзных вопроса:

- Каков максимальный размер доменного имени?
- Точку на конце надо ставить?
- Что именно спрашивает ресолвер и что отвечают DNS-сервера при рекурсивном обходе?

Как устроен DNS

здесь схемка

HL 2021 Saint HighLoad++

Особенности классического DNS

- UDP транспорт. Нет соединения
- Нет идентификации серверов DNS
- Нет контроля данных
- Нет шифрования

HL 2021 Saint HighLoad++

Угорозы в системе DNS

здесь схемка

HL 2021 Saint HighLoad++

Заложенная в DNS безопасность

Saint HighLoad++ 2021

Основные проблемы

- Подделка
  - Отравление
  - Взлом серверов и замена записей
  - Поддельные серверы, BGP-injection
- Прослушка
  - Шпионаж и промышленный шпионаж
    - … с использованием госрегулирования
  - Маркетинговые исследования
  - Система блокировок сайтов

HL 2021 Saint HighLoad++

Вопросы

В любом случае пишите мне

schors@gmail.com

Saint HighLoad++ 2021

Ссылки

[0] *Beamer - Overleaf, Online LaTeX Editor*. https://www.overleaf.com/learn/latex/Beamer.

[0] Uri Nativ. *How to present code.* 2016. https://www.slideshare.net/LookAtMySlides/codeware.

[0] Филипп Кулин. *Пишем презентации в LaTeX*. 14 окт. 2019. https://habr.com/ru/post/471352/.

Saint HighLoad++ 2021