Направление подготовки бакалавров
090301 «Информатика и вычислительная техника»

DoS и DDoS атаки

Караваева Ольга Владимировна

ВЯТСКИЙ
ГОСУДАРСТВЕННЫ
УНИВЕРСИТЕТ

DoS и DDoS атаки

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Проблема

Internet и информационная безопасность несовместны по самой природе Internet. Эта сеть родилась как чисто корпоративная сеть, однако, в настоящее время с помощью единого стека протоколов TCP/IP и единого адресного пространства объединяет не только корпоративные и ведомственные сети (образовательные, государственные, коммерческие, военные и т.д.), являющиеся, по определению, сетями с ограниченным доступом, но и рядовых пользователей, которые имеют возможность получить прямой доступ в Internet со своих домашних компьютеров с помощью модемов и телефонной сети общего пользования.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Проблема

Как известно, чем проще доступ в Сеть, тем хуже ее информационная безопасность.
Платой за пользование Internet является всеобщее снижение информационной безопасности.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

DoS и DDoS атаки

В области информации дилемма безопасности формулируется следующим образом: следует выбирать между защищенностью системы и ее открытостью. Правильнее, впрочем, говорить не о выборе, а о балансе, так как система, не обладающая свойством открытости, не может быть использована.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

DoS и DDoS атаки

DoS-атака *(атака типа «отказ в обслуживании», от англ. Denial of Service)* — атака на вычислительную систему с целью довести её до отказа, то есть создание таких условий, при которых легитимные (правомерные) пользователи системы не могут получить доступ к предоставляемым системой ресурсам (серверам), либо этот доступ затруднён.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

DoS и DDoS атаки

Отказ «вражеской» системы может быть и шагом к овладению системой (если во внештатной ситуации ПО выдаёт какую-либо критическую информацию — например, версию, часть программного кода и т. д.). Но чаще это мера экономического давления: простои службы, приносящей доход, счета от провайдера и меры по уходу от атаки ощутимо бьют «цель» по карману.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

DoS и DDoS атаки

Все DDoS-атаки, классифицируя их по целям, можно разделить на следующие группы:

Атаки, целью которых является перегрузка полосы пропускания. Примерами атак этого типа могут служить уже упоминавшийся выше UDP-флуд, ICMP-флуд (он же пинг-флуд), и другие практики рассылки пакетов, которые не запрашивались. Сила таких атак измеряется в гигабитах в секунду. Она постоянно увеличивается и сейчас может составлять до 100 и более гигабит в секунду.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

DoS и DDoS атаки

Атаки на уровне протоколов. Как и следует из названия, атаки этого типа используют ограничения и уязвимости различных сетевых протоколов. Они «бомбардируют» сервер паразитными пакетами,и он становится неспособным обработать запросы легальных пользователей. В качестве примера можно привести SYN-flood, teardrop и другие атаки, нарушающие нормальное движение пакетов внутри протокола на разных стадиях.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

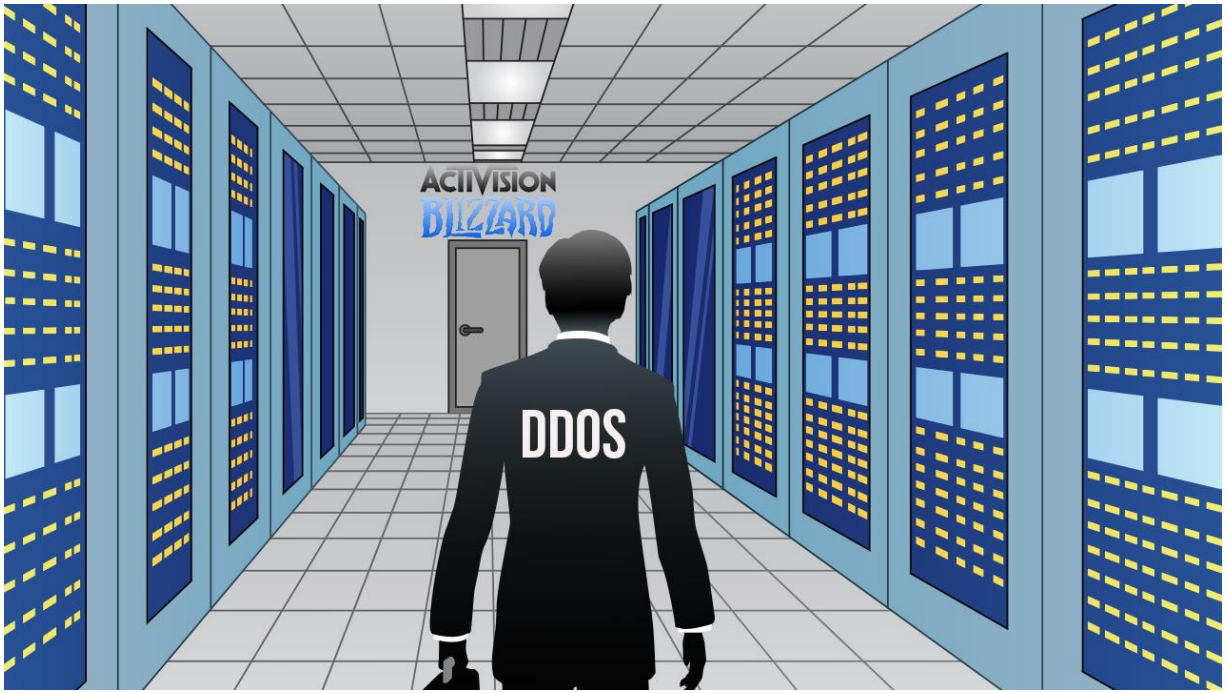
DoS и DDoS атаки

Атаки на уровне приложений, которые нарушают нормальное функционирование системы, используя уязвимости и слабые места приложений и операционных систем. Эти атаки незаметны для стандартных анализаторов, так как составляют порой до 1 Kpps. Стандартные меры защиты не могут выявить столь мелкий всплеск трафика, следовательно для защиты требуется всегда постоянная фильтрация и комплекс очистки всегда должен знать алгоритмы работы самого приложения.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

DoS и DDoS атаки

Если атака выполняется одновременно с большого числа компьютеров, говорят о **DDoS-атаке** *(от англ. Distributed Denial of Service, распределённая атака типа «отказ в обслуживании*



ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

DoS и DDoS атаки

В некоторых случаях к фактической DDoS-атаке приводит непреднамеренное действие, например, размещение на популярном интернет-ресурсе ссылки на сайт, размещённый на не очень производительном сервере (слэшдот-эффект). Большой наплыв пользователей приводит к превышению допустимой нагрузки на сервер и, следовательно, отказу в обслуживании части из них.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

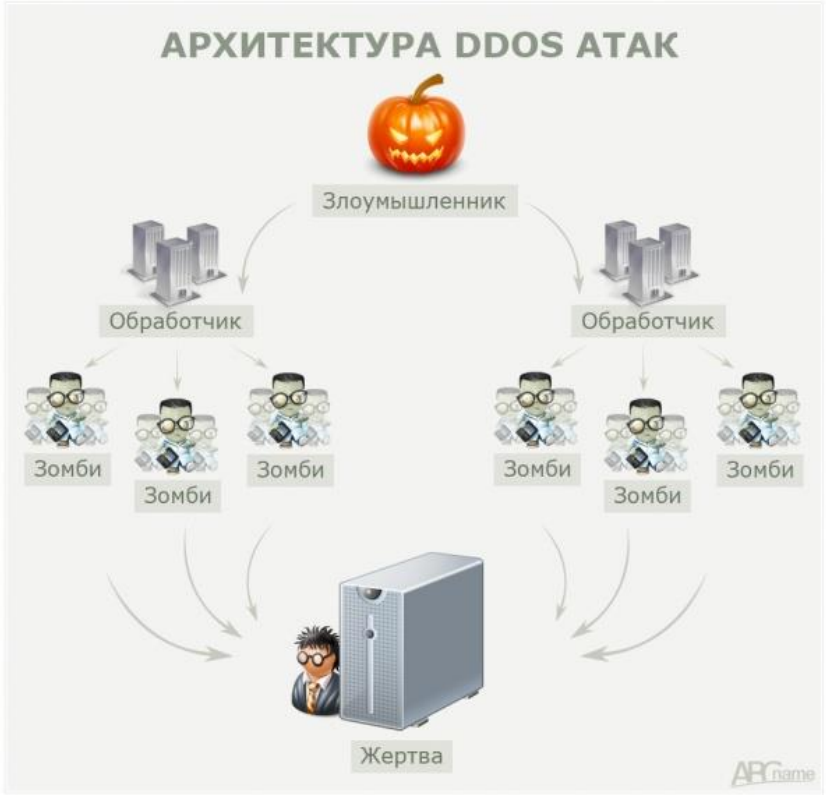
DoS и DDoS атаки

Существуют различные причины, из-за которых может возникнуть DoS-условие:

* *Ошибка в программном коде*, приводящая к обращению к неиспользуемому фрагменту адресного пространства, выполнению недопустимой инструкции или другой необрабатываемой исключительной ситуации, когда происходит аварийное завершение программы-сервера — серверной программы.).

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

DoS и DDoS атаки



Классическим примером является обращение по нулевому (англ. null) адресу. Недостаточная проверка данных пользователя, приводящая к бесконечному либо длительному циклу или повышенному длительному потреблению процессорных ресурсов (вплоть до исчерпания процессорных ресурсов) либо выделению большого объёма оперативной памяти (вплоть до исчерпания доступной памяти).

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Модели атак

Распределенные атаки основаны на "классических" атаках типа «отказ в обслуживании", а точнее на их подмножестве, известном как ***Flood-атаки*** или ***Storm-атаки***.

Смысл данных атак заключается в посылке большого количества пакетов на атакуемый узел.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

DoS и DDoS атаки

* *Флуд* (англ. flood — «наводнение», «переполнение») — атака, связанная с большим количеством обычно бессмысленных или сформированных в неправильном формате запросов к компьютерной системе или сетевому оборудованию, имеющая своей целью или приведшая к отказу в работе системы из-за исчерпания системных ресурсов — процессора, памяти или каналов связи.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

DoS и DDoS атаки

* Атака второго рода — атака, которая стремится вызвать ложное срабатывание системы защиты и таким образом привести к недоступности ресурса.

Если атака (обычно флуд) производится одновременно с большого количества IP-адресов — с нескольких рассредоточенных в сети компьютеров — то в этом случае она называется распределённой атакой на отказ в обслуживании (DDoS).

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Типы флуда

Флуд – это информация, не несущая смысловой нагрузки. В контексте DoS/DDoS-атак флуд представляет собой лавину пустых, бессмысленных запросов того или иного уровня, которые принимающий узел вынужден обрабатывать.

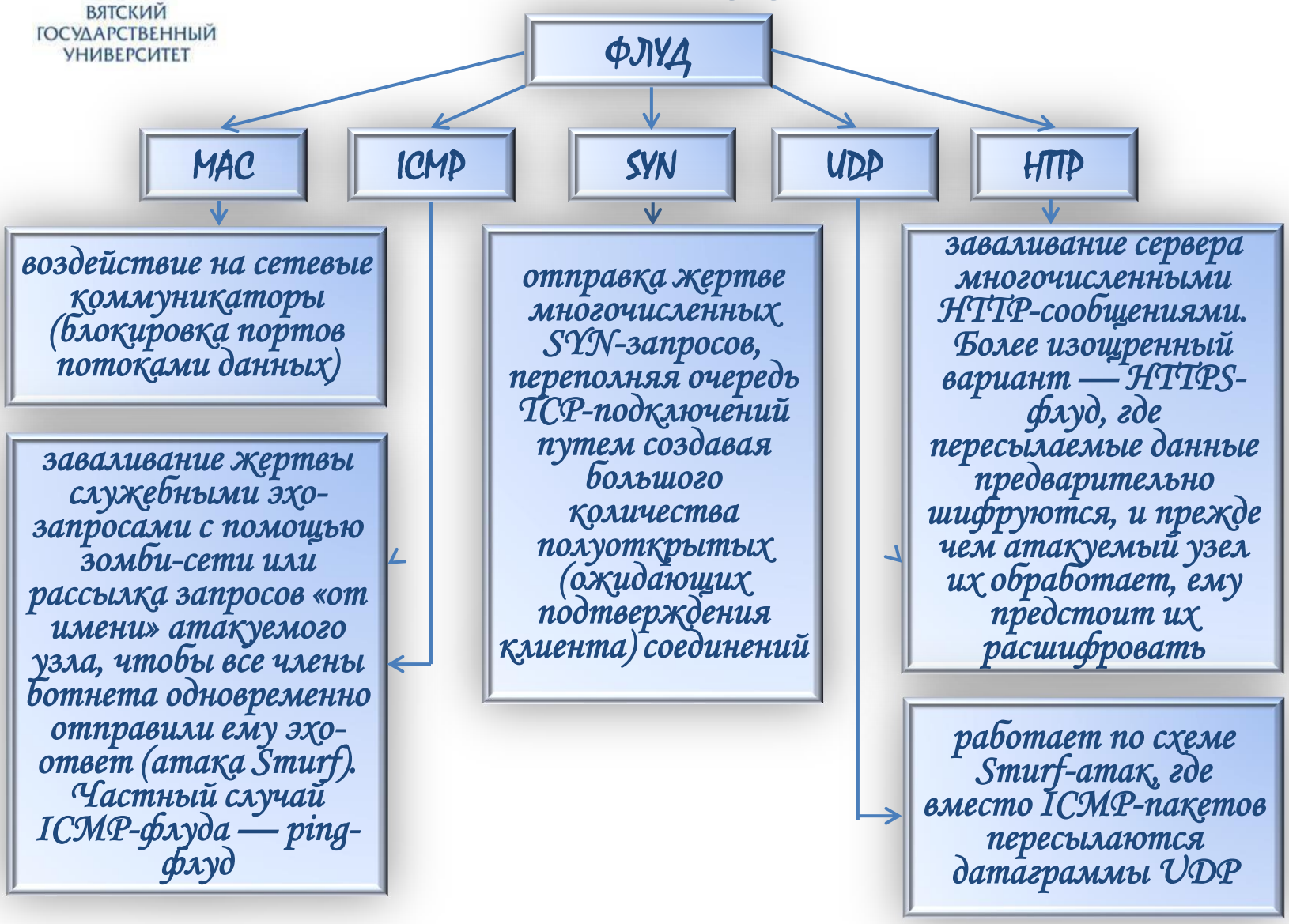
ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Типы флуда

Основная цель использования флуда — полностью забить каналы связи, насытить полосу пропускания до максимума.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Модели атак



ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Storm-атаки

Storm засылает не «мусорные» пакеты, а бессмысленные URL-запросы.

Создателям Storm удалось уже создать исполинскую бот-сеть, количество заражённых компьютеров в которой может составлять, по некоторым оценкам, до 50 миллионов, — а это значит, что вычислительная мощь такой бот-сети превосходит даже самые мощные суперкомпьютеры.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Storm-атаки

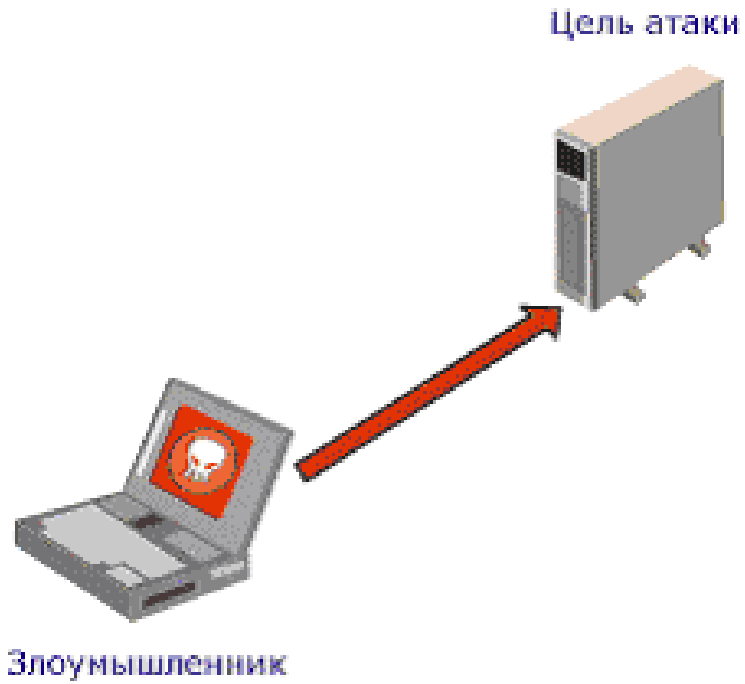
Троян Storm (он же Peed, он же Peacomm, он же NuWar, он же Zhelatin) предположительно имеет российское происхождение, — во всяком случае, так утверждает фирма MessageLabs.

Вирус довольно старый, однако время от времени антивирусные компании фиксируют резкие всплески его активности, как правило, вследствие массовых рассылок, осуществляемых злоумышленниками

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Модели атак

Традиционная модель атаки строится по принципу «один к одному» или «один ко многим» т.е. атака исходит из одного источника.



ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Модели атак

В отличие от традиционной модели в распределенной модели используются отношения

«многие к одному» и «многие ко многим»

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Модели атак

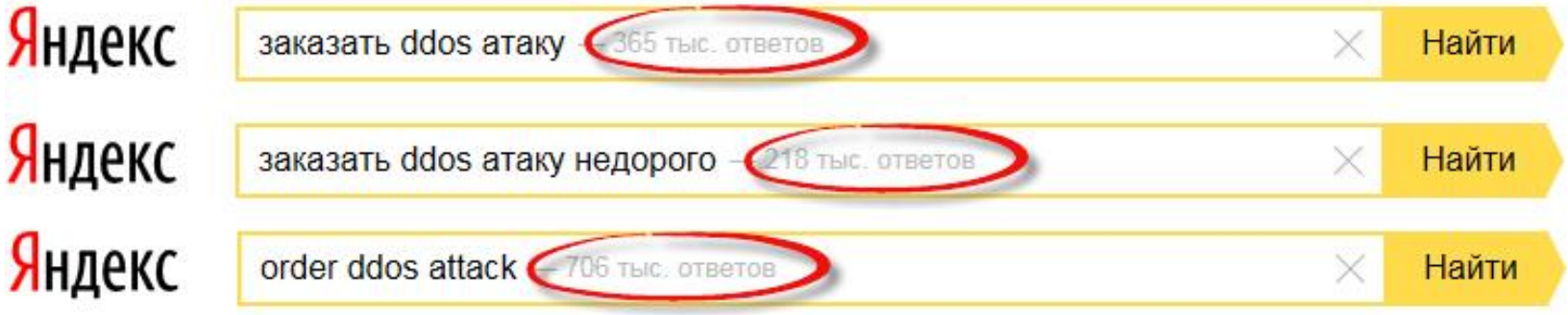
По такому принципу работают атаки SYN-Flood, Smurf, UDP Flood, Targa3 и т.д.

Но если пропускная способность канала до атакуемого узла превышает пропускную способность атакующего или атакуемый узел некорректно сконфигурирован, то к "успеху" такая атака не приведет.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

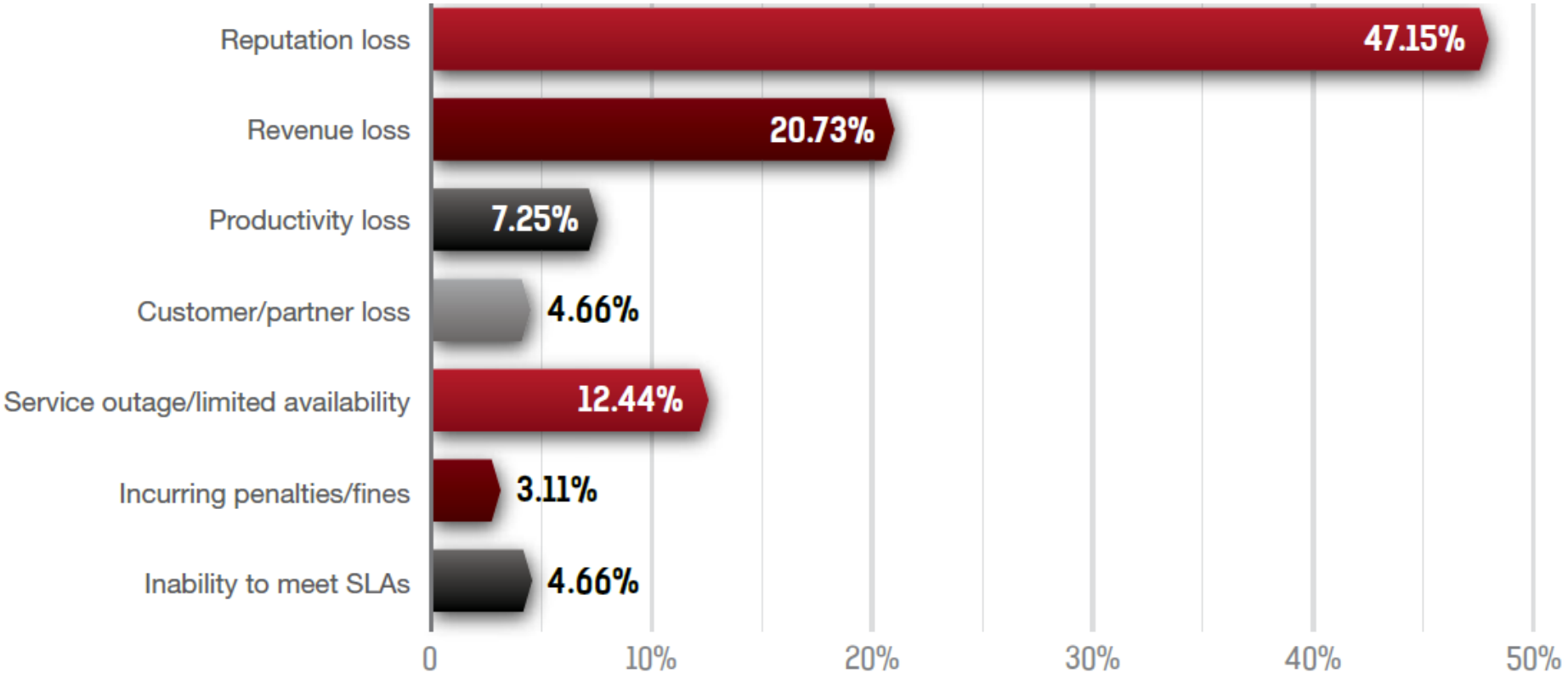
Модели атак

DDoS стал методом нечестной конкурентной борьбы, получившим широкое распространение ввиду именно простоты его использования. Существует огромное число организаций, предлагающих DDoS как услугу, по сути, облачный и недорогой сервис. Сервис предоставляется на хорошем профессиональном уровне, и оплата может браться только в случае успешной атаки. Так что не так уж и сложно будет уничтожить любой бизнес с помощью ИТ.



ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Потери от DoS/DDoS атак



SLA – Service Level Agreement (соглашение об уровне обслуживания).

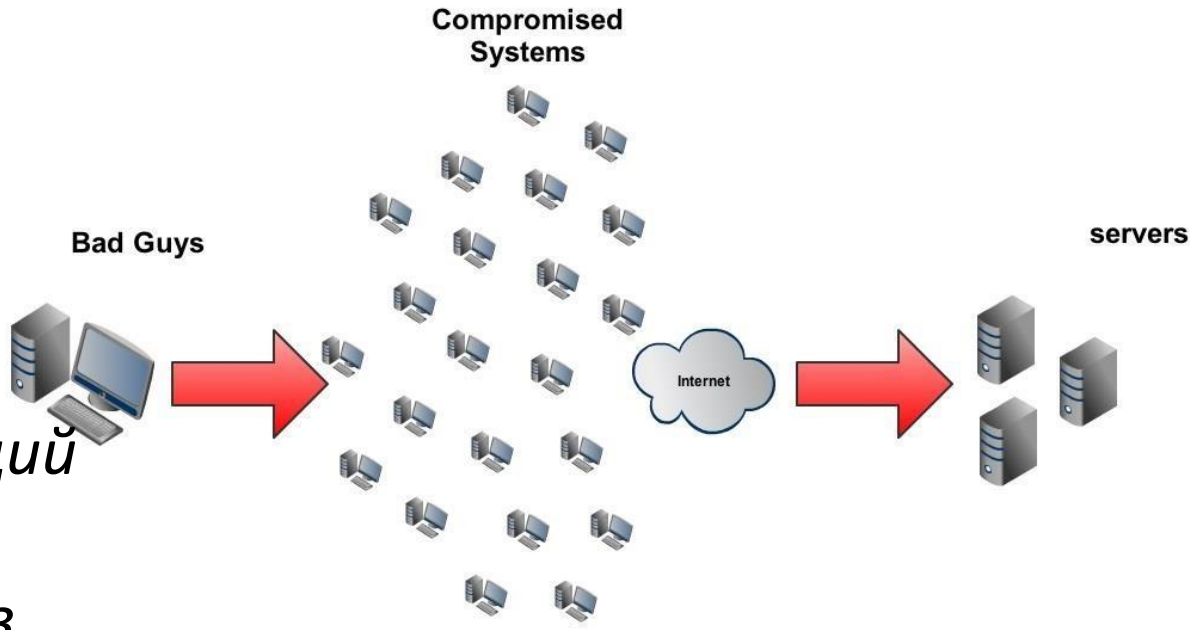
ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Данные исследования «Информационная безопасность бизнеса 2014» лаборатории Касперского.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Модели атак

По данным опроса компании [HaltDos](), DDoS-атаки рассматриваются половиной организаций как одна из самых серьезных киберугроз.



Опасность DDoS даже выше, чем опасность несанкционированного доступа, вирусов, мошенничества и фишинга, не говоря о прочих угрозах.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

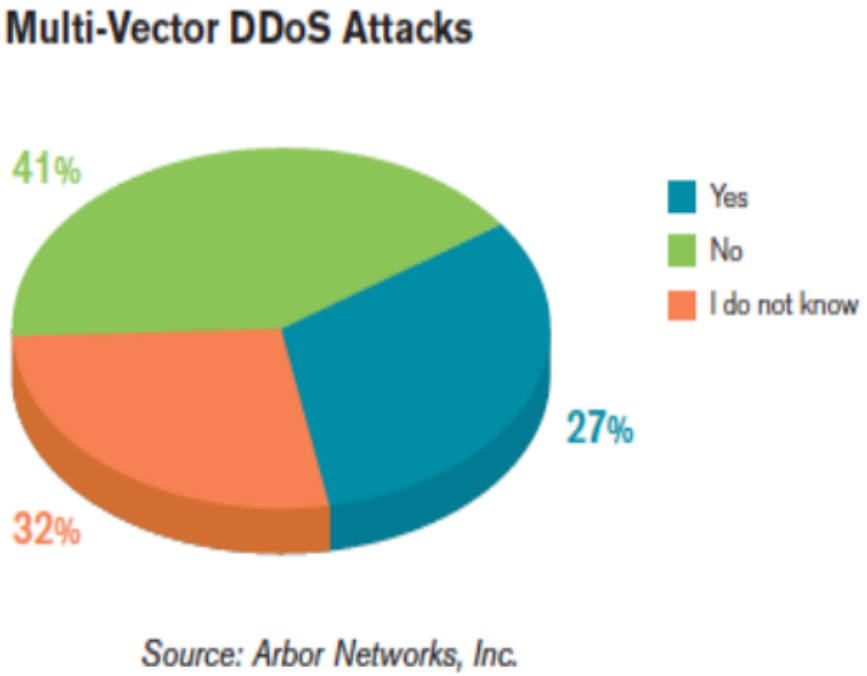
Модели атак

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Цели атак

Цели L7 атак:

- HTTP/S
- DNS
- VoIP
- SMTP
- POP



ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

IoT

Устройства IoT приобретают все большую популярность в качестве инструментов для осуществления DDoS-атак. Знаменательным событием стала предпринятая в сентябре 2016 года DDoS-атака с помощью вредоносного кода Mirai. В ней в роли средств нападения выступили сотни тысяч камер и других устройств из систем видеонаблюдения.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Типы DDoS-атак

- DDoS атаки делятся на 2 типа:
  — DDoS Layer 3&4 по модели OSI. Одна из характеристик данной атаки – большое количество пакетов, которыми атакуется ресурс. На данный момент средняя мощность атаки по миру – 9,7 Gb/s и 19 Mpps.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Типы DDoS-атак

— DDoS Layer 7 по модели OSI, то есть атака на уровень приложений. Как правило, атака не содержит большое количество пакетов (на порядки ниже, чем при DDoS L3&4), скорее характеризуется точечным ударом по слабому месту атакуемого сайта.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Цели атак

Подключение к сервисам защищающим от DDoS атак происходит следующим образом:
— Для защищаемого ресурса в DNS прописывается адрес защищающего;
— Клиент указывает, на какой ip адрес пересылать очищенный трафик (как правило, на тот же адрес, который и был до подключения к сервису).

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Цели атак

при попытке получить ip-адрес заказчика по имени сайта можно получить ip-адрес сервиса по защите:

$ nslookup www.XXXXXXXX.ru

www.XXXXXXXX.ru canonical name = xxx.incapdns.net.

Name: xxx.incapdns.net

Address: 149.126.xxx.xxx

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Цели атак

Но можно посмотреть DNS history по данному имени. Можно зайти на любой сайт, предоставляющий подобную информацию и увидеть:

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Цели атак

IP Address	Location	IP Address Owner	Last seen on this IP
149.126.xxx.xxx	Binghamton — United States	Incapsula Inc.	2015
149.126.yyy.yyy	Binghamton — United States	Incapsula Inc.	2015
zzz.zzz.zzz.zzz	United States	HOSTER LTD	2014

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

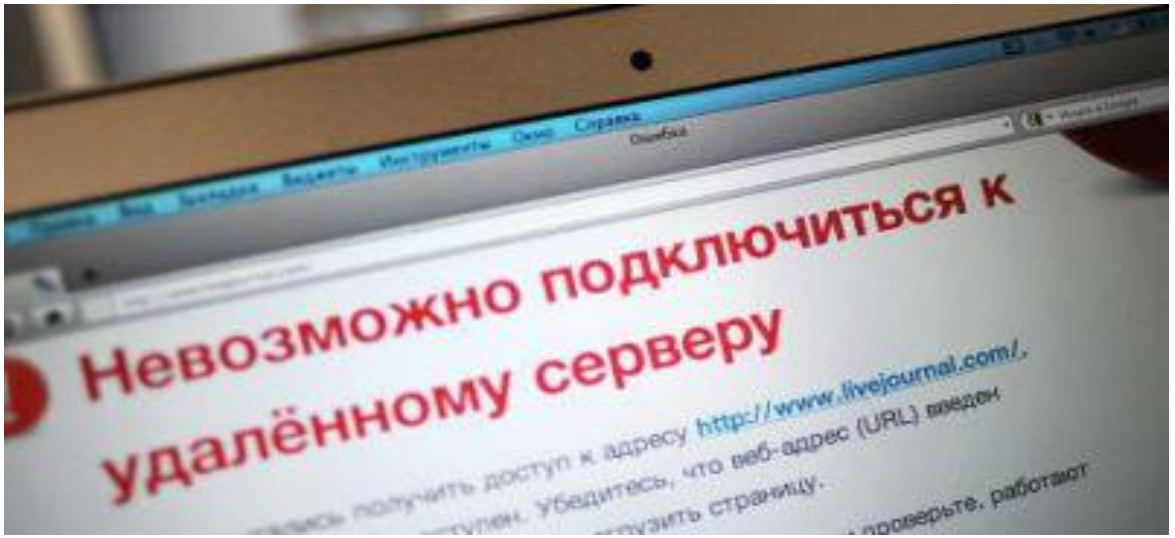
Цели атак

В результате оказывается, что его предыдущий ip-адрес — zzz.zzz.zzz.zzz; более того, видно, что он находится на площадке HOSTER LTD в США.

Остается только внимательно посмотреть на сервер, который имеет этот ip-адрес . Если это искомый сервер заказчика, можно его атаковать по ip-адресу. Защита не работает.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Выявление DoS/DD0S-атак



Существует мнение, что специальные средства для выявления DoS-атак не требуются, поскольку факт DoS/DDoS-атаки невозможно не заметить. Во многих случаях это действительно так. Однако достаточно часто наблюдались удачные DoS-атаки, которые были замечены жертвами лишь спустя 2-3 суток

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Выявление DoS/DDOS-атак

Методы обнаружения DoS-атак можно разделить на несколько больших групп:

- **сигнатурные** — основанные на качественном анализе трафика,
- **статистические** — основанные на количественном анализе трафика,
- **гибридные (комбинированные)** — сочетающие в себе достоинства обоих вышеназванных методов.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Защита от DoS/DDoS-атак

Меры противодействия DoS-атакам можно разделить на пассивные и активные, а также на превентивные и реакционные.

- **Предотвращение.** Профилактика причин, побуждающих тех или иных лиц организовывать и предпринять DoS-атаки.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Защита от DoS/DDoS-атак

- **Фильтрация и блэкхолинг.** Блокирование трафика, исходящего от атакующих машин. Эффективность этих методов снижается по мере приближения к объекту атаки и повышается по мере приближения к атакующей машине.
- **Устранение уязвимостей.** Не работает против флуд-атак, для которых «уязвимостью» является конечность тех или иных системных ресурсов.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Защита от DoS/DDoS-атак

- **Наращивание ресурсов.** Абсолютной защиты естественно не дает, но является хорошим фоном для применения других видов защиты от DoS-атак.
- **Рассредоточение.** Построение распределённых и дублирование систем, которые не прекратят обслуживать пользователей, даже если некоторые их элементы станут недоступны из-за DoS-атаки.

ВЯТСКИЙ
ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ

Защита от DoS/DDoS-атак

- **Уклонение.** Увод непосредственной цели атаки (доменного имени или IP-адреса) подальше от других ресурсов, которые часто также подвергаются воздействию вместе с непосредственной целью атаки.
- **Активные ответные меры.** Воздействие на источники, организатора или центр управления атакой, как техногенными, так и организационно-правовыми средствами.

ВЯТСКИЙ
ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ

Защита от DoS/DDoS-атак

- **Использование оборудования для отражения DoS-атак.** Например DefensePro® (Radware), Периметр (МФИ Софт), Arbor Peakflow® и от других производителей.
- **Приобретение сервиса по защите от DoS-атак.** Актуально в случае превышения флудом пропускной способности сетевого канала.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Семь уровней модели OSI

7	Прикладной уровень	Сетевые процессы с прикладными программами
6	Уровень представления	Представление данных
5	Сеансовый уровень	Связь между хостами
4	Транспортный уровень	Связь между конечными устройствами
3	Сетевой уровень	Адреса и маршрутизация
2	Канальный уровень	Доступ к среде передачи данных
1	Физический уровень	Двоичная передача

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Ссылки

- https://habrahabr.ru/company/ruvds/blog/321992/
- https://vsesam.org/chto-takoe-brandmauer-i-dlya-chego-nuzhen/
- http://compconfig.ru/net/dos-i-ddos-ataki.html