Противодействие атакам на сети передачи данных на основе анализа состояния сети

Анатолий Корсаков, генеральный директор ООО МФИ Софт

2011 год

Бизнес оператора. Цели и задачи

Цели:

- Максимизация прибыли
- Наращивание абонентской базы

Задачи:

- Запуск услуг
- Запуск и эксплуатация сети
- Обеспечение сервисной поддержки абонентов
- Продвижение услуг

Действия оператора по сохранению абонентской базы

- Ценовая политика
- Новые услуги
- Качество предоставляемых услуг
- Сервис

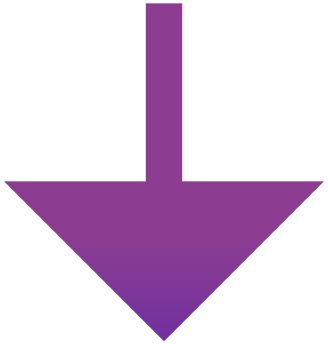
Почему абонент может сменить оператора?

Причины смены оператора:

- Цена
- Качество услуг:
  - скорость
  - надежность
- Дополнительные услуги
- Сервис

Анализ состояния сети. Зачем?

Сетевые атаки



Разглашение персональных данных

Раскрытие коммерческой информации

Отказ в обслуживании

Сетевая атака. Зачем и кому она нужна?

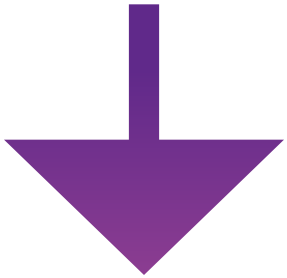
- Компьютерное хулиганство
- Кража данных
- Устранение конкурента
- Интернет-рэкет

Потери оператора от сетевых атак

- Финансовые потери
- Снижение количества клиентов
- Репутационные риски
- Сокращение размеров бизнеса

Мониторинг состояния сети

- Загрузка каналов
- Типы трафика
- Размеры пакетов по различным направлениям трафика
- Статистические данные по движению трафика



Программа для анализа NetFlow трафика

А что используете Вы?

Мониторинг сетевого трафика

НЕ ТОЛЬКО:

- Загрузка каналов
- Типы трафика
- Размеры пакетов по различным направлениям трафика

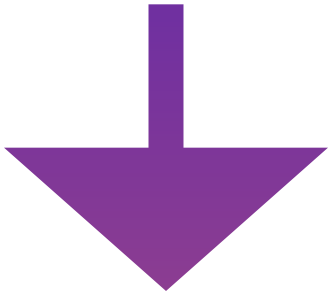
НО И:

- Выбор партнеров для пиринга
- Оценка эффективности имеющихся точек обмена трафиком

А что используете Вы?

Мониторинг сетевых атак

- Атаки на сеть: роутеры, каналы, серверы
- Атаки на/от клиента
- Входящие/исходящие/транзитные атаки



Обнаружение

Локализация

Изучение характера атаки

А что используете Вы?

Подавление сетевых атак

- Средства защиты
- Превентивные меры

А что используете Вы?

Подавление сетевых атак

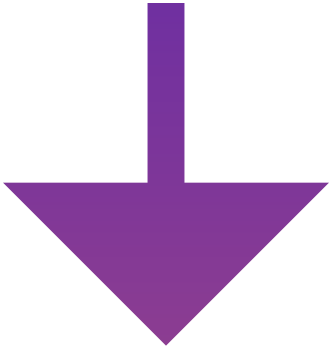
- Анализ маршрутизации
- Несоответствие физического источника трафика его характеристикам
- Принадлежность трафика известным скомпрометированным ресурсам
- Трафик, соответствующий сигнатурам атак
- Трафик, содержащий ответы от ресурсов

Подавление сетевых атак

- Отслеживание маршрутизации
- Расшифровка противодействия
  - средствами централизованного управления сетевым оборудованием
  - средствами специализированного DPI-based очистителя

Существующие на рынке решения – система Периметр

- Мониторинг сетевого трафика
- Обнаружение атак и аномалий
- Оптимизация, планирование и контроль инфраструктуры сети



- Базовая очистка
- Стат. фильтр
- Bot-сети
- IP-authentication
- Ограничение TCP-сессий

- Контроль TCP-сессий
- Интеллектуальный shaping
- Контроль простаивающих соединений
- DNS-authentication
- VOIP-защита/мониторинг

Спасибо за внимание

ООО «МФИ Софт»
125009, Москва, ул. Тверская 27, стр.1
тел. (495) 6427075
info@mfisoft.ru, sales@mfisoft.ru
www.mfisoft.ru