Предлагаю Вашему вниманию материал по DoS/DDoS-атакам, которым поделился со мной коллега "по теме информбезопасности" Алексей Бебинов. На мой взгляд, это один из наиболее толковых материалов, отражающих организационные и технические аспекты проблемы. Он может служить дополнением к материалу юридического характера, который ранее подготовила и распространяла "АГОРА".

https://www.accessnow.org/page/-/docs/DoS_Russian.pdf

Хочу заметить, что тема DoS любима журналистами и встречает живой отклик в онлайновой среде. Однако, по моим оценкам, сегодня для большинства российских правозащитных НКО эта угроза носит условный характер. DoS - незаконное дело, которое требует какой-никакой, но все-таки организации (и денег). Крупные, раскрученные, оперативно обновляющиеся новостные сайты действительно могут оказаться в "зоне риска". Небольшим ресурсам со средней или малой посещаемостью DoS вряд ли грозит, хотя гражданские активисты могут переоценивать "привлекательность" своего сайта для DoS. Это способно привести к тому, что (например) внезапная проблема с оборудованием провайдера ошибочно будет воспринята как атака с поспешными заявлениями в СМИ, что, в свою очередь, повлечет за собой репутационные риски.

Тем не менее, знать о DDoS полезно: наши сайты растут, становятся более насыщенными и динамичными.

Я придерживаюсь той точки зрения, что в смысле противодействия DoS-атаке мы должны стремиться к двум целям: 1) как можно быстрее вернуть наш ресурс "в строй" и 2) минимизировать ущерб. К статье прилагаются мои комментарии. Они учитывают наш опыт и некоторую российскую специфику.

- - - - - - - - - - - - - -

ВВЕДЕНИЕ

1. Отдавая первое место DoS в числе кибер-угроз для гражданского общества, авторы статьи, скорее всего, имели в виду не столько распространенность угрозы, сколько тот факт, что противодействие DoS-атаке является технически одним из наиболее сложных действий для неподготовленной НКО (особенно учитывая "нервозность момента").

2. Для лучшего понимания: DoS-атака заключается в одновременной отправке на сайт-жертву огромного числа запросов. Эти запросы создают длинную "очередь", из-за которой обычные пользователи не могут зайти на сайт. Визуально это выражается в длительном ожидании загрузки страницы в браузере (в конечном счете браузер, как правило, показывает пустую страницу).

3. Авторы статьи часто исходят из предположения, что пользователь имеет широкие технические возможности в отношении своего сайта. Местами вы встретите советы, выполнить которые "по плечу" только владельцам сайтов на собственном "железе". Большинство сайтов правозащитных НКО в нашей стране расположено на недорогом хостинге, где возможности владельца ограничены набором предустановленного программного обеспечения. Полномочий что-то всерьез настраивать (и, тем более, делать апгрейд "железа") у пользователя нет. Это ограничивает способность владельца противостоять DoS-атаке. К счастью, сайты на виртуальном хостинге обычно невелики и не представляют интерес для организаторов DoS-атак (см. выше).

НА КАКОМ ХОСТИНГЕ РАЗМЕЩАТЬ САЙТ

4. Диалог с провайдером может оказаться непростым или безрезультатным. По здравому смыслу, провайдер не заинтересован в размещении у себя интернет-ресурсов, которые заведомо являются мишенью для DoS-атак. Ведь в случае атаки нагрузка ложится на оборудование и каналы провайдера, да и разбирательства с паникующим клиентом и его недовольными "соседями" по хостингу провайдеру ни к чему. Пытаясь прояснить вопросы типа "возможно ли при DoS-атаке перенести наш сайт на отдельный сервер" и "сколько дней вы готовы терпеть DoS-атаку", вы, скорее всего, не ощутите энтузиазм провайдера и не получите четких ответов (тем более - гарантий).

Полезным при выборе хостинг-провайдера может быть изучение отзывов коллег и публикаций в интернете. (Естественно, со скидкой на то, что часть позитивных публикаций может быть проплачена самим провайдером, а негативных - опубликована его конкурентами). Более объективными, на мой взгляд, могут оказаться суждения на форумах разработчиков веб-сайтов, в частности, систем управления сайтами (CMS). Изучая эти отзывы, соотносите упоминаемые в них технические требования с требованиями для своего сайта.

5. Отдельно можно поговорить о выборе типа хостинга: на основе готовых шаблонов; виртуальный; виртуальный выделенный сервер (VDS/VPS); выделенный сервер (dedicated); размещение собственного оборудования в стойке провайдера (co-location). Подробный разбор особенностей, плюсов и минусов каждого варианта в условиях правозащитных проектов и бюджетов - тема для отдельного разговора.

6. При выборе хостинга рекомендую обращать внимание на инструменты статистики, которые по умолчанию предлагает провайдер. Они могут оказаться полезными в случае DoS. При анализе трафика (неподготовленным пользователем) DDoS можно считать вероятным, если отмечается аномальный рост входящего трафика (в несколько раз больше обычного), а также (иногда) если существенно возрастает зарубежный трафик. Обратите внимание, что многие хостинг-провайдеры обещают "неограниченный трафик". Это рекламный ход, которым провайдер завлекает клиентов. Провайдер выполняет свое обещание в отношении подавляющего большинства клиентов просто потому, что эти клиенты потребляют мало ресурсов. Как только объем трафика "прыгает вверх" (при атаке), провайдер начинает волноваться вплоть до отключения клиентского сайта. В пользовательских соглашениях иногда указано, что "неограниченный трафик" подразумевает условия вроде "российский трафик превышает зарубежный" и/или "входящий трафик не более 1/4 от исходящего" (как раз те соотношения, которые бывают нарушены при DoS-атаке).

7. Еще один (но не последний) фактор выбора провайдера - доступность техподдержки. Многие хостинг-провайдеры, утомленные назойливыми телефонными жалобщиками и некомпетентными скандалистами, переводят всю свою систему общения "провайдер-клиент" на так называемые "тикеты" (заявки), которые клиент должен оформлять на веб-сайте. Важно попытаться узнать, насколько надежно и оперативно работает эта система у провайдера (можно попробовать оценить по отзывам). Неплохо также иметь альтернативные способы связи (в первую очередь, телефон). Из опыта известно, что злоумышленники часто выбирают для DoS-атаки вечер пятницы или утро субботы - с расчетом, что в выходные дни техподдержка провайдера не так отзывчива, если вообще работает. Этот расчет, увы, нередко оправдывается.

ЗАРУБЕЖНЫЙ ХОСТИНГ

8. В случае DoS-атаки провайдер может не только "ничего не делать для защиты своих клиентов", но и усугублять их бедственное положение. В нашем опыте был случай, когда провайдер, "почуяв" DoS-атаку, просто отключил атакуемый сайт ("выдернул вилку из розетки"), формально известив клиента, что сайт будет возвращен в рабочее состояние через сутки. Таким образом, даже после фактического прекращения атаки на все остальные сайты из "группы риска" в этот день и возвращения их "в строй" - данный сайт оставался недоступен читателям.

9. Предполагаемое давление властей на хостинг-провайдеров - вероятно, не единственная не главная причина "ничегонеделанья". Основная причина такова: провайдер считает более простым и действенным избавиться (пусть на время) от одного "проблемного" клиента, чем тратить собственные ресурсы и вдобавок выслушивать претензии от десяти других клиентов.

10. Особенность хостинга "в дальнем зарубежье" (как правило) - отсутствие русскоязычной поддержки. Оценивайте собственные способности оперативно общаться с техподдержкой на английском языке.

11. Не следует идеализировать зарубежный хостинг. Например, один известный зарубежный хостер предусматривает свой способ "борьбы с превышением трафика": в случае такового провайдер урезает пропускную способность канала, что делает сайт труднодоступным. Провайдер возвращает все "на круги своя" лишь за дополнительную плату. Получается, что потерпевшему назначается дополнительное наказание за DoS-атаку, которой он подвергся. Изучайте пользовательское соглашение и наводите справки в независимых (относительно независимых) источниках.

МЕСТНЫЙ ХОСТИНГ

12. Подавляющее большинство сайтов НКО в России нацелено на аудиторию жителей России. Естественным хостингом для таких сайтов были бы российские площадки. Но риски, описанные в статье (и частично в моих комментариях выше), заставляют обращать внимание на зарубежный хостинг. Время доступа к сайту можно оценить, например, по времени прохождения пакетов данных путем использования команд ping и tracert. Для европейских, а тем более американских площадок это время будет больше, чем для российских. Однако опыт показывает, что при не слишком нагруженном сайте (скажем так: не галерее видеоматериалов) разница на практике малозаметна. Поэтому размещение сайта на зарубежном хостинге сегодня вряд ли драматично отразится на скорости его загрузки в браузерах читателей. Принимать решение о необходимости хостинга на Западе, на мой взгляд, следует после спокойной и всесторонней оценки риска быть подвергнутым онлайновым преследованиям со стороны властей.

13. Для российской реальности существует "компромиссный" вариант размещения хостинга в одной из республик бывшего СССР с более мягким режимом, например, в Прибалтике или Украине. Достоинством такого варианта является меньшее время доступа, чем для хостинга "в дальнем зарубежье", и (не всегда, но часто) готовность техподдержки вести диалог на русском языке.

14. Факт принадлежности юридического лица той или иной стране еще не означает, что "железо" (дата-центр) находится в той же стране. Многие крупные хостинг-провайдеры имеют дата-центры в разных странах. Иногда клиенту предлагается выбрать себе площадку "по вкусу" (например, в Москве, Франкфурте или Далласе).

15. Существует популярная схема аренды, известная как "реселлинг хостинга". Фирма А раскручивает свой хостинг не на собственном дата-центре, а на мощностях, арендованных у фирмы Б. Договариваясь с А, вы имеете дело с посредником, который в случае атаки с большей вероятностью будет заинтересован в удержании остальных своих клиентов и "выталкивании" вашего сайта. Как правило, реселлер не афиширует то, что он - реселлер. Определить это иногда можно по отзывам, иногда с помощью той же команды tracert.

УСЛУГИ ЗАЩИТЫ КЛИЕНТОВ ОТ DoS

16. Для недорогого хостинга сколь-нибудь серьезная защита обычно не предлагается.

17. Услуги специализированных служб вроде упомянутого DoSarrest и его конкурентов (например, ServerOrigin) колеблются в широком спектре от нескольких десятков до нескольких тысяч долларов ежемесячно. Сравнительный обзор таких услуг в контексте их возможного использования российскими НКО - отдельная тема.

СОЗДАНИЕ ЗЕРКАЛ САЙТА
РАСПРЕДЕЛЕНИЕ НАГРУЗКИ НА ЗЕРКАЛА

18. Упоминание о том, чтобы "сайт легко копировался", справедливо не только в контексте противодействия атакам, но и для ряда других ситуаций, например, выхода из строя "железа" провайдера или несанкционированного доступа к сайту, который может привести к удалению материалов. Любой администратор сайта должен уметь делать резервные копии базы данных и файлов сайта, автоматически и/или вручную. Наличие под рукой свежей копии сайта позволит сравнительно быстро перенести его на другую площадку. Например, в большинстве случаев для базы используется MySQL - стандартная ("универсальная") опция в хостинг-планах самых разных провайдеров. Для создания резервной копии базы обычно используют утилиту phpMyAdmin, которая предлагается хостинг-провайдерами повсеместно; я советую попробовать php-утилиту Sypex Dumper.

19. Создание зеркал, как справедливо отмечают авторы статьи, подразумевает, что "тренироваться нужно регулярно и планово". Иными словами, зеркала должны быть постоянно "под рукой", доступны, оплачены в соответствии с их тарифными планами, да и сторонний коммерческий балансировщик будет стоить денег (например, tzoha.com предлагает варианты от 174 долл./мес.).

20. Возможность редактировать записи DNS чрезвычайно важна. Хостинг-провайдеры, как правило, предлагают сами зарегистрировать для вас домен. Однако, я склоняюсь к тому, что владельцу сайта лучше регистрировать домен самостоятельно (у одного из регистраторов доменных имен) и загодя

освоить панель управления доменом. К доменным именам применимы те же размышления насчет "зарубежного/российского", что и для хостинга, и даже более. Ведь хостинг - это лишь площадка, которую при наличии резервных копий сравнительно легко сменить. Доменное имя - главный путь к сайту, и если владелец его потеряет, он рискует потерять всех читателей. Лишиться доменного имени гораздо хуже, чем лишиться хостинг-площадки. В 2010 году в России произошла нашумевшая история с прекращением делегирования домена torrents.ru, принадлежавшего крупнейшему российскому торрент-трекеру. Инициатором выступила прокуратура, исполнителем - регистратор доменных имен Ru-Center. Принимая решение о выборе и регистрации домена, возможно, следует вспомнить этот случай. Если для вашего сайта вероятны DoS-атаки, то недовольные "оппоненты" могут пойти и по другому, описанному выше сценарию. Возможно, для сайта из "группы риска" лучше иметь регистрацию домена у регистратора, находящегося вне юрисдикции "своей" страны.

ДУБЛИРОВАНИЕ СОДЕРЖАНИЯ НА ОТКРЫТЫХ РЕСУРСАХ

21. Это в последнее время становится популярным и без DoS-атак. Сегодня многие разработчики сайтов стараются предложить читателям собственные материалы в блогосфере и социальных сетях (для России это, в первую очередь, "Живой журнал", "ВКонтакте" и Facebook). Системы управления сайтами (CMS) имеют модули, позволяющие автоматизировать процесс размещения материалов, например, в ЖЖ-сообществе или на странице Facebook. Тем не менее, никакая из виденных мной площадок такого рода не являлась копией оригинального сайта, и дело не только в упрощенных шаблонах (как пишут авторы статьи), но и в том, что блоги и социальные сети по своему смыслу предназначены для оперативного обновления сравнительно короткими материалами, и такие фундаментальные разделы, как "Законы" и "Доклады" (значительный процент содержания сайтов наших НКО), в блоги и социальные сети не переносятся. Таким образом, при блокировании сайта DoS-атакой читатель не увидит его копии где-нибудь в ЖЖ, так что говорить о "зеркале" не вполне корректно. Можно сказать, что использование блогов и социальных сетей при DoS-атаке позволит продолжить онлайновую работу в целом и даст некоторой части читателей понимание того, что команда сайта жива и по-прежнему публикует информацию.

22. "Открытые ресурсы", как правило, представляют собой дискуссионные площадки. Это позволяет владельцам пострадавшего от DoS-атаки сайта поддерживать живой контакт с читателями и, возможно, получить от сочувствующих специалистов дельный совет.

ПРОВАЙДЕРЫ С ШИРОКИМ КАНАЛОМ СВЯЗИ

23. Можно предположить, что чем известнее и крупнее провайдер, тем легче он способен перенести DoS-атаку. Впрочем, это очень грубое приближение. Может быть, даже неправда :)

РАСПРЕДЕЛЕНИЕ КОНТЕНТА ПО ДРУГИМ САЙТАМ

24. К приведенной на этой странице иллюстрации: следует понимать, что "настоящие пользователи веб-сайта" в случае DoS-атаки не смогут попасть на копии материалов на сайтах организаций-партнеров, зная лишь доменное имя пострадавшего сайта. Это значит, что пользователям должны быть заранее (до DoS-атаки) известны "альтернативные площадки", где бы они смогли найти материалы. Сообщить им эту информацию можно через блоги и социальные сети (см. выше).

25. Независимо от DoS-атак я рекомендую тем "сайтовладельцам", кто это еще не сделал, но сравнительно часто обновляет сайт, обзавестись RSS-лентами.

ПРОТИВОДЕЙСТВИЕ DOS-АТАКЕ

26. Блок-схема предлагает последовательность действий для технического персонала. (Как вы можете убедиться, рекомендации здесь подразумевают широкие возможности этого персонала). Вне зависимости от того, какими возможностями обладает техподдержка сайта в вашей НКО, если вы считаете, что находитесь в "зоне риска", разумно подготовить кризисный план действий на случай DoS. Этот план может/должен включать не только сугубо технические решения, но и организационные аспекты. К примеру, ответы на такие вопросы: "Кого из специалистов мы попросим о помощи и как можно связаться с этими людьми", "Как мы будем реагировать на вопросы читателей и журналистов о причинах неработоспособности сайта", "Кто в нашей организации будет размещать материалы в блогах и социальных сетях".

27. Кризисный план на случай DoS может/должен стать частью политики информационной безопасности организации, включающей такие темы, как создание надежных паролей и их хранение защищенным способом, правила создания резервных копий данных, защита компьютеров и сетей в НКО от вирусов и прочего вредоносного кода, и так далее. Хорошим стартом для размышления о собственной политике информационной безопасности могут быть материалы сайта "Безопасность-в-коробке" (http://security.ngo-in-a-box.org/ru). "Правозащитная сеть" и портал "Права человека в России" (hro.org) время от времени проводят семинары для НКО по теме информационной безопасности (для связи: Сергей Смирнов, moscow@hro.org).

ЭТАПЫ ПРОТИВОДЕЙСТВИЯ DOS-АТАКАМ

28. Как я уже говорил выше, авторы статьи идеализируют хостинг-провайдеров. Довольно часто в нашей российской реальности провайдер идет "по пути наименьшего сопротивления", закрывая пострадавший сайт и избегая переговоров с его владельцем.

НАЧАЛЬНЫЙ ЭТАП

29. Пострадавшие от DoS-атаки, бывает, торопятся с заявлениями в самом начале обнаружения атаки. Я рекомендую поступать осторожнее. Если вы еще не знаете масштаб и тип атаки, вряд ли есть смысл драматизировать события. Это может выразиться в последующих репутационных рисках. В одном из своих интервью Евгений Касперский рассказывал о собственных попытках узнать подробности о DoS-атаках у владельцев атакуемых сайтов. Некоторые не предоставили никакую дополнительную информацию кроме общих слов "нас атаковали". Это побудило исследователя предположить, что владельцы сайтов, возможно, маскируют какие-то досадные проблемы, не связанные с DoS, например, сбой аппаратного обеспечения, или даже набивают себе цену ("нас атакуют, стало быть, нам придают большое значение"). Особенно осторожным, на мой взгляд, следует быть, отвечая на любимый журналистами вопрос: "Как вы думаете, кто организовал на вас атаку?". На начальном этапе почти никогда нельзя дать технически грамотный ответ. Более того, руководитель или пресс-секретарь НКО, которому задан вопрос, бывают склонны давать политизированные ответы, не подкрепленные фактами. По моему мнению, формулировку ответа членам НКО следует согласовать еще до атаки в упомянутом выше кризисном плане. Этой формулировке, на мой взгляд, следует быть лаконичной, спокойной и выдержанной в стиле "да, атака ведется; технические специалисты работают; помимо прочего, сейчас они анализируют источники и оценивают масштаб; проблема носит временный характер; мы продолжаем давать информацию в интернет, в том числе и об этой атаке (ссылки на площадки)".

ИСПОЛЬЗОВАНИЕ СЕТЕВОГО ЭКРАНА

30. Возможно, это один из наиболее эффективных (хотя далеко не панацейных) способов защиты от DoS. В нашей практике мы применяли блокирование "подозрительных" адресов (откуда шел наибольший трафик), добиваясь этим, как и рассказывается в статье, некоторого снижения нагрузки.

ЗЕРКАЛА СОДЕРЖИМОГО САЙТА НА ОТКРЫТЫХ РЕСУРСАХ

31. Как уже было сказано, в данном контексте слово "зеркало" можно употреблять только в кавычках, так как создать настоящее зеркало (копию сайта) на таких площадках вряд ли удастся. Как бы то ни было, я не думаю, что есть хоть какой-либо смысл создавать и обустраивать эту резервную площадку во время DoS-атаки. Резервные площадки, на мой взгляд, нужно готовить до атаки. Поспешное "сайтостроительство" во время DoS-атаки способно стать причиной нерационального расходования ресурсов, особенно ценных в такой момент.

РАСПРЕДЕЛЕНИЕ КОНТЕНТА ПО ДРУГИМ САЙТАМ

32. На других сайтах существуют свои редакционные политики, а их владельцы имеют собственные "взгляды на жизнь". Даже в "мирное время" (то есть, вне DoS-атаки) идея трансляции вашей RSS-ленты на чужой сайт может вызвать сомнения у его владельца. Во время атаки, в обстановке нервозности и спешки в ленте вполне могут появиться более эмоциональные, "алармистские" материалы, и "сайтовладельцы" со стажем это понимают. Кроме того, в отличие от открытых площадок, размещение материалов на партнерском сайте обычно требует предварительной работы администратора, что (в лучшем случае) растянет процесс во времени. Поэтому договоренности о

трансляции ваших материалов (на постоянной основе или при атаке) лучше устанавливать заранее.

УКЛОНЕНИЕ ОТ АТАКИ

33. Атака часто предпринимается не на IP-адрес (который владелец обычно может относительно легко сменить), а на доменное имя.

34. В данном разделе авторы, по-видимому, говорят о продолжительных DDoS-атаках.

ГДЕ РАЗМЕЩАЕТСЯ САЙТ

35. При решении вопроса о хостинге сайта есть смысл проанализировать, как повел себя в критической ситуации хостинг-провайдер. Если вы не получили от него ощутимую поддержку, и тем более, если во время атаки провайдер вас игнорировал или даже усугублял ваше положение (отключал сайт, выставлял счета за перерасход трафика и так далее), это серьезное основание для того, чтобы подумать о смене хостинга.

ПОЛЕЗНЫЕ СОВЕТЫ

36. Среди этих советов мельком упоминается кэширование материалов сайта. Кэширование может осуществляться не только владельцем сайта, но и сторонней службой (например, такая опция есть у некоторых балансировщиков нагрузки). При обращении к сайту пользователям выдается кэшированная (заранее сохраненная) копия. Брать элементы страницы из кэша заметно быстрее, чем динамически формировать страницу. Особенно это заметно для "нагруженных" сайтов с множеством элементов, где для формирования страниц CMS (система управления сайтом) неоднократно обращается к базе данных. Кэширование позволяет уменьшить нагрузку на ресурсы сервера и увеличить вероятность выдачи пользователю страниц вашего сайта при возрастании числа запросов.

37. Не упомянутый, но критически важный организационный совет. Позаботьтесь о надежных быстрых каналах связи между сотрудниками вашей НКО, которые могут/должны быть вовлечены в процесс противодействия DoS (учитывая, что в выходной день, когда чаще всего и случается атака, люди могут быть не в офисе, а в самых разных местах). Электронная почта может оказаться недостаточно быстрым способом связи. Очень хорошо, если все вовлеченные люди знали телефоны друг друга. Удобным средством коммуникации в этом случае может стать Skype. Посредством Skype можно устроить мини-встречу в онлайне для обсуждения ситуации и принятия оперативных решений. Если вы предполагаете, что в какой-либо определенный день (например, день выборов или крупного митинга в вашем городе) риск DoS-атаки на ваш сайт возрастает, лучше, чтобы в этот день ответственные за сайт люди не отлучались далеко от компьютера и могли отреагировать на DoS.

В заключение.

На мой взгляд, владельцу сайта следует соотнести временнЫе расходы на вынужденный простой сайта во время DoS-атаки с тем временем, которое понадобится для организации противодействия этой атаке и приведение сайта в более-менее рабочее состояние. Атаки на российские сайты, "приуроченные" к дням выборов 2011 и 2012 гг., обычно "умещались" в интервал одного дня, то есть, дня выборов. Комплекс мер, описанных в этой статье, может занять соизмеримое время, учитывая всевозможные трудности, как-то: отсутствие многих людей на рабочих местах в выходной день; заторможенность техподдержки провайдера; задержки срочных платежей и т.д. Конечно, это не повод вовсе отказываться от противодействия DoS, но достаточная причина, чтобы как следует подготовиться и продумать политику информационной безопасности, включая кризисный план на случай DoS. Очень много зависит от того, насколько четким, ясным и реализуемым будет этот план, а также насколько слаженно и аккуратно работают все члены вашей команды.

С уважением,

Сергей Смирнов, HRO.org