

DDOS для руководителя

Взгляд с неожиданной стороны



Москва, 20.09.2017

КТО Я ?

Образование

*окончил МИФИ в 2006 году
факультет «Информационная
безопасность»*

*специалист по информационной
безопасности банковских систем*

Опыт работы

более 12 лет в банке ТОП-3 РФ

более 16 лет в сфере ИБ

*5 лет – сетевая безопасность,
администрирование технических
средств защиты, противодействие
сетевым атакам, проведение
расследований и устранение
последствий вредоносных
воздействий на инфраструктуру*

Алексей Плешков

Кому адресовано выступление

- Сотрудники ИБ и СБ финансовых организаций
- Сетевые инженеры и администраторы
- Руководители ИБ и ИТ направлений

Моя задача-тах на сегодня

Предоставить дополнительные аргументы в общении с руководством, которое не понимает критичности DDOS, его последствий и не знает, зачем от него защищаться.

Чего не будет в презентации?

- Ответов на типовые вопросы
- Классификаций DDOS
- Обсуждения коммерческих решений и названий продуктов
- Рецептов на все случаи жизни
- Рекламы

РЕЙТИНГ «ЖЕРТВ» ПО СПЕЦИАЛИЗАЦИИ РЕСУРСА
(по процентному соотношению количества атак на ресурс)



Во втором квартале замечено значительное усиление атак на интернет-магазины и игровые проекты. Это можно объяснить тем, что весной, в преддверии отпусков, люди больше тратят времени на шоппинг, соответственно, усиливаются и DDoS-атаки в это время

DDOS стал еще доступнее

Яндекс заказать ddos атаку - 365 тыс. ответов

Яндекс заказать ddos атаку недорого - 218 тыс. ответов

Яндекс order ddos attack - 706 тыс. ответов

ip/домен:

Сканер портов

Скан портов -

Открытые порты

Сканируется порт

Сканировать

DOS

порт

интервал соединений

Потоков

Максимум соединений

Убить

Соединений 0

Пик 0

Неудач 0

TCP сообщения

интервал

сообщение

Отправлено

Отправлять tcp

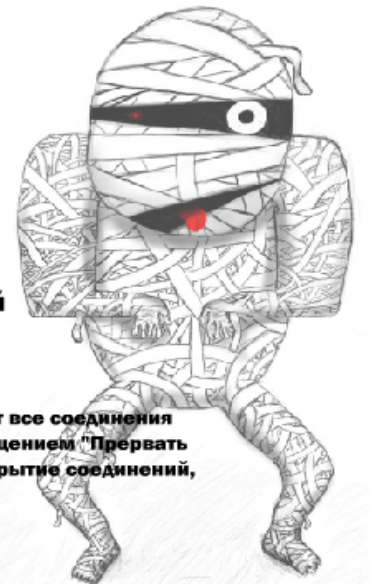
dos циклом

Открыть соединений

Открыть

Программа будет висеть пока не откроет все соединения в процессе может открыться окно с сообщением "Прервать сценарий", если вы хотите продолжить открытие соединений, жмите "нет"

Интеллект. дос



happy-hack.ru

DDOS vs нагрузочное тестирование

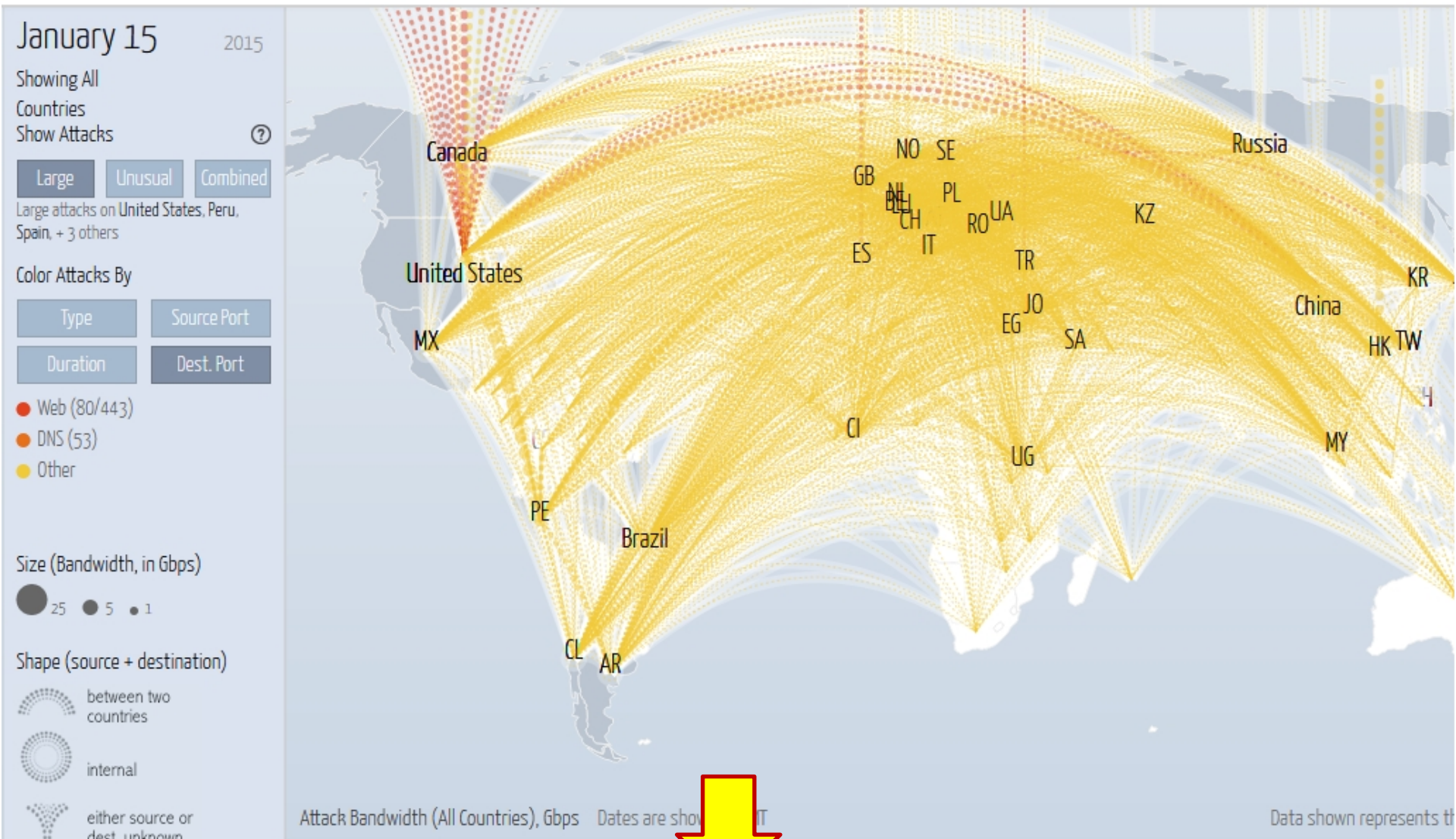
- Online бесплатные сервисы нагрузочного тестирования
- Бот-неты
- Аренда облачного сервиса
- Платные сервисы на коммерческой основе

Каков будет выбор хакеров злоумышленников?

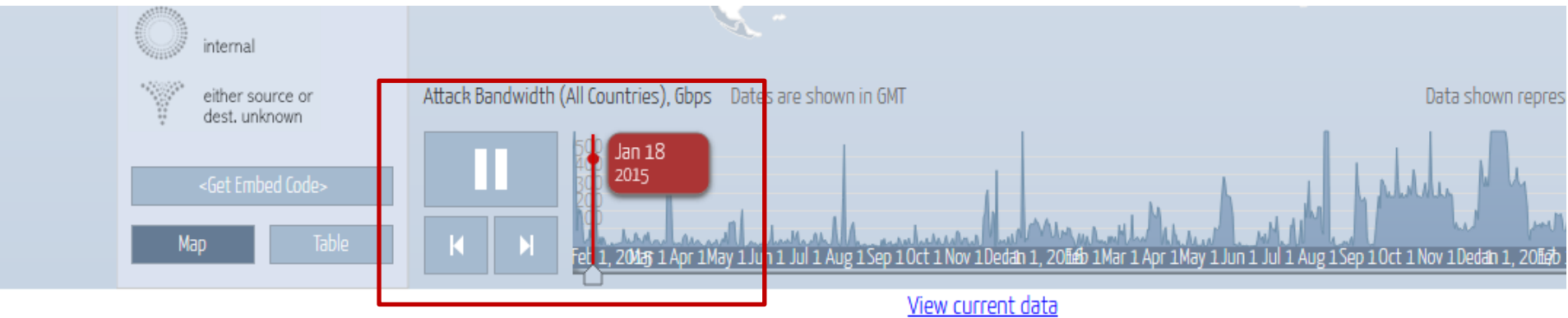
source: Digitalattackmap.com

Digital Attack Map Top daily DDoS attacks worldwide

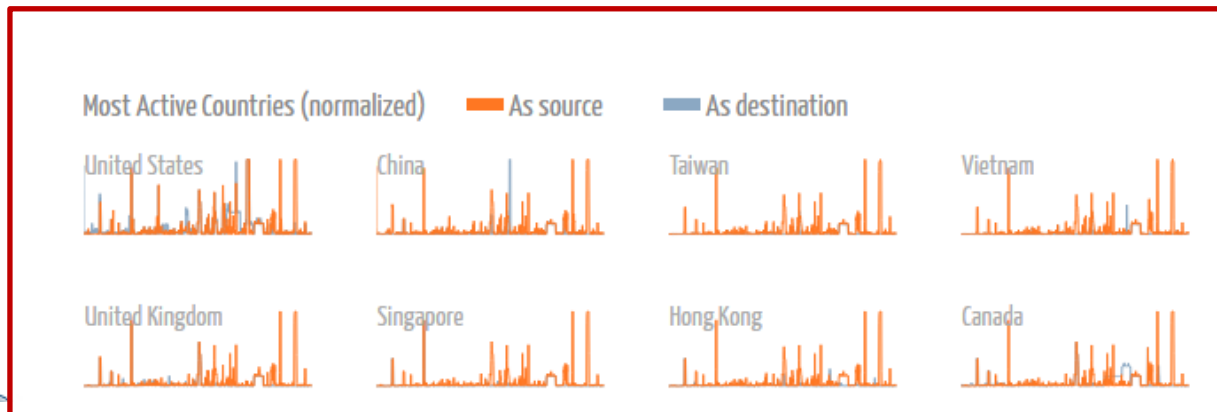
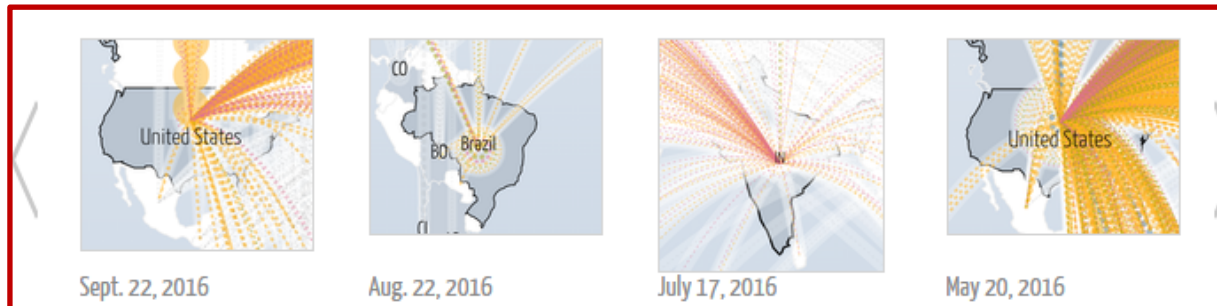
[Map](#) · [Gallery](#) · [Understanding DDoS](#) · [FAQ](#)



source: digitalattackmap.com



Notable Recent Attacks — [Explore the gallery](#)



Web & News Results (Sep 18 - 20)

[Hacked home devices caused massive Internet o](#)
[www.usatoday.com](#) - Oct 21, 2016

Attackers used a leaked code to launch DDoS at
The attack hit the Dyn server that contains that a

[Examining the FCC claim that DDoS attacks hit](#)
[arstechnica.com](#) - May 23, 2017

Attacks came from either an unusual type of DDoS
bots.

[Today's Brutal DDoS Attack Is the Beginning of a](#)
[gizmodo.com](#) - Oct 21, 2016

Today's Brutal DDoS Attack Is the Beginning of a
able to solve the problem of being hit with a huge

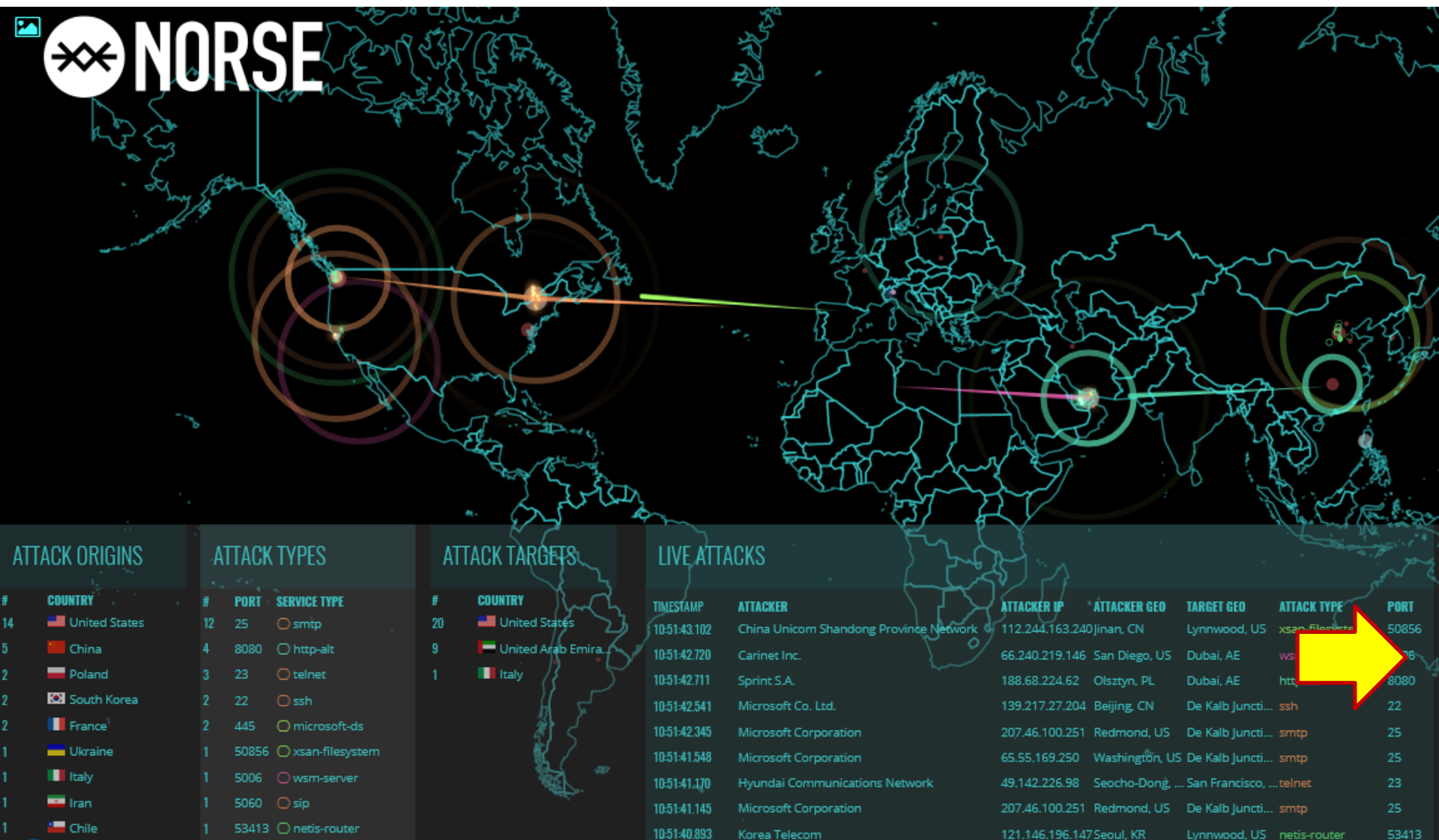
[FCC has no documentation of DDoS attack that](#)
[arstechnica.com](#) - Jul 20, 2017

Examining the FCC claim that DDoS attacks hit
appeal or to a followup e-mail we sent on Tuesda

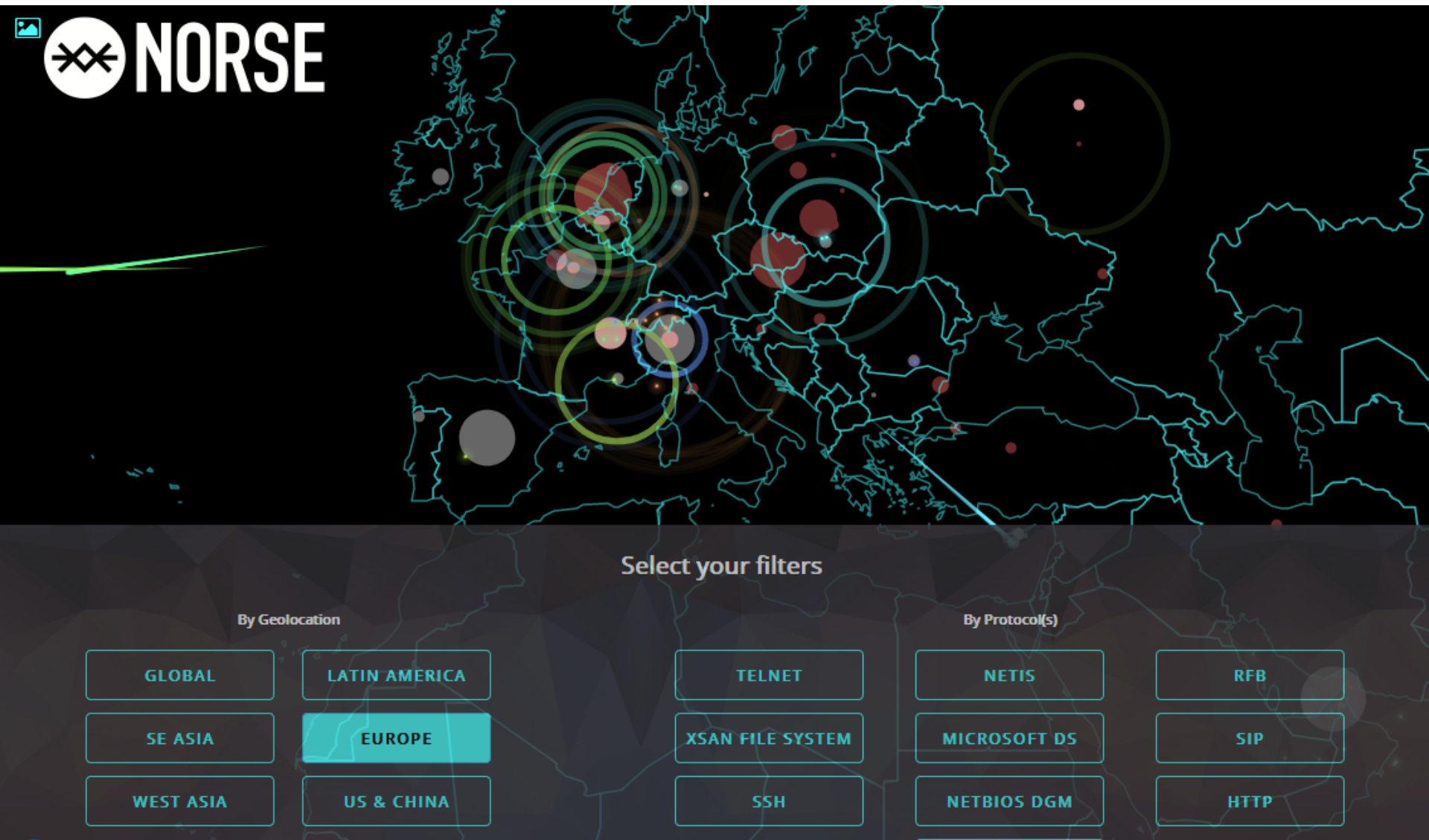
[FCC Claims It Was Hit by Denial Of Service Atta](#)
[gizmodo.com](#) - May 8, 2017

"Beginning on Sunday night at midnight, our anal
was subject to multiple distributed denial-of-serv

source: map.norsecorp.com



source: map.norsecorp.com



Управляем риском DDOS

1. Снижаем (за счет покупки/оплаты компенсационных мер)
2. Делегируем (возлагаем по договору на провайдера)
3. Страхуем (оплачиваем покрытие)
4. Принимаем (письменно, на уровне руководства)
5. ~~Не рассматриваем.~~

Серебряной пули.net

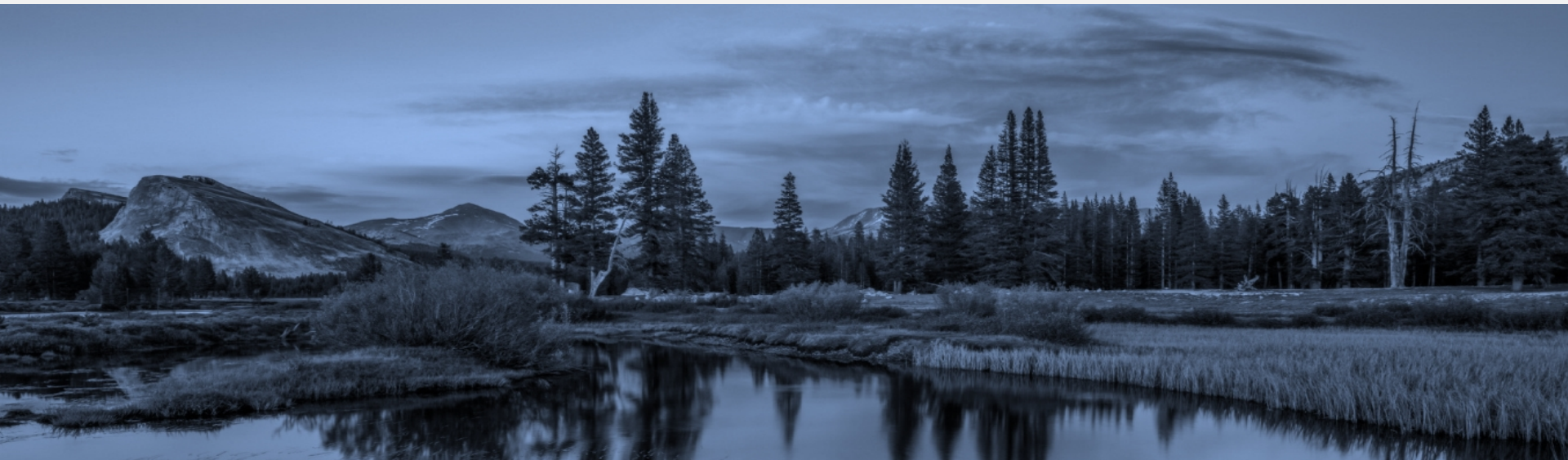
1> Риски DDOS на Вашу инфраструктуру > 0

Если злоумышленники задались целью совершить DDOS атаку – совершат

Гарантированной защиты от DDOS на рынке в природе не существует

Нужно ли Вашей организации тратить деньги на защиту от DDOS?

Благодарю за внимание!



Готов ответить на Ваши вопросы