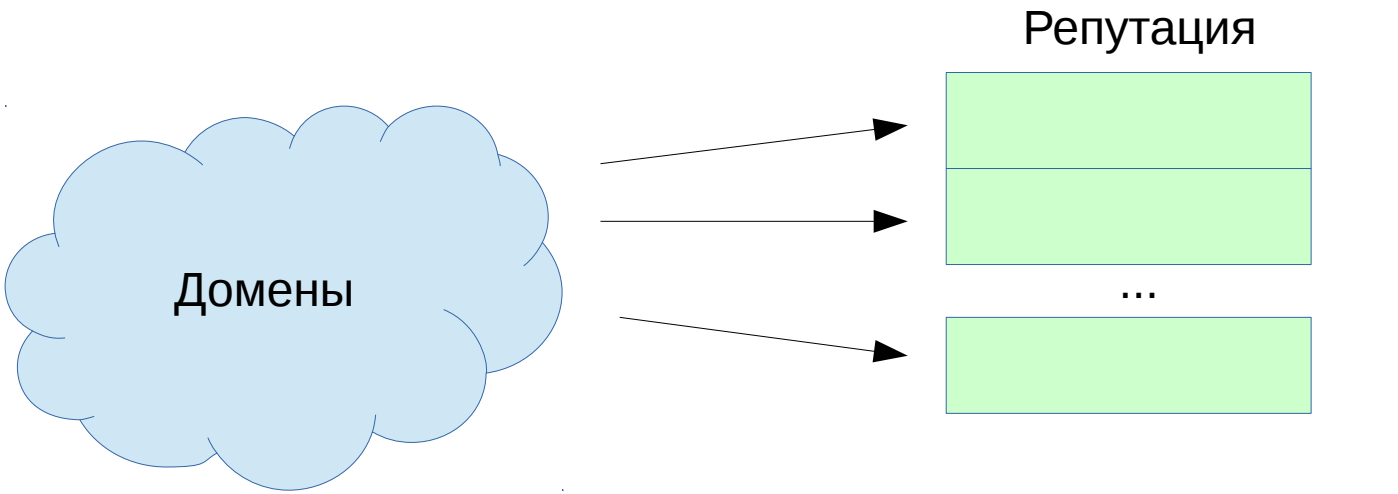
Технический
Центр
Интернет

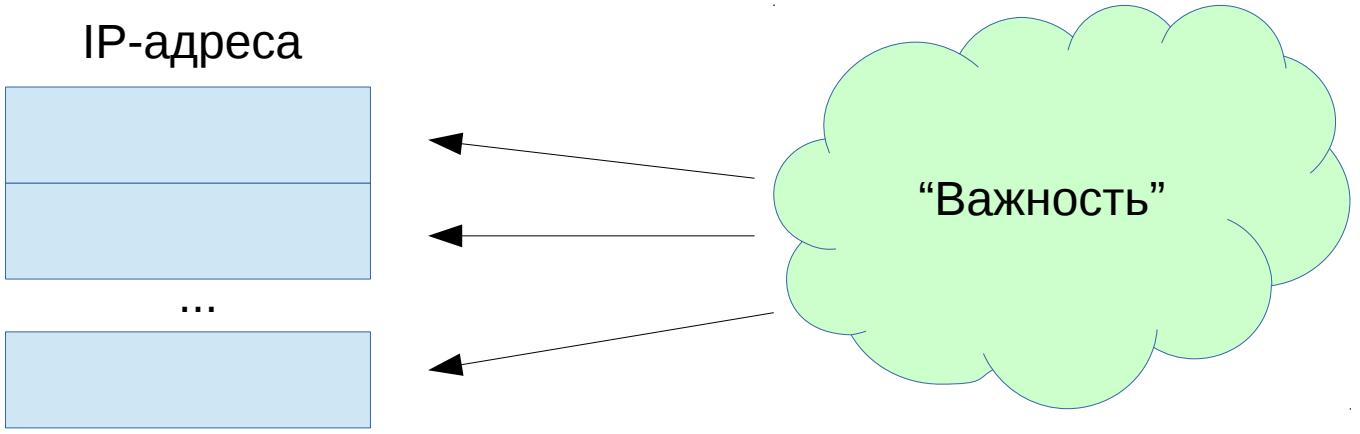
Возможности прогнозирования при нарушении связности

Александр Венедюхин,
ТЦИ

TLDCON, 2018

Технический
Центр
Интернет





Технический Центр Интернет

Задача

В наборе произвольных IP-адресов заранее выявить адреса **“значимых” ресурсов**

Технический
Центр
Интернет

Задача

В наборе произвольных IP-адресов обнаружить адреса “значимых” ресурсов

“Значимый” ресурс - ресурс, потеря доступа к которому окажется “значимым событием”

(Рекурсия. Помогает с определениями)

Технический Центр Интернет

Задача

В наборе произвольных IP-адресов обнаружить адреса “значимых” ресурсов

Технический Центр Интернет

Задача

В наборе произвольных IP-адресов обнаружить адреса “значимых” ресурсов

Технический Центр Интернет

Задача

В наборе произвольных IP-адресов обнаружить адреса “значимых” ресурсов

Технический Центр Интернет

Задача

В наборе произвольных IP-адресов обнаружить адреса “значимых” ресурсов

Не только веб-ресурсы

Технический Центр Интернет

Источники информации:

DNS: файлы зон
DNS: запросы резолверов (снифинг трафика)

трафик: адреса, число пакетов
трафик: типы протоколов

Технический Центр Интернет

Трафик:

Объёмы (число пакетов) говорят только о числе пакетов

80/tcp - но это “контроллер” ботнета, работает не по HTTP

**резервные узлы CRM - трафика нет, до тех пор,
пока не сломались основные**

Про “значимость” IP-адресов ничего сказать нельзя

Технический Центр Интернет

Трафик:

Online-игры: сотни тысяч пользователей и *огромный UDP-трафик* с собственным протоколом внутри

DDoS-атака: пара “пользователей” и *огромный UDP-трафик* с плохо предсказуемым контентом внутри

Как различить, с точки зрения “значимости”?

Технический Центр Интернет

DNS:

Файлы зон:

1) наличие делегирования - только *возможность* доступа;
2) для TLD - не видны домены ниже второго уровня;
3) *ничего* не говорит о ресурсах, не использующих общепринятую DNS.

Passive DNS (сниффинг):

1) видно *много,* даже то, чего нет в зонах;
2) статистика относится к резолверам и ботам, а не к пользователям;
3) можно увидеть зловреды и атаки, но не “значимые” ресурсы.

Технический Центр Интернет

DNS:

Крупные ресурсы - резолвятся в динамические списки адресов:

география, загруженность, время суток.

Технический Центр Интернет

DNS и трафик:

Можно увидеть, что происходит в каждый момент времени, но

определить значимые и важные ресурсы нельзя

Технический
Центр
Интернет

Разнообразия добавляет

IoT

Технический Центр Интернет

IoT

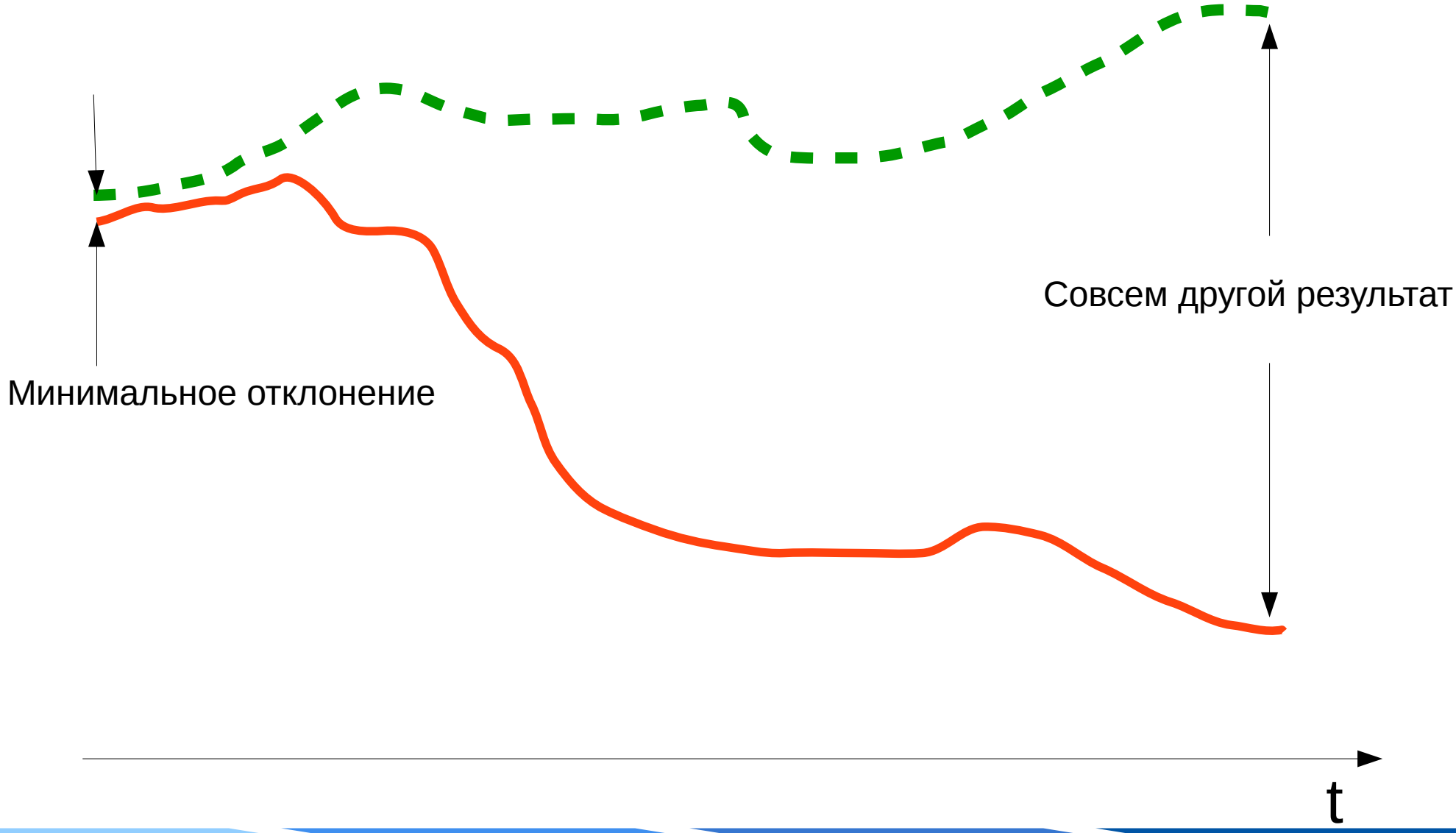
Непредсказуемое разнообразие протоколов (telnet на порт 3138 и текстовые команды в Unicode)

Относительно маленький трафик,

но пользователи не готовы остаться без освещения, запертыми в домах

Технический Центр Интернет

Сложная система



Технический Центр Интернет

Сложная система

Нет точных измерений, а погрешность - меняет всё дело

Выводы:

Технический Центр Интернет

Важно сохранение и улучшение связности: связность делает Интернет - Сетью

Для Сети значимы все ресурсы => связность нельзя преднамеренно ухудшать

Технический Центр Интернет

Спасибо за внимание!

Вопросы?