EDGE ЦЕНТР

# Стражи Виртуального Мира: Операторы связи и их борьба с DDoS-атаками, ботами и хактивистами


## Артём Избаенков

Директор по развитию направления кибербезопасности

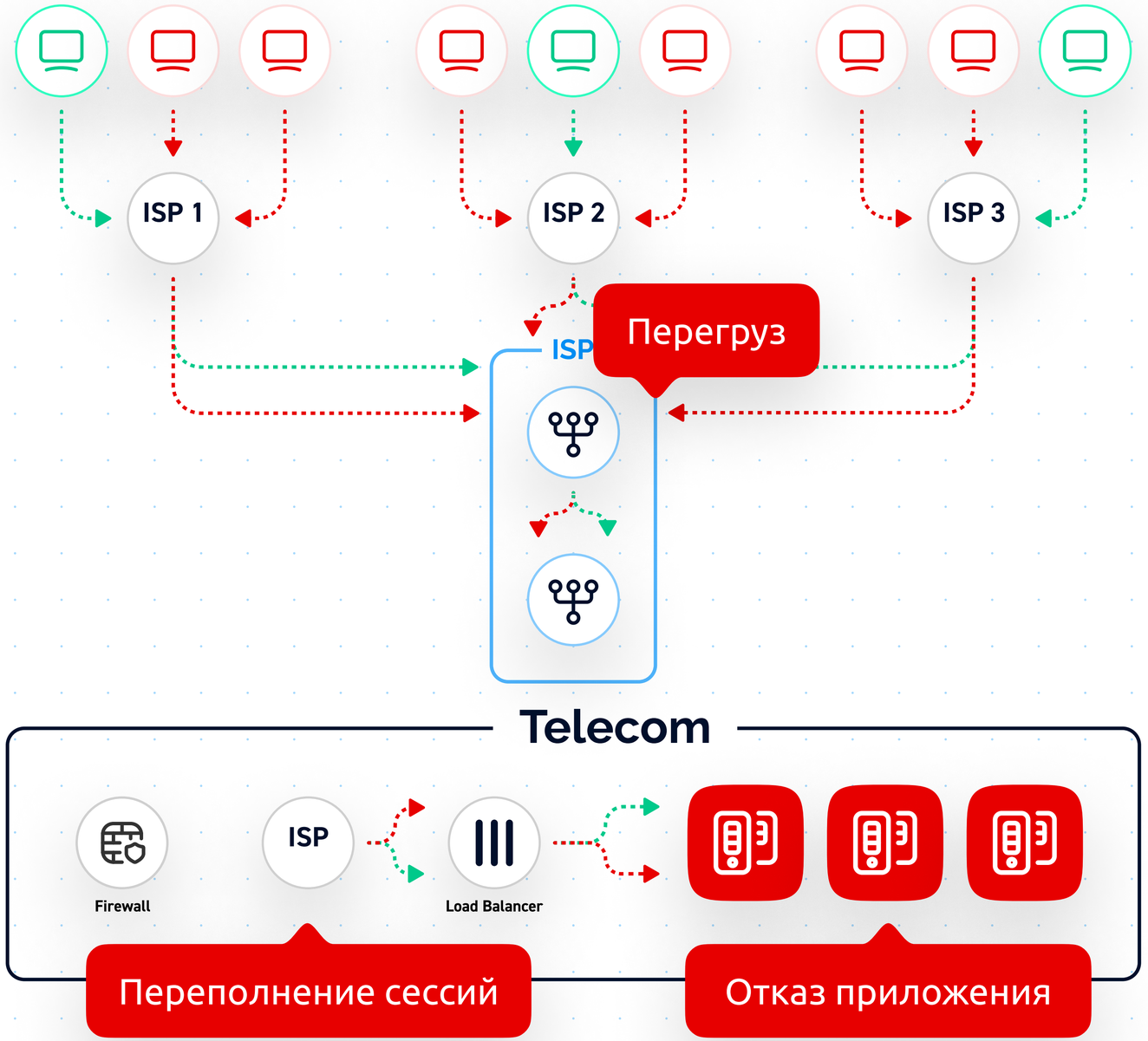
Член правления АРСИБ

Член ISDEF

# Сложность современных DDoS-атак

**Сегодня DDoS можно разделить на 3 типа:**

1. Перегрузку канала
2. Переполнений таблиц сессий
3. Отказ сервиса (приложения)



# Как влияют DDoS-атаки на операторов связи

Как объемные атаки, так и атаки уровня приложения могут привести к отказу в обслуживании сервисов в операторе связи, тем самым закрыв доступ к множеству ресурсов.

- Недоступность ресурсов клиентов
- Недоступность call-центра
- Огромные убытки по нарушению SLA
- Недоступность всех сервисов

# Недоступность сервисов влечет не только финансовые потери

### IT-отдел

Сколько людей требуется для отражения атаки?

### Help Desk

Сколько звонков будет во время атаки?

### Потеря данных

Сколько ручной работы нужно сделать, если сервис прерван?

### Напрасная работа

Каков объем работы, проделанной зря, если сервис недоступен?

### Штрафы

Сколько необходимо выплатить при нарушении SLA?

### Потеря бизнеса

Сколько стоит потеря новых клиентов?

### Ущерб репутации

Сколько стоит ущерб имиджу компании?

# Планирование рисков

DDoS-атаки — угроза доступности №1 – должны быть частью анализа рисков.

Измеряя риски доступности и надежности сервиса, необходимо понять, где риск угрозы DDoS-атак в вашем случае?

1. Выбор площадки
2. Физическая безопасность
3. Пожарная безопасность
4. Электричество
5. Окружающая среда
6. DDoS-атаки

# Тренды DDoS атак 2023

- Атаки уровня L7 (Приложения) на web инфраструктуру
- Целенаправленные атаки на DNS сервера компаний
- Обьем атак ботнетов на РФ легко перешел границу в 1,2 Тбит/с и более 500 Mpps
- Рост Мощности + Длительности атак >1 Тбит/с >10 дней
- Существенную долю ботов составляют боты из РФ
- Использование облачных ЦОДов для организации и монитизации DDoS атак
- “Ковровые” атаки на инфраструктуру операторов связи

# Уязвимые места

**Сетевая инфраструктура:** Недостаточно защищенные и производительные маршрутизаторы и коммутаторы могут стать точкой входа для злоумышленников.

**DNS-серверы:** Атаки на DNS-серверы могут вызвать перенаправление трафика или даже отказ в обслуживании.

**Серверы аутентификации:** Серверы, контролирующие доступ к сети, могут стать целью для атак на уровне аутентификации.

**Серверы приложений:** Плохо защищенные серверы приложений могут быть перегружены запросами и привести к снижению производительности или отказу в обслуживании.

**BGP стыки:** Сессии организованные на “белых” IP адресах могут быть атакованы небольшим TCP SYN флудом и отключены клиенту.

**BGP Hijacking (хищение BGP-маршрутов):** Злоумышленники могут отправить ложные маршрутные обновления, чтобы перенаправить трафик через свои серверы. Это может привести к перехвату данных или даже к отказу в обслуживании.

# Рекомендации для операторов связи

1. Возрастающая сложность и масштабность DDoS-атак создают серьезные риски для операторов связи.
2. DDoS-атаки могут привести к снижению качества обслуживания, потере доходов и негативно повлиять на репутацию оператора.
3. Операторы связи должны разрабатывать и внедрять эффективные меры защиты, чтобы минимизировать влияние DDoS-атак на их инфраструктуру.
4. Использование облачных технологий и распределенных систем помогает операторам связи справляться с большими и сложными DDoS-атаками.
5. Сотрудничество с поставщиками услуг по безопасности и обмен опытом с другими операторами могут повысить эффективность защиты от DDoS.

# Рекомендации для операторов связи

6. Операторы связи также должны регулярно анализировать свои сети на наличие уязвимостей и обновлять системы для предотвращения успешных атак.

7. Обучение персонала оператора связи в области кибербезопасности позволяет более оперативно реагировать на DDoS-угрозы и минимизировать последствия.

8. Мониторинг сетевого трафика и анализ его характеристик позволяют операторам оперативно выявлять аномалии, связанные с возможными DDoS-атаками.

9. Разработка четких планов реагирования на DDoS-атаки помогает операторам связи минимизировать простои и быстро восстанавливать работоспособность систем.

10. В условиях постоянно меняющейся угрозной ландшафта операторы связи должны непрерывно совершенствовать свои стратегии защиты от DDoS.

# Что поможет избежать проблем с DDoS?

- **Грубые межсетевые экраны (Firewalls) на DPDK/XDP:** Использование межсетевых экранов помогает фильтровать вредоносный трафик и блокировать подозрительные запросы, предотвращая их до достижения целевых серверов с высокой производительностью >1 Тбит/с
- **Распределенные облачные сервисы партнеров по защите от DDoS:** Применение облачных защитных сервисов позволяет фильтровать трафик еще до его достижения инфраструктуры оператора, разгружая сеть и снижая нагрузку. Есть схемы интеграции с перемаршрутизацией трафика (re-route)
- **Мониторинг и анализ трафика:** Системы мониторинга и анализа трафика позволяют операторам своевременно выявлять аномалии и странные паттерны поведения, что помогает оперативно реагировать на атаки. Анализаторы работают с BGP/SNMP/Flow
- **BGP FlowSpec:** Ограничение передачи трафика для конкретных IP-адресов или протоколов по множеству тонких параметров может снизить влияние атаки на сеть.
- **BGP Blackhole Filtering:** Пересылка весь трафика от атакующего IP-адреса в "черную дыру" (blackhole) помогает отключить злоумышленников от целевой инфраструктуры.

# Интересные кейсы

## Клиент

# Федеральный оператор связи

## Проблема

Злоумышленники развернули бот-сеть, способную распространяться автоматически, заражая устройства под управлением уязвимого программного обеспечения. Боты были программированы на осуществление DDoS-атак из сети оператора, создавая дополнительную нагрузку.

## Решение

Командой EdgeЦентр Security был развернут анализатор трафика на сети оператора связи для выявления аномальной активности как во внешнем периметре сети так и во внутреннем. Дополнительно были организованы меры подавления в виде BGP Blackhole/BGP FlowSpec и возможность перемаршутизации трафика на локальные региональные узлы фильтрации EdgeЦентр

## Клиент

# ТОП 15 провайдер Москвы

## Проблема

Злоумышленники направили массивный объем запросов к DNS-серверам оператора связи. Это вызвало перегрузку серверов, что привело к снижению качества обслуживания для клиентов, которые испытывали задержки при обращении к веб-сайтам и другим ресурсам.

## Решение

Командой EdgeЦентр Security был предоставлен защищенный DNS сервер и помощь в переносе DNS зоны под защиту. В дополнении собран физический стык для фильтрации DDoS атак.

## Клиент

# Городской провайдер

## Проблема

Повышенная популярность и много внимания в СМИ вызвали зависть конкурентов и они заказали DDoS атак на городского провайдера. Атака заключалась в генерации большой спуф активности на каждый хост именно в инфраструктуре (AS) провайдера (“ковровая атака”) что привело его к отказу.

## Решение

Командой EdgeЦентр Security был срочно организован стык с провайдером. Трафик перемаршутизирован через защищенный BGP стык на серых адресах, атака зафильтрована.

EDGE ЦЕНТР

edgecenter.ru

**8 800 775 08 54**