EDGE ЦЕНТР

АРПП Отечественный софт

Sk

Тонкости DDoS защиты на кейсах

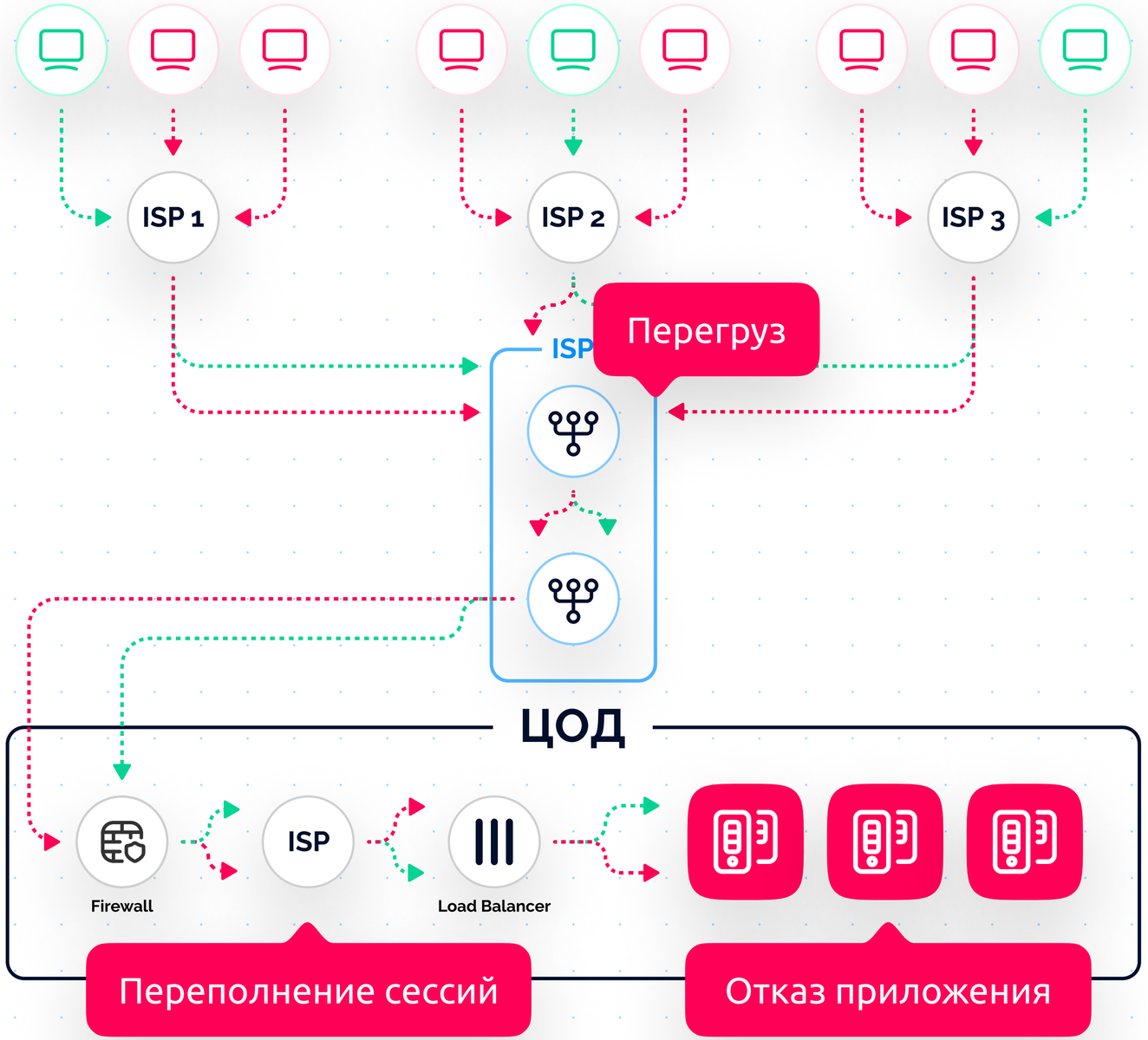
Артем Избаенков

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)



Кибероперация

- Госструктуры
- Металлургия
- Крупный E-commerce
- Телеком
- Электроэнергетика
- Машиностроение
- Нефтегазовая отрасль
- Авиакомпании
- Доменные регистраторы
- Банки
- 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

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

Новостной портал с большим количеством доменов в городах России

Проблема

Сайт регулярно подвергался DDoS-атакам на уровне приложений. Боты делали ресурс недоступным.

Решение

Сначала мы подключили защиту от DDoS-атак на уровне приложений. Выяснилось, что необходима также и защита от ботов.

Чуть позже мы подключили WAF и обеспечили комплексную защиту от DDoS-атак, ботов и хакеров.

Клиент

Интернет-аптека

Проблема

Боты собирали данные о товарах и ценах и специально замедляли работу сайта. Кроме того, они использовали уязвимость в бизнес-логике: на сайт можно было войти с помощью СМС. Боты отправляли огромное количество запросов на отправку СМС. В результате на отправку сообщений клиент потратил миллионы рублей.

Решение

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

В защите от ботов использовали дополнительные метрики, чтобы детально выявлять и блокировать вредоносный трафик.

Клиент

Интернет-аптека с доставкой в 350 городах России

Проблема

Сайт, единственный источник выручки, начал работать медленно и с ошибками. Причина была в ботах, которые собирали информацию о товарах и ценах. 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 50% бот-запросов.

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

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

Московский ресторан

Проблема

На сайте клиента была уязвимость, которой воспользовались злоумышленники. С помощью этой уязвимости они разместили на сайте ресторана фейковую страницу, копирующую страницу оплаты швейцарской почты.

Интерпол попросил регистратора снять домен с делегирования. Так ресторан чуть не лишился своего сайта. Домен удалось восстановить, но устранить уязвимость клиент не смог.

Решение

Мы подключили ресторану постоянную защиту от ботов и закрыли уязвимость для злоумышленников.

Интересные истории

- Один из топ-5 банков
- Электронная торговая площадка
- Крупная сеть интернет-аптек
- Один из топ-5 новостных ресурсов
- Правительственный портал
- Крупная металлургическая компания
- Премиальный дата-центр
- Один из топ-5 операторов связи в Москве

EDGE ЦЕНТР

edgecenter.ru

8 800 775 08 54