



Новейшие тренды и развитие DDoS-атак

Артем Избаенков

Директор по развитию направления Кибербезопасности

Член правления АРСИБ

Член ISDEF

Типы DDoS-атак по модели OSI

Layer 7

Application

OWASP Top 10 (e.g. XSS),
Slowloris, Slow Post/Read, HTTP
GET/POST floods

Layer 5, 6

Session, SSL, DNS, NTP

DNS UPD floods, DNS query floods,
DNS NXDOMAIN floods, SSL floods,
SSL renegotiation

Layer 1, 2, 3, 4

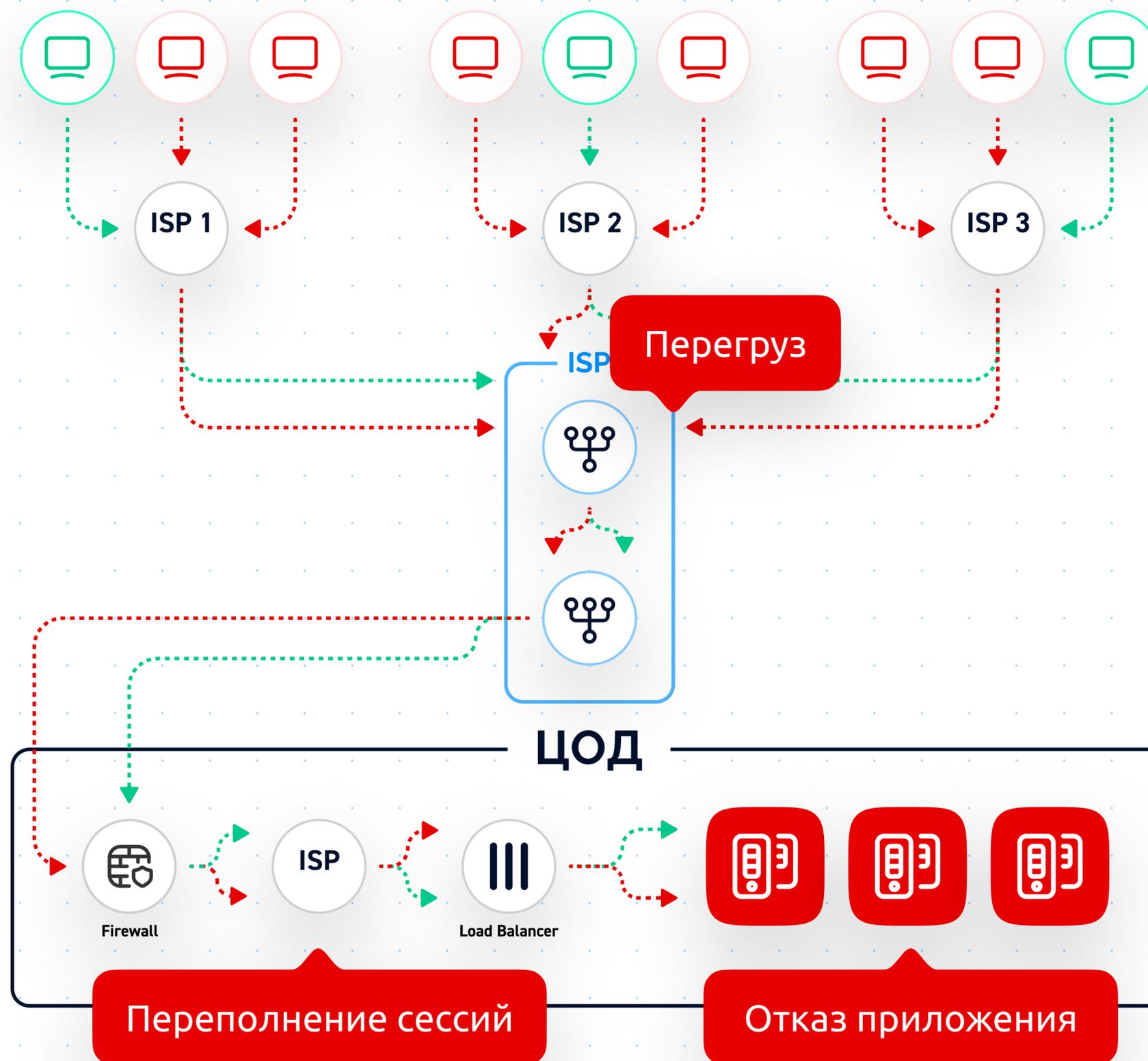
Network

SYN/UPD/Conn. floods,
PUSH and ACK floods,
ICMP/Ping floods,
Teardrop, Smurf Attacks

Сложность современных DDoS-атак

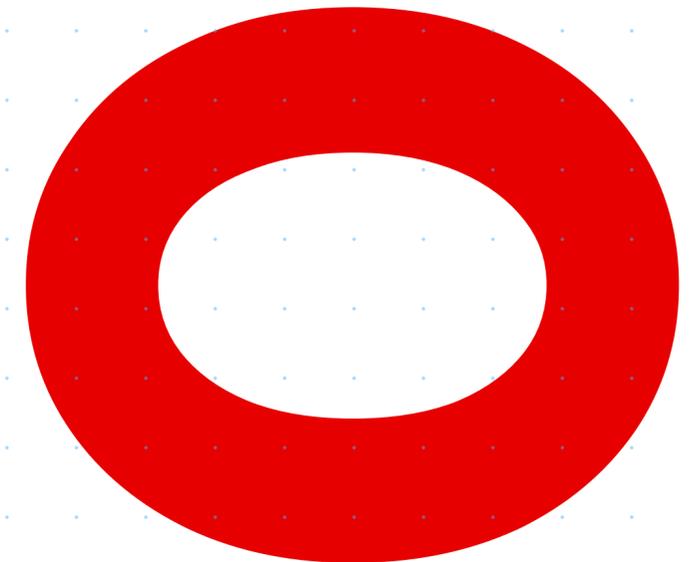
Сегодня DDoS можно разделить на 3 типа:

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



Тренды DDoS атак 2023

- Атаки уровня L7 (Приложения) на web инфраструктуру
- Целенаправленные атаки на DNS сервера компаний
- Объем 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
- Быстрое обновление новых зараженных устройств
- Атаки на API
- Ботнеты собирают на базе VDS/VPS



Кибервойна

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

Поиск уязвимостей

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

Искажённая аналитика

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

Брутфорс

Боты взламывают аккаунты с помощью автоматического перебора паролей.

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.

Кардинг

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

Скрейпинг

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

Скальперские покупки

Злоумышленники автоматически скупают ограниченный товар, чтобы перепродать его дороже.

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 DDoS атак, ботов и хакеров наших клиентов

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

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

Клиент

Интернет-аптека

Проблема

Боты собирали данные о товарах и ценах и специально замедляли работу сайта. Боты использовали открытый API для сбора аналитики.

Решение

Все парсеры данных - это автоматизированные процессы, поэтому подключение антибот системы отрубило их полностью. В защите от ботов использовали дополнительные метрики, чтобы детально выявлять и блокировать вредоносный трафик.

Клиент

Операционные офисы банка

Проблема

Злоумышленник вычислили автономную систему Банка и определили IP адреса, используемые для операционных офисов. Они направили распределенную DDoS атаку на все подразделения офиса одновременно, что парализовало 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.

Партнер

TrueConf

Проблема

Клиенты, приобретая ПО, разворачивают его в своей инфраструктуре или на внешнем виртуальном хостинге. Злоумышленники атакуют данные сервера, чтобы сорвать проведения важных ВКС и нанести репутационный урон.

Решение

Защита канальной части обеспечивается за счет построение GRE туннеля или L2VPN канала до сервера ВКС.

Далее, когда канал защищен, интегрируется веб-защита на уровне приложения от DDoS атак и ботов по технологии Reverse Proxy.

Клиент

Крупный call-центр на базе Asterisk

Проблема

Злоумышленники вычислили SIP сервера клиента, в момент важного мероприятия генерировали DDoS атаку по SIP протоколу скомпромитированными пакетами, дополняя атаку ботовой нагрузкой на веб-сайты.

Убытки более **10 млн рублей** за сутки в момент акции.

Решение

Предоставление защиты ИТ инфраструктуры клиента с возможностью фильтрации вредоносных запросов в SIP протоколе.

Дополнительно подключение антибот системы к веб сайтам компании,



EDGE
ЦЕНТР



edgecenter.ru

8 800 775 08 54