EDGE ЦЕНТР

АРПП Отечественный софт

Проактивная защита от DDoS атак: стратегии и инструменты

Артём Избаенков

Директор по развитию направления кибербезопасности

Член правления АРСИБ

Член ISDEF

Член РОЦИТ

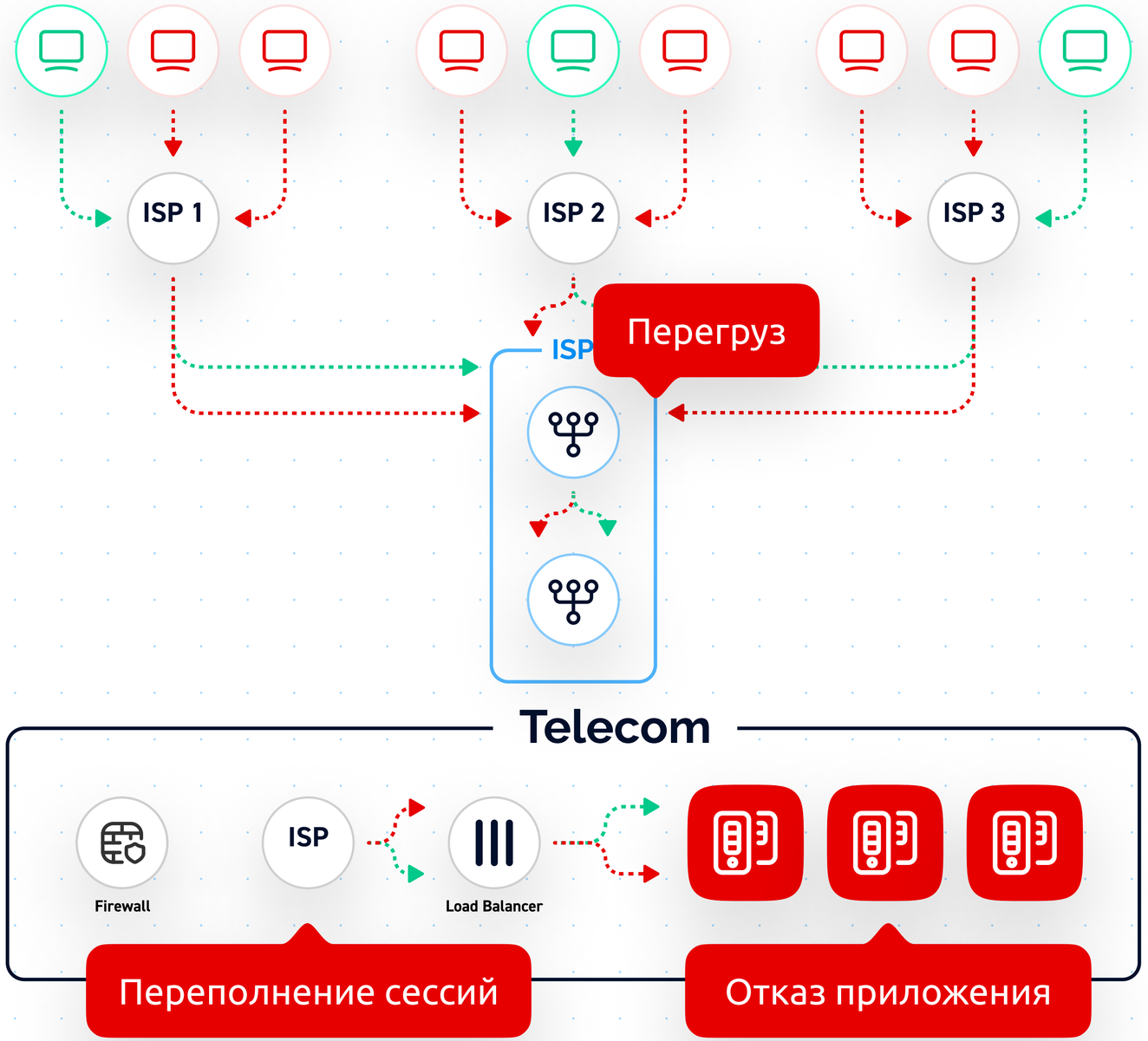
DDoS-атака

Во время DDoS-атаки заражённые хосты (боты) из разных сетей перегружают ресурсы сервера, канала или приложения нелегитимным трафиком. Тем самым они не позволяют легитимным пользователям получить доступ к информации.

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 бизнес

Как объемные атаки, так и атаки уровня приложения могут привести к отказу в обслуживании сервисов в бизнесе, 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?

Кибервойна и Хактивисты

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

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

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

Интересные кейсы

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

Онлайн бронирование авиакомпаний

Проблема

Целью ИТ Армии Украины было вывести из строя работу авиакомпаний. Случайным образом одной из целей стала система регистрации онлайн бронирования. Успешная атака поралезовала работу аэропортов и привела к огромным убыткам.

Решение

Командой EdgeЦентр Security был срочно организован стык с Клиентом. Трафик перемаршутизирован через защищенный BGP стык на серых адресах, атака зафильтрована. построены дополнительные резервные стыки.

Клиент

Агрегатор e-mail рассылки

Проблема

Целью ИТ Армии Украины Был один крупный e-com, на части доменов был сервис агрегатора рассылки. В связи с чем он оказался под массированной атакой в следсвтии которой остановилась треть рассылки по РФ для гос и бизнес структур

Решение

Командой EdgeЦентр Security был срочно организован стык с Клиентом. Трафик перемаршутизирован через защищенный BGP стык на серых адресах, атака зафильтрована. построены дополнительные резервные стыки. Организована защита веб-приложений в течении 1-2 часов после начала атаки

Клиент

ТОП 5 СМИ РФ

Проблема

SEO оптимизация сайта стала ухудшаться. По определенным поисковым запросам касательно СВО, сайт находился даже не в топ 10 ссылок.

Была выявлена ботовая активность направленная на ухудшения поисковых позиций сайта.

Решение

Командой EdgeЦентр Security был выявлен ботнет в Новосибирске, который вел хитрую деятельность с более чем 4 000 виртуальных машин и уникальных IP адресов из РФ. Его работа заключалась в малоактивном посещении определенных статей сайта, что снижала его SEO и понижала рейтинг для поисковых систем, выводя зарубежные ресурсы в ТОП.

Ботнет был заблокирован средствами Антибот системы.

Клиент

Одна космическая компания или DDoS как инструмент информационной войны

Проблема

После значимых событий в жизнедеятельности компании, хактивисты решили использовать DDoS атаку для манипулированием общественным мнением. В след за событиями, хактивисты организовали DDoS атаку на сайты и инфраструктуру компании, пытаясь недопустить публикации официальной информации в интернете от лица компании.

Решение

Команда EdgeЦентр Security мониторила сетевую активность компании. Вычислила DDoS атаку на инфраструктуру и веб-приложения и отразила весь вредоносный трафик.

Клиент

Международный e-comm

Проблема

Аналитики EdgeЦентр Security выявили подозрительную активность по подмене cookies и выгрузки персональных данных и бонусного счета клиентов. Клиент, до выяснения причин, погасил всю инфраструктуру и продажи по РФ.

Решение

Информация подтвердилась спустя 1 час. Вредоносный тип запросов был заблокирован. Инфраструктура была запущена. Клиент произвел доработку API приложения и устранил уязвимость.

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

Международный грузоперевозчик

Проблема

Злоумышленники использовали украденную базу данных клиентов и несколько тысяч ботов, чтобы создать несколько сотен тысяч фейковых заказов в течении суток.

Решение

Внедрение защиты от ботов, поомгло срезать нелегитимные запросы. В защите от ботов использовали дополнительные метрики, чтобы детально выявлять
и блокировать вредоносный трафик.

Клиент

Энциклопедия Руниверсалис

Проблема

После объявления о запуске энциклопедии в федеральных СМИ случился скачок посещаемости и «активность, похожая на DDoS-атаку».

Серверы хостера, чьими услугами пользовались Руниверсалис, не справились с нагрузкой, и сайт стал недоступен.

Решение

Мы разместили сайт энциклопедии на своих мощных серверах, подключили CDN и комплексную защиту от DDoS-атак и ботов. Работа ресурса была восстановлена.

После этого на Руниверсалис обрушилось несколько мощных DDoS-атак, но наша защита успешно отразила их. Вредоносный трафик никак не повлиял на работу ресурса.

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.

EDGE ЦЕНТР

edgecenter.ru

8 800 775 08 54