EDGE ЦЕНТР

АРПП Отечественный софт

Sk

DDoS как инструмент кибероперации. Цели, подходы, защита.

Артем Избаенков

Директор по развитию направления Кибербезопасности

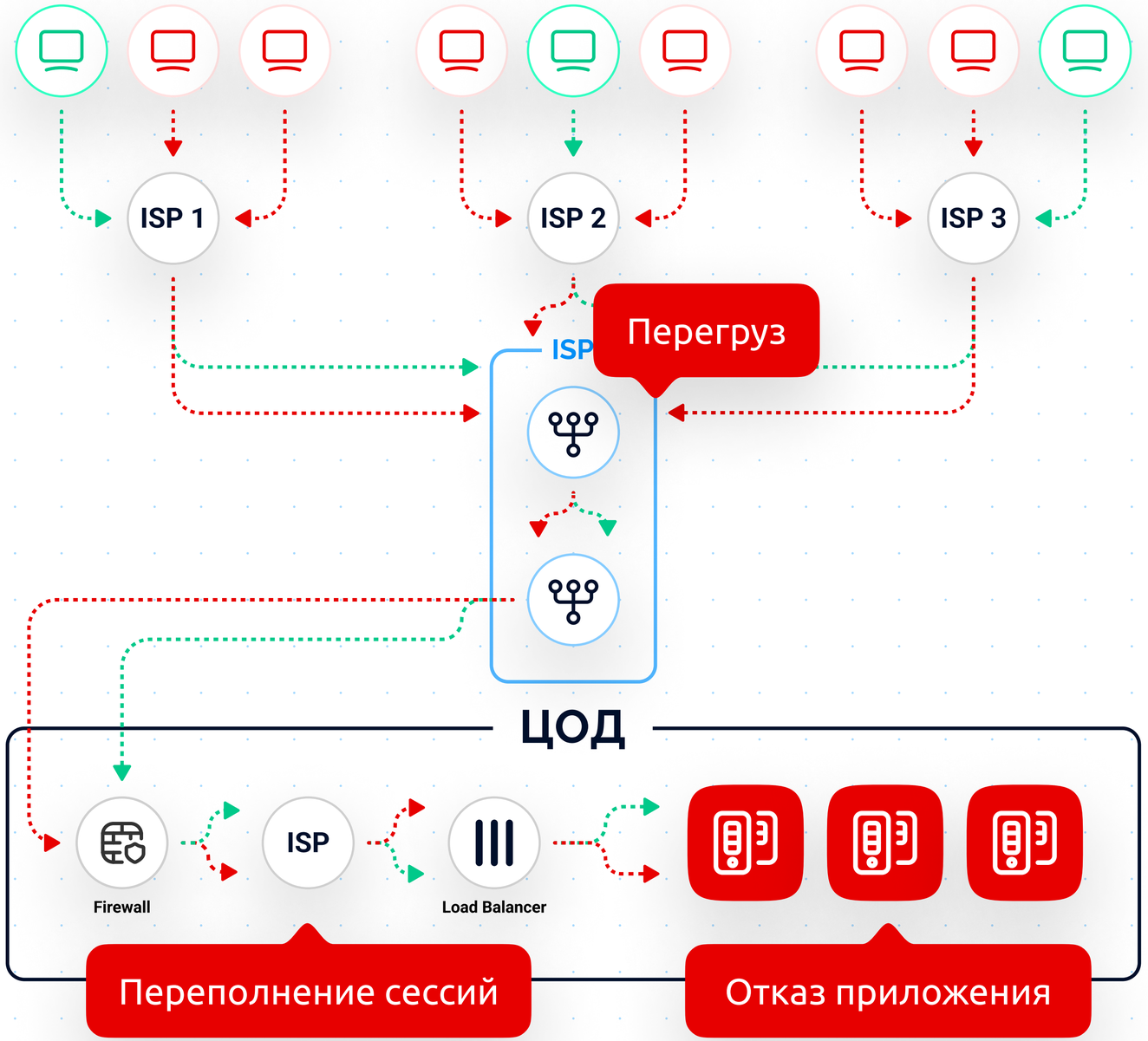
Член правления АРСИБ

Член ISDEF

Сложность современных DDoS-атак

Сегодня DDoS можно разделить на 3 типа:

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



Основные цели DDoS-атак: борьба с конкурентами, политическое давление, шантаж, хулиганство

Незащищенные хостинг-провайдеры зачастую просто отключают атакуемый ресурс.

Кибероперация

- Госструктуры
- Банки
- Телеком
- Крупный E-commerce
- Электроэнергетика
- Машиностроение
- Нефтегазовая отрасль
- Авиакомпании
- Доменные регистраторы
- Металлургя
- Хостинговые компании
- Грузоперевозчики
- Платежные системы
- Информационные порталы
- Электронные торговые площадки

Самые распространённые бот-атаки

DoS- и DDoS-атаки

Боты генерируют огромное количество запросов, чтобы сделать ресурсы недоступными.

Брутфорс

Боты взламывают аккаунты с помощью автоматического перебора паролей.

Скрейпинг

Боты собирают данные с сайтов и могут, например, передать их конкурентам или использовать для спам-рассылок и т.п.

Поиск уязвимостей

С помощью ботов злоумышленники ищут уязвимости приложений и эксплуатируют zero-day уязвимости.

Рекламный фрод

Боты могут кликать на платную рекламу. В итоге компания платит за трафик, который не конвертируется в покупки, ухудшаются позиции сайта в поисковой выдаче.

Скальперские покупки

Злоумышленники автоматически скупают ограниченный товар, чтобы перепродать его дороже.

Искажённая аналитика

Бот-трафик искажает реальную картину поведения пользователей. Компании не получают достоверных данных и не могут оптимизировать конверсии.

Кардинг

Боты могут использовать украденные данные карт, чтобы покупать товары без участия владельцев карт.

Исчерпание товаров (Denial of Inventory)

Товары: например, заполнить корзины или забронировать весь товар. Реальные пользователи не смогут его купить, но товар так и не будет продан.

Комплексный подход к защите сетевого периметра

Как мы защищаем от ботов наших клиентов

Клиент

Интернет-банк

Проблема

Сайт, единственный источник выручки, начал работать медленно и с ошибками. Причина была в ботах, которые собирали информацию о курсах валют и предложениях. Бот-трафик создавал дополнительную нагрузку. А из-за плохой работы сайта начали падать продажи, покупатели уходили к конкурентам.

Решение

Наш сервис проанализировал трафик, выявил паттерны ботов, добавил их в свои сигнатуры и успешно заблокировал всех ботов.

Нагрузка снизилась, и сайт снова стал работать быстро и корректно.

Клиент

Правительственный ЦОД

Проблема

После событий 24 февраля команда по ИБ ЦОД поменяла провайдеров и подключила защищенные решения, но во время построения защищенных каналов, остались уязвимые места, которые позволяли злоумышленникам провести небольшую DDoS атаку и положить всю инфраструктуру региона.

Решение

Проведено стресс-тестирование, предоставлен отчет об язывимостях. разработано совместное решение на базе двух независимых операторов с защитой от DDoS атак.

Планируется размещение очистителей непосредственно в регионе.

Клиент

Топ 10 Банк РФ

Проблема

Злоумышленники использовали уязвимость в бизнес-логике: в личный кабинет можно было войти с помощью СМС.

Боты отправляли огромное количество запросов на отправку СМС. В результате на отправку сообщений клиент потратил миллионы рублей за пару часов

Решение

В первую очередь мы исправили уязвимость: ввели ограничение на количество запросов СМС.

Далее подлкючили защиту от ботов и срезали все нелегитимные запросы. В защите от ботов использовали дополнительные метрики, чтобы детально выявлять
и блокировать вредоносный трафик.

Клиент

Букмекерская компания

Проблема

Компании требовалась защита корпоративных порталов и Битрикса.

Решение

Мы настраивали защиту параллельно с разработкой сайта.

Вместе с этим предоставили защиту Битрикса, которая заблокировала большую часть вредоносных запросов.

Клиент

Операционные офисы банка

Проблема

Злоумышленник вычислили автономную систему Банка и определили IP адреса, используемые для операционных офисов. Они направили распределнную DDoS атаку на все подразделения офиса одновременно, что порализовало работу целого региона не на один час.

Решение

Мы предоставили защищенные каналы до офисов и дополнительно дали защищенный IP транзит для всей автономной системы Банка. Защитив канальную часть полностью от любых DDoS атак со стороны злоумышленников.

EDGE ЦЕНТР

edgecenter.ru

8 800 775 08 54