EDGE ЦЕНТР

Sk Сколково

АРПП Отечественный софт

2023: Кибервойна и вызовы в DDoS

Артём Избаенков

Директор по развитию направления кибербезопасности

Член правления АРСИБ

Член РОЦИТ

Член ISDEF

Тренды DDoS-атак в 2023/2024

1. Атаки уровня L7 (приложения) на веб-инфраструктуру
2. Целенаправленные атаки на DNS-серверы компаний
3. Объём атак ботнетов на РФ перёшел границу в **1,2 Тбит/с и более 500 Mpps**
4. Рост мощности и длительности атак **до >1 Тбит/с и >10 дней**
5. Существенную долю составляют боты из РФ
6. Использование облачных ЦОДов для организации и монетизации DDoS-атак
7. «Ковровые» атаки на инфраструктуру

EDGE ЦЕНТР

Клиент

Одна космическая компания

Проблема

После значимых событий в компании, хактивисты решили использовать DDoS-атаку для манипулирования общественным мнением.

Хактивисты организовали DDoS-атаку на сайты и инфраструктуру компании, пытаясь не допустить публикации официальной информации в интернете от лица компании.

Решение

Постоянный мониторинг трафика, защита инфраструктуры и каналов связи в совокупности с защитой веб-приложений, позволило обеспечить стабильную работу всех сервисов даже во время атаки.

EDGE ЦЕНТР

Клиент

Сервис бронирования авиабилетов

Проблема

Целью хактивистов было вывести из строя работу авиакомпаний.

Случайным образом одной из целей стала система регистрации онлайн бронирования.

Успешная атака парализовала работу аэропортов и привела к огромным убыткам.

Решение

Проблема решена срочной организацией защищенного интернет-канала.

Перемаршутизировали трафик через защищённый BGP стык на серых адресах, чтобы зафильтровать атаку. Также были построены дополнительные резервные стыки.

Клиент

Агрегатор e-mail рассылки

Проблема

Хактивисты нацелились на один крупный e-com, на части доменов которого находился сервис агрегатора рассылок.

Сервис оказался под массированной атакой, которая заблокировала треть рассылок по РФ для государственных и бизнес-структур.

Решение

В срочном порядке организовали стык.

Перемаршрутизировали трафик через защищённый BGP стык на серых адресах, чтобы зафильтровать атаку.
Также были построены дополнительные резервные стыки.

Защита веб-приложений была организована в течение 1–2 часов после начала атаки.

Клиент

ТОП СМИ

Проблема

SEO оптимизация сайта стала ухудшаться.

По определённым поисковым запросам касательно СВО сайт находился даже не в топ-10 ссылок.

Была выявлена ботовая активность, направленная на ухудшение поисковых позиций сайта со стороны Хактивистов.

Решение

Был вычислен ботнет в Новосибирске, который использовал **более 4 000** виртуальных машин и уникальных IP-адресов из РФ.

Работа ботнета заключалась в малоактивном посещении определённых статей сайта, что снижало его SEO и понижало рейтинг сайта для поисковых систем, выводя зарубежные ресурсы в топ.

Ботнет заблокировали с помощью системы Антибот. Организаторы были найдены.

Клиент

Правительственный ЦОД

Проблема

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

Решение

Проведено стресс-тестирование, предоставлен отчёт об уязвимостях. Разработано совместное решение на базе двух независимых операторов с защитой от DDoS-атак.

Планируется размещение очистителей непосредственно в регионе.

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

Крупный оператор связи Москвы

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

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

Кубок CTF России

Проблема

Мероприятие проводится on-line. Платформа содержит дашборд для подачи правильных ответов - флагов и некоторое количество серверов, на которых лежат задания. Злоумышленники организовывали DDoS атаки ботами с плавающими даннами на дашборд, паралельно атакую рабочие порты заданий на серверах

Решение

Обучение трафику мобильного API на основном дашборде и включение системы Антибот предварительно, позволило отразить атаку 20 млн RPM. Для отражения атаки на порты заданий на сервере, были выделены защищенные виртуальыне мощности в облаке, где возможна фильтрация L4 шифрованного трафика и L7 не шифрованного без передачи SSL ключей для всего диапозона портов.

Клиент

Международный грузоперевозчик

Проблема

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

Решение

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

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

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.

Клиент

Крупный call-центр на базе Asterisk

Проблема

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

Убытки более **10 млн рублей** за сутки в момент важного события.

Решение

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

Дополнительно подключение антибот системы к веб сайтам компании,

Клиент

Букмекерская компания

Проблема

Компании требовалась защита корпоративных офисов, порталов и Битрикса.

Решение

Мы настраивали защиту параллельно с разработкой сайта.

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

Клиент

Один крупный грузопассажирский перевозчик

Проблема

ИТ Армия Украины пыталась нарушить пассажирские перевозки. Произведена успешная бот атака на систему онлайн бронирования. Пассажиры не могли в течении суток оформить билеты.

Решение

Через сутки обратился клиент для решения проблемы. Аналитики произвели анализ в течении 15 мин и разработали правила для отражения бот-атаки. Атака была отражена

EDGE ЦЕНТР

edgecenter.ru

8 800 775 08 54