DDOS-атаки на инфраструктуру оператора ЭДО

Александр Тупицын

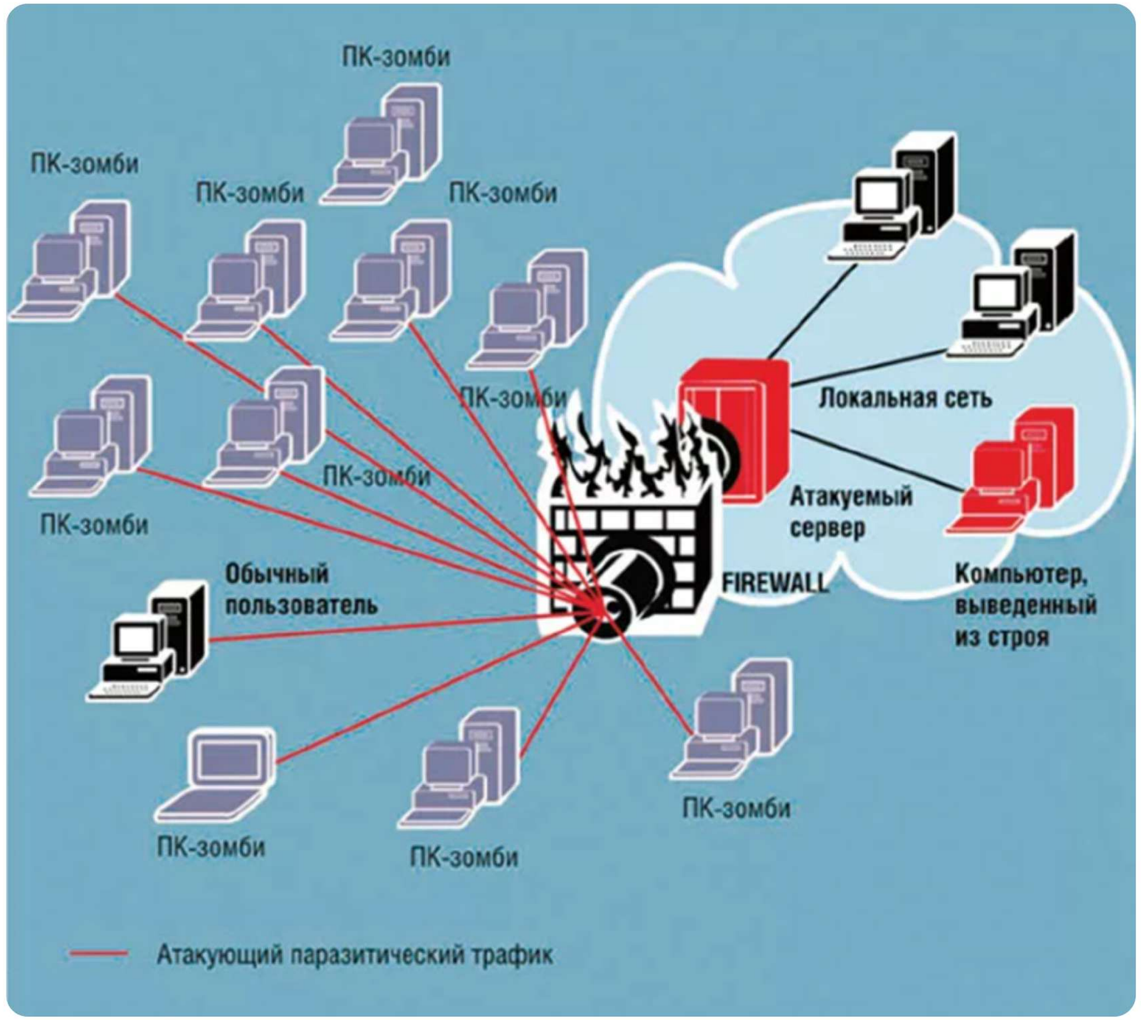
технический директор

Что такое DDOS-атака

DDOS-атака — лавинообразный рост количества запросов к ресурсам

Часто участники атаки даже не подозревают о своем участии. Включение участника производится через вредоносное ПО

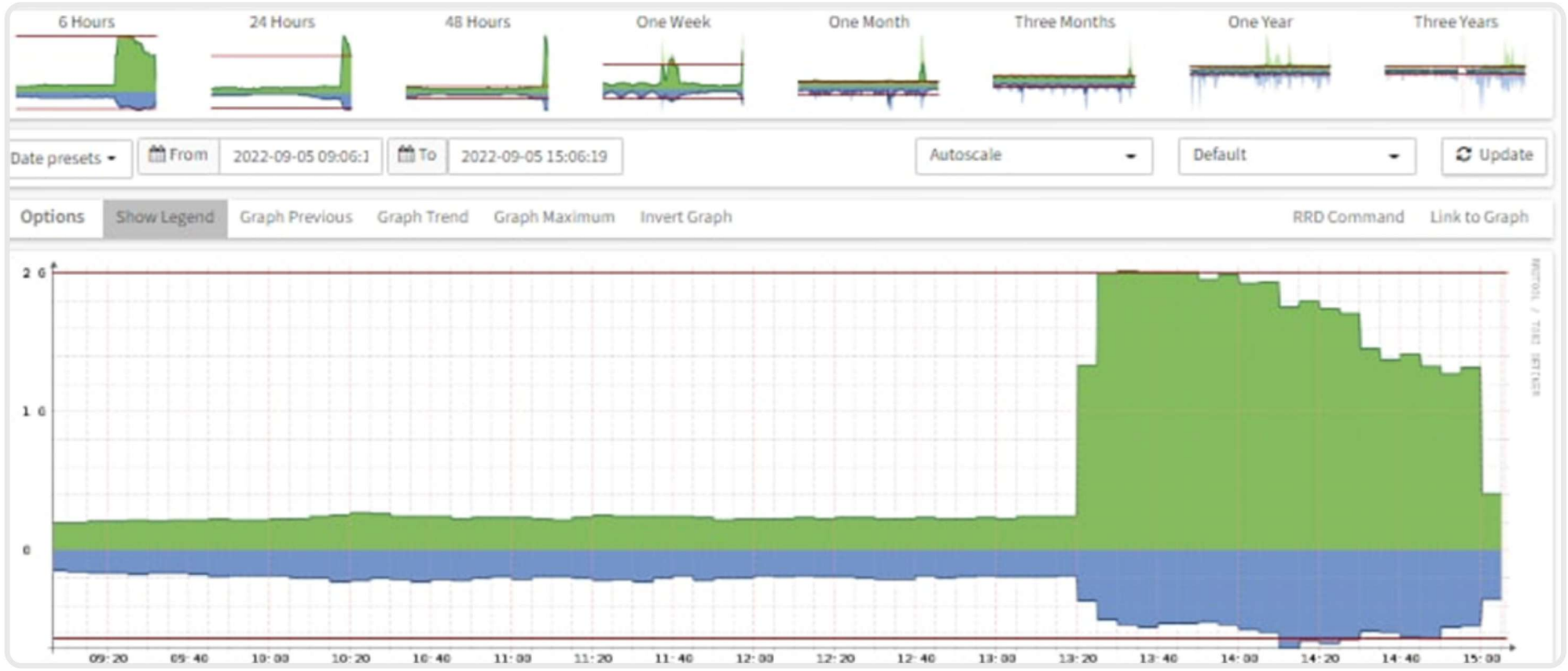
Атака может выводить из строя или существенно ограничивать как доступ к каким-то ресурсам, так и просто пропускную способность канала связи для полезного трафика



Реальный пример – 05.09.2022

Вредоносный трафик полностью загрузил канал доступа в ЦОДе

Для полной загрузки потребовалось несколько минут



Меры защиты. Внутренние

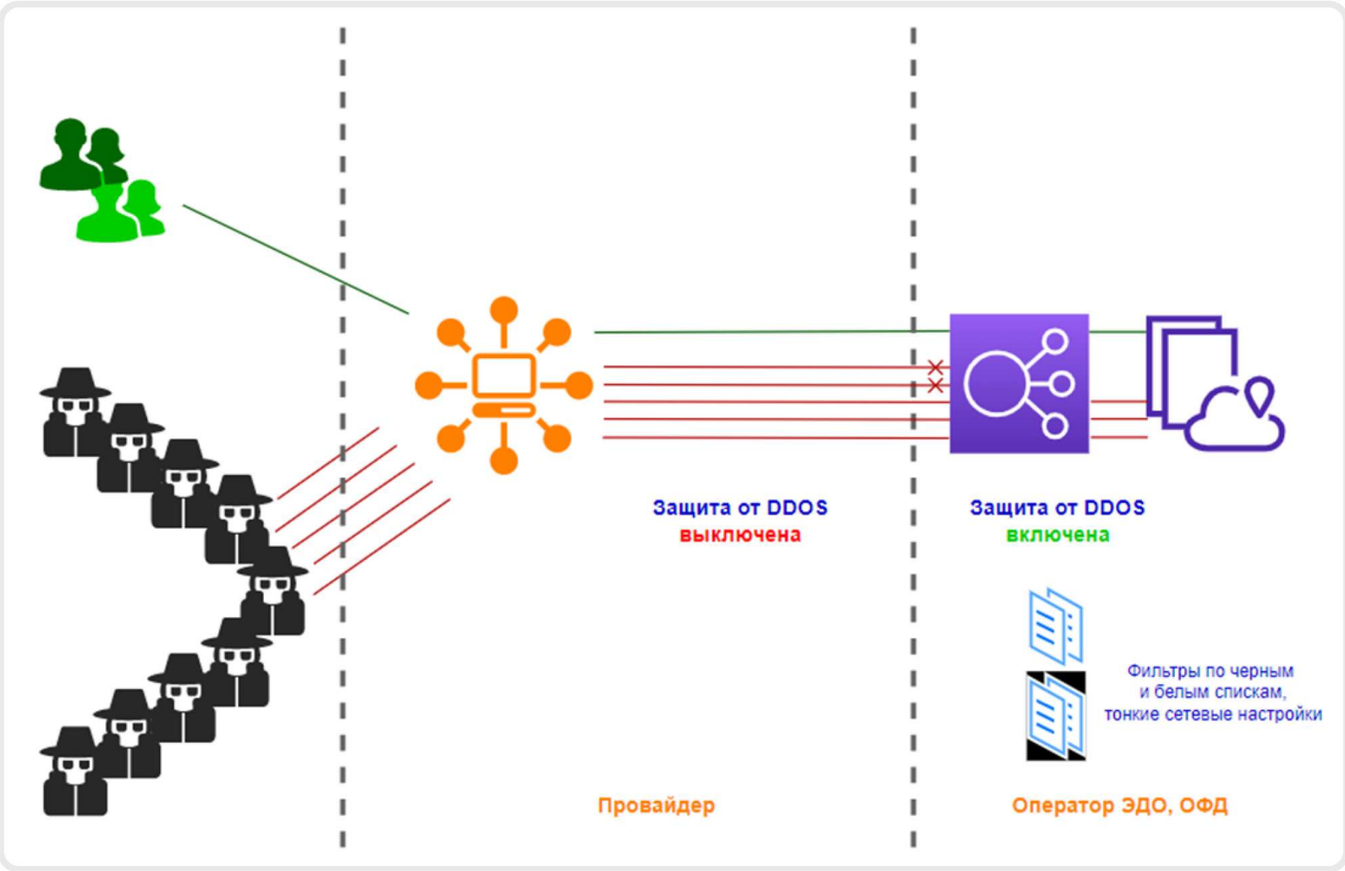
Весь входящий трафик попадает на пограничные межсетевые экраны в ДМЗ сегменте сети

В локальной сети развернута система обнаружения вторжений (DLP) и антивирусная защита данных

На межсетевом экране действует фильтрация по принудительному закрытию вредоносных сессий по ряду признаков

Трафик дополнительно проходит через внутреннюю систему анализа и фильтрации

На её основе формируется «черный список» адресов, которые подвергаются блокировке. Отдельно ведется и «белый список», исключающий блокировку легитимного трафика



Меры защиты. Внешние

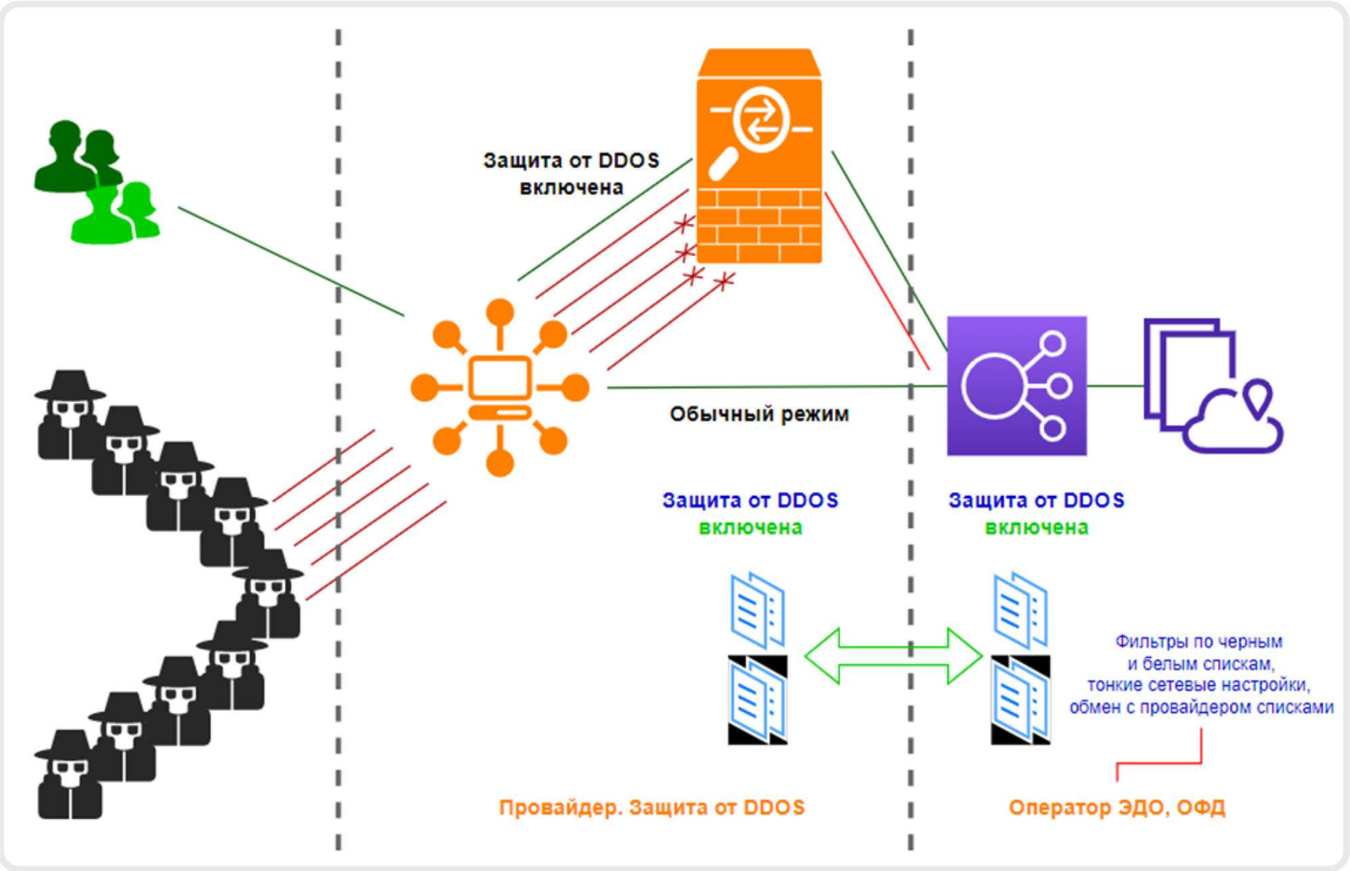
Дополнительно к внутренним мерам подключаются меры защиты от внешнего провайдера, сетевого или специализированного

Использование ресурсов внешнего провайдера более эффективно за счёт специализированного оборудования и более «широких» каналов.

Весь трафик заворачивается на специализированное оборудование провайдера, где производится его «очистка» различными методами.

Также включается обмен чёрными и белыми списками между провайдером и оператором

Очищенный (полезный) трафик с «примесью» паразитного поступает оператору



Как получить доступ и не попасть в фильтры.

Что фильтрует ресурс под DDOS-атакой = как не попасть в фильтры.

Для добросовестного пользователя основную угрозу представляют следующие фильтры:

Фильтр геолокации

Включается в первую очередь.
Блокируются все ip-адреса,
не зарегистрированные на территории России. Это самый эффективный фильтр, отсекающий 50-80% паразитного трафика.

Проверьте (через системного администратора), что ваш маршрут к ресурсу провайдера проходит через Россию. Смените маршрут или сообщите свой адрес оператору ЭДО для внесения в белый список

Черный список

IP-адрес, с которым вы выходите в интернет по каким-то причинам мог попасть в черный список у провайдера или у оператора ЭДО.

Проверьте (через системного администратора) доступность ресурса из другой сети (из дома, с мобильного телефона, из другого офиса и т.п.). Если с другого адреса ресурс доступен, то проблема с вашим IP-адресом. Смените адрес или сообщите его оператору ЭДО для внесения в белый список.

DDOS атаки на инфраструктуру Оператора ЭДО

Александр Тупицын

tav@taxcom.ru