SAC 056

Информационное сообщение ККБС о последствиях блокирования содержимого через систему доменных имен

Информационное сообщение Консультативного комитета по вопросам безопасности и стабильности (ККБС) ICANN

09 октября 2012 г.

Введение

Настоящий документ является заключением Консультативного комитета по безопасности и стабильности (ККБС). ККБС консультирует сообщество и Совет директоров ICANN по вопросам, связанным с безопасностью и целостностью систем распределения имен и адресов Интернета. К таким вопросам относятся эксплуатационные вопросы (например, вопросы, относящиеся к правильной и надежной работе системы корневых имен), административные вопросы (например, вопросы, относящиеся к распределению и назначению интернет-адресов) и регистрационные вопросы (например, вопросы, связанные с услугами реестров и регистраторов). ККБС занимается постоянной оценкой угроз и анализом рисков для служб распределения имен и адресов Интернета с целью определения источников основных угроз стабильности и безопасности, и предоставляет соответствующие рекомендации сообществу ICANN. ККБС не обладает полномочиями регламентировать, обеспечивать соблюдение или выносить решения по спорам. Эти функции принадлежат другим органам, и содержащиеся здесь сведения и должны рассматриваться по существу дела.

Имена авторов этого информационного сообщения, ссылки на биографии членов комитета и заявления о заинтересованности, а также возражения членов комитета, касающиеся выводов или рекомендаций, содержатся в конце настоящего документа.

Содержание

1. Сводное резюме

Использование блокирования через систему доменных имен (DNS) для ограничения доступа к ресурсам в Интернете стало предметом обсуждения в различных структурах управления Интернетом. Некоторые правительственные органы во всем мире либо уже осуществляют блокирование DNS посредством законов, договоров, распоряжений суда, правоприменительных мер или других действий и соглашений, либо активно рассматривают такую возможность. Однако, в силу специфики архитектуры Интернета, блокирование по имени домена может быть с легкостью обойдено конечными пользователями и поэтому является в значительной степени неэффективным в долгосрочной перспективе и чревато непредвиденными последствиями в ближайшем будущем. Кроме того, блокирование DNS может привести к конфликтам в связи с внедрением расширений безопасности DNS (DNSSEC) и к «балканизации» Интернета, когда в каждой стране будет существовать свой особый взгляд на пространство имен Интернета.

Настоящий документ ограничивается изучением технических последствий, связанных с блокированием DNS, которые включают в себя следующее.

- Блокирование домена посредством:
  - реестра или регистратора;
  - полномочного сервера;
  - рекурсивного распознавателя через перенаправление, несуществующее доменное имя, отвергнутый код отклика на запрос, другие коды возврата или отсутствие отклика на запрос.
- Блокирование DNS в рекурсивных распознавателях и конфликты с DNSSEC.
- Привлечение конечных пользователей к более активному использованию сквозного шифрования.
- Избыточное блокирование.
- Типографские ошибки.
- Маршрутизация трафика из страны, которая осуществляет блокирование.
- Последствия смены пользователями распознавателей.
- Нарушение локализации сетей распределения контента (CDN) при смене пользователями распознавателей.

Нетехнические вопросы, такие как ограничение свободы выражения мнений, не рассматриваются в настоящем документе. Интернет-сообщество, правительственные и другие органы должны четко осознать и тщательно рассмотреть все проблемы, связанные с блокированием DNS, как технического, так и нетехнического характера.

2. Введение

Настоящий документ основан на документе «SAC050: Блокирование DNS: преимущества и недостатки – информационное сообщение Консультативного комитета по безопасности и стабильности», который может представлять интерес для читателей настоящего документа.[1]

В 2011 и 2012 годах некоторые правительства предложили или внедрили официальные руководящие принципы, законы, распоряжения суда или правоприменительные меры, связанные с блокированием DNS, фильтрацией DNS и/или наложением ареста на доменное имя.[2] В одних случаях цель этих мероприятий заключалась в разработке нового законодательства, способствующего контролю над использованием Интернета, а в других случаях суды или правоохранительные органы использовали блокирование DNS или наложение ареста на доменное имя в качестве механизма блокировки доступа к определенным интернет-сайтам или адресам.[3,4,5,6]

В настоящем документе рассматриваются технические последствия различных типов блокирования DNS, которые были реализованы или предложены. Целью настоящего документа является информирование интернет-сообщества, политиков, правительственных служащих и других лиц о технических последствиях использования блокирования DNS для контроля доступа к интернет-ресурсам.[7]

---

[1] См. «SAC050: Блокирование DNS: преимущества и недостатки – информационное сообщение Консультативного комитета по безопасности и стабильности по вопросу блокирования доменов верхнего уровня в системе доменных имен», Корпорация Интернета по распределению адресов и номеров (ICANN), Консультативный комитет по безопасности и стабильности, 14 июня 2011 г.,http://www.icann.org/en/groups/ssac/documents/sac-050-en.pdf.

[2] См. H.R. 3261 (Акт о прекращении интернет-пиратства), Палата представителей США, 112-й конгресс, версия от 16 декабря 2011 г. и закон Эстонии о блокировании незаконных игровых сайтов, https://www.riigiteataja.ee/akt/125042012010.

[3] См. Инициатива OpenNet, http://opennet.net/youtube-censored-a-recent-history.

[4] См. http://arstechnica.com/tech-policy/2011/01/amidst-chaos-and-riots-egypt-turns-off-the-internet/.

[5] См. http://www.dhs.gov/ynews/releases/pr_1297804574965.shtm.

[6] См. http://www.telegraph.co.uk/technology/internet/9084540/Serious-Organised-Crime-Agency-closes-down-rnbxclusive.com-filesharing-website.html.

[7] Описание DNS см. по ссылке http://queue.acm.org/detail.cfm?id=1242499

3. Блокирование DNS: преимущества и недостатки

Основные выводы SAC050 сводятся к следующему.

> «Фильтрация на основе доменного имени или IP-адреса (или предотвращение доступа, например, к веб-контенту, который заражает компьютер вирусами или рассматривается как ненадлежащее использование ресурсов предприятия) может рассматриваться некоторыми организациями как естественное продолжение исторически сложившихся политик, которые не позволяли сотрудникам этих организаций нести расходы, связанные с междугородними телефонными переговорами.
> …
> Независимо от используемого механизма, организации, внедряющие блокирование, должны также применять следующие принципы.
>
> 1. Организация реализует политику по отношению к сети и ее пользователям, находящимся под административным контролем этой организации (т.е. она является администратором домена, подпадающего под действие политики).
> 2. Организация считает, что данная политика полезна для реализации задач организации и/или интересов ее пользователей.
> 3. Организация осуществляет реализацию данной политики с использованием метода, приносящего наименьший вред функционированию ее сети и пользователям, за исключением случаев, когда конкретные методы предписаны законами или нормативными актами.
> 4. Организация прилагает скоординированные усилия для предотвращения вреда для пользователей за пределами домена, в котором реализуется данная политика, вследствие внедрения этой политики.
>
> Если эти принципы не будут применяться, блокирование использования DNS может причинить косвенный ущерб или привести к непредвиденным последствиям при наличии лишь ограниченных средств защиты заинтересованных сторон или в отсутствие таковых».

В продолжение выводов, содержащихся в документе SAC050, и в целях должного удовлетворения и обеспечения общей стабильности Интернета необходимо, чтобы любые политики или действия, связанные с блокированием DNS, были полностью прозрачны для всех заинтересованных сторон, в том числе конечных пользователей,

поставщиков услуг и разработчиков приложений. Блокирование DNS в отсутствие такой прозрачности может привести к ненужным действиям по устранению неисправностей, а также к адаптивным и, возможно, даже обходным действиям со стороны операторов сетей и конечных пользователей. Соответствующая информация должна охватывать мотивы, предполагаемые последствия и возможные побочные эффекты. При отсутствии подобной прозрачности блокирование DNS может быть неверно диагностировано как отключение либо вредоносная атака и может вызвать ответные действия со стороны конечных пользователей, администраторов сетей, поставщиков услуг и т.д., направленные на смягчение ущерба.

Эта возможность ошибочного диагноза и неизбежный поиск обходных путей может стать причиной дополнительного ущерба или непредвиденных последствий. Необходимость независимой общественной оценки отмечается также в отчете специального докладчика Управления верховного комиссара ООН по правам человека по вопросу содействия и защиты права на свободу убеждений и их свободное выражение, где говорится, в частности, следующее.

> «31. […] В-третьих, даже если представлено достаточное обоснование, блокирующие меры представляют собой ненужные или несоразмерные средства достижения предполагаемой цели, поскольку они зачастую оказываются недостаточно целенаправленными и охватывают широкий спектр контента, недоступного вне того, что признано незаконным. Наконец, содержимое часто блокируется без вмешательства судебного или независимого органа и без возможности его оценки». [8]

Изучение типов и последствий блокирования DNS является темой оставшейся части настоящего документа.

4. Блокирование содержимого в контексте архитектуры Интернета

Одним из фундаментальных принципов архитектуры Интернета является его «сквозная» абстракция, благодаря которой интеллектуальные средства сводятся к минимуму в ядре (центре) сети, но охватываются на периферии (на отдельных хост-узлах). Эта архитектура обеспечивает огромный диапазон и глубину инноваций, например позволяя разработчику на одном конце сети развернуть новое приложение на узле, а конечному

[8] Франк ля Рю, «Отчет специального докладчика по вопросу содействия и защиты права на свободу убеждений и их свободное выражение»A.HRC.17.27., http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.

пользователю на другом конце установить соответствующий клиент, обеспечивающий новые формы связи без каких-либо специальных разрешений или элементов управления в любой другой части сети.

Блокирование содержимого через систему доменных имен иногда выполняется в «ядре», а иногда «на границе» Интернета. Взаимосвязи между поставщиком услуг Интернета, его источниками трафика и получателями называются «границей». Взаимосвязи внутри или между операторами называются «ядром». Примеры блокирования на базе ядра включают черные списки в веб-браузерах и фильтрацию IP-трафика на одном конце соединения. Если в ядре сети применяется блокирование на базе границы, конечные пользователи могут обойти блокировку, изменив поставщиков услуг DNS или с помощью использования виртуальных частных сетей, прокси-серверов или подключаемых модулей. Блокирование DNS на базе границы будет эффективным только в тех случаях, когда фильтрация на основе политик присутствует во всех возможных путях между конечными пользователями и сетями, с которыми они могут обмениваться пакетами. Примерами таких топологий являются национальные и корпоративные брандмауэры.

Побочным эффектом такой архитектуры является то, что попытки блокирования трафика по доменному имени (например, example.com) или по IP-адресу (например, 192.0.2.117) в любой точке сети, не находящейся на границе, *можно обойти*, например, с помощью использования виртуальной частной сети (VPN).[9] Частные виртуальные сети и аналогичные методы являются легкодоступными и удобными в использовании даже для не очень опытных пользователей. Даже в тех случаях, когда возможен полный административный и оперативный контроль над доступом к сетям Интернета (например, в рамках сетей одного поставщика услуг Интернета или в некоторых точках обмена интернет-трафиком[10]), конечные пользователи все же имеют возможность доступа к запрещенному содержимому.[11]

Общей характеристикой этих более успешных типов фильтрации является то, что конечный пользователь и его сетевой оператор в прямой или косвенной форме выражают свое согласие относительно того, что именно подлежит фильтрации и каким образом выполняется блокирование содержимого. В этом случае конечный пользователь рассматривает блокирование DNS как полезную услугу.

---

[9] См. http://www.prlog.org/11725655-how-to-bypass-blocked-sites-with-vpn-account.html or http://vpn-account.com/bypassblockedsites.html.

[10] См. http://en.wikipedia.org/wiki/Internet_exchange_point.

[11] См. http://www.foreignpolicy.com/articles/2011/01/26/can_governments_really_block_twitter.

5. Существующие и предлагаемые типы блокирования DNS

В течение последних лет были предложены или реализованы различные методы блокирования DNS. Одни методы влекут за собой больше технических сложностей, чем другие. Неполный список включает следующее.

1. **Наложение ареста на доменное имя реестром или регистратором**. При использовании данного метода данные DNS удаляются из источника реестром DNS или регистратором, действующим в качестве агента реестра. Реестр является органом, ответственным за создание полномочной базы данных DNS, включающей блокируемые домены. Примером подобного метода может служить издание правительством указа о «прекращении деятельности» доменного имени регистратору или реестру, которые должны выполнить такой указ на законных основаниях. Реакция реестра или регистратора на подобное требование зависит от конкретного содержания указа. Варианты включают удаление доменного имени из зоны (известное как «приостановка домена», когда сохраняются регистрационные данные об этом домене), препятствующее разрешению доменного имени, связанного с определенным сайтом, для конечных пользователей, или сопоставление доменного имени с другим сервером имен, который будет перенаправлять пользователей на веб-страницу, отображающую дополнительную информацию, например юридическое уведомление о приостановке деятельности. В ситуации «приостановки домена», после истечения срока настроек жизненного цикла в записи DNS домена (обычно в течение нескольких часов или дней), домен становится неразрешимым глобально. Это означает, что, когда пользователь вводит это доменное имя, возвращается ответ «домен не существует». Если арест налагается на правильные доменные имена, не существует прямых отрицательных технических последствий, специфичных для метода «приостановки домена». Косвенные отрицательные технические последствия могут включать сбои дистанционных служб, если другие домены зависят от службы имен, службы электронной почты или веб-службы на домене, подвергшемся такой «приостановке». При использовании метода «приостановки домена» или метода изменения сервера имен регистратор или реестр должен также обновить или удалить все данные DNSSEC для соответствующего домена. В противном случае DNSSEC-совместимые приложения будут обнаруживать недействительные данные в ответах на запросы DNS, в результате чего невозможной станет всякая связь, в том числе и с целью объяснения пользователям, почему тот или иной домен более не доступен.

2. **Блокирование домена на полномочном сервере.** Этот тип блокирования, осуществляемый оператором полномочного сервера имен соответствующего доменного имени, обходит реестр и, в отдельных случаях, регистратора и направлен непосредственно на механизм, посредством которого доменное имя становится доступным в Интернете. После того как регистратор получает и должным образом настраивает доменное имя, реестр генерирует данные DNS и публикует эти данные на ряде «полномочных серверов». Во многих случаях регистратор одновременно является и оператором этих полномочных серверов, однако это не является необходимым условием, как не является необходимым и требование о том, чтобы все полномочные серверы находились под управлением одного и того же органа. Независимо от того кто является оператором полномочного сервера, серверы представляют собой механизм публикации и, таким образом, являются точкой, на которой может быть реализовано блокирование DNS. Примером подобной формы блокирования может служить издание правительством указа о прекращении деятельности доменного имени оператору DNS-сервера, который является полномочным для соответствующего доменного имени. После этого оператор удаляет или изменяет свою копию полномочных записей DNS для данного доменного имени. При условии что указ о прекращении деятельности разослан всем операторам полномочных серверов для домена и выполнен ими, домен немедленно становится ненадежным на глобальном уровне и в конечном итоге неразрешимым по истечении жизненного цикла DNS-записей домена. Помимо того что блокирование осуществляется различными органами, этот метод отличается от блокирования реестром/регистратором еще и тем, что может создавать проблемы в случае использования DNSSEC, поскольку оператор полномочного сервера может оказаться не в состоянии сохранить подписи DNSSEC реестра при изменении содержимого домена реестра.
3. **Блокирование домена на рекурсивном распознавателе.** Рекурсивные распознаватели являются обычным местом для реализации блокирования DNS с помощью целого ряда инструментов (как коммерческих, так и с открытым кодом), позволяющих оператору распознавателя легко осуществлять блокирование.[12] Однако, в связи с особенностями архитектуры DNS, блокирование на рекурсивном распознавателе находится в ряду тех, которые легче всего обойти. Рекурсивные распознаватели, обычно управляемые поставщиками интернет-услуг конечного пользователя, собирают данные DNS с полномочных серверов по запросу конечных

[12] См. http://blog.operationreality.org/2011/10/05/belgian-isps-to-block-pirate-bay-domain-names/ и http://news.cnet.com/8301-13578_3-57472718-38/pirate-bay-blocks-did-little-to-curb-file-sharing/.

пользователей. Когда конечный пользователь хочет соединиться с веб-сайтом или другой службой, рекурсивный распознаватель, обслуживающий этого конечного пользователя, переводит доменное имя сайта или службы в соответствующий IP-адрес. Целью блокирования DNS через рекурсивный распознаватель является фильтрация, изменение или блокирование этого перевода, которые могут быть выполнены несколькими способами.

a. **Через перенаправление.** При этой форме блокирования через рекурсивный распознаватель ответ, полученный с полномочного сервера, модифицируется с целью замены значений, указанных в политике блокирования DNS. Например, вместо IP-адреса нежелательного веб-сервера рекурсивный распознаватель возвращает IP-адрес сервера восстановления, который отображает сообщение о том, что сайт блокирован.[13]

   Эта форма блокирования требует от сервера восстановления поддержки всех протоколов и служб, используемых исходными конечными серверами, для которых отображение сообщения о перенаправлении является технически возможным. Таким образом, если объект блокировки использует протокол передачи файлов (FTP) для предоставления контента, сервер, на который перенаправляется пользователь, также должен использовать FTP для отображения сообщения.[14] В связи с особенностями функционирования некоторых протоколов этот тип перенаправления возможен не во всех случаях.[15] Однако для наиболее распространенных протоколов, таких как протокол передачи гипертекста (HTTP, основной протокол Интернета), этот тип перенаправления возможен.

b. **Через код ответа несуществующего доменного имени (NXDOMAIN)**. Как и в случае с перенаправлением, при использовании этой формы блокирования изменяется ответ от полномочного сервера; однако вместо возвращения IP-адреса другого сервера ответ содержит указание о том, что запрашиваемый домен не существует.

---

[13] См. http://www.sigcomm.org/sites/default/files/ccr/papers/2012/July/2317307-2317311.pdf.

[14] См. «Протокол передачи файлов» по адресу http://en.wikipedia.org/wiki/File_Transfer_Protocol.

[15] См. «Перенаправление в доменах COM и NET (9 июля 2004 г.)», Консультативный комитет по безопасности и стабильности ICANN по адресу http://www.icann.org/en/groups/ssac/report-redirection-com-net-09jul04-en.pdf.

c. **С использованием кода ответа на запрос REFUSED.** В протоколе DNS имеется код REFUSED (ОТКАЗ), который указывает на то, что домен является неразрешимым по административным причинам. Блокирование DNS может осуществляться посредством изменения ответа от полномочного сервера на ответ REFUSED для заблокированных доменов.

   Одной из абсолютно действительных и разумных интерпретаций спецификаций протокола DNS является указание посредством кода ответа REFUSED на то, что данный сервер имен вообще не должен опрашиваться, результатом чего может оказаться удаление операционной системой этого рекурсивного распознавателя из списка серверов имен. Это происходит, потому что ответ REFUSED интерпретируется как проблема управления доступом для клиента и для всех доменных имен, запрашиваемых этим клиентом, а не как отказ в ответе на запрос об определенном доменном имени. При достаточном количестве запросов конечных пользователей этот тип блокировки может привести к удалению всех серверов имен, используемых конечным пользователем, и к тому, что компьютер конечного пользователя окажется неспособным к запросу любого имени. Таким образом, возврат кода REFUSED для блокируемого домена может привести к нанесению непоправимого косвенного ущерба.

d. **С использованием других кодов ответа.** Существуют дополнительные коды ответа, содержащиеся в протоколе DNS, которые могут использоваться для сигнализации о неразрешимости домена и для указания на то, что произошла та или иная ошибка. Эти коды ответов включают «сбой сервера» (SERVFAIL), «не реализовано» (NOTIMPL), и «ошибка формата» (FORMERR).

   Как и в случае с кодом REFUSED, блокирование с использованием этих кодов ответа может привести к тому, что операционная система объявит рекурсивный распознаватель нефункциональным и удалит его из списка рекурсивных серверов имен, опрашиваемых операционной системой. По этой причине ни один из этих альтернативных ответов не подходит для блокирования DNS.

e. **Посредством отсутствия ответа на запрос.** Наконец, рекурсивный распознаватель может быть настроен на игнорирование запросов того или иного домена. Это может привести к повторным попыткам приложений соединиться с

блокируемым сайтом и выполнить разрешение посредством нескольких итераций запроса.

Как и при использовании кода REFUSED и других кодов ответа, операционная система может удалить рекурсивный распознаватель из списка серверов имен, опрашиваемых для любого имени (а не только для блокируемого). Однако, в отличие от блокирования с использованием описанных выше кодов ответа, блокирование посредством невозвращения ответа приводит к значительно менее эффективному взаимодействию с пользователем, поскольку приложение должно ожидать истечения времени ожидания всех операций поиска. Это может побудить пользователей к поиску альтернативных рекурсивных распознавателей и потенциальному использованию серверов, не охватываемых указом о прекращении деятельности или соответствующей политикой блокирования.

Перенастройка рекурсивных распознавателей зависит от операционной системы, но обычно требует лишь нескольких щелчков мышью в графическом интерфейсе пользователя «Параметры системы», а многие приложения в общих операционных системах и интеллектуальных устройствах также позволяют выполнить это одним щелчком. Практически во всех случаях эту перенастройку способны выполнить все, кроме самых технически неграмотных пользователей.

Как упоминалось ранее, блокирование посредством рекурсивных распознавателей сегодня является одной из наиболее распространенных форм блокирования DNS; однако конечные пользователи могут обойти эту форму блокирования посредством использования рекурсивного распознавателя, который не выполняет блокирование, например «открытого» распознавателя, принимающего запросы с любого IP-адреса источника,[16] либо посредством использования собственных рекурсивных распознавателей.

Кроме того, поскольку при блокировании DNS на базе рекурсивных распознавателей переписываются или изменяются ответы на запросы DNS, получаемые от полномочных серверов, нарушается цепочка модели доверия, используемая DNSSEC, и генерируются ошибки, связанные с DNSSEC. Эти ошибки могут привести конечного

[16] Среди популярных открытых распознавателей можно назвать OpenDNS (http://www.opendns.com/) и Google Public DNS (https://developers.google.com/speed/public-dns/).

пользователя к заключению, что рекурсивный распознаватель DNS испытывает проблемы или подвергся атаке. Это заключение будет правдоподобным, поскольку при использовании DNSSEC ответы на запросы DNS, переписываемые по требованию правительственных органов, технически ничем не отличаются от тех, которые можно наблюдать при вредоносном заражении кэша.

6. Сравнение блокирования DNS на базе полномочных серверов и реестра с блокированием на базе рекурсивных распознавателей

Некоторые страны, например Великобритания или США, принимая меры в доменах высшего уровня .uk[17] или .com[18] соответственно, наложили арест на доменные имена, обслуживаемые реестрами, работающими в пределах границ этих стран. В некоторых случаях доменное имя было приостановлено в реестре, в других случаях записи DNS были изменены для перенаправления трафика на веб-сайт, контролируемый правительством.

Учитывая, что количество заблокированных доменных имен невелико и что задача создания новых доменных имен, обслуживающих ту же аудиторию и с той же целью, не является обыденной или не требующей вложений, наложение ареста на доменное имя может быть эффективным при блокировании интернет-контента. Поскольку меры в ДВУ предпринимаются в точке публикации, все заблокированные имена будут глобально удалены из всех рекурсивных распознавателей DNS в сравнительно короткие сроки, а именно в течение жизненного цикла блокируемых записей DNS.

Когда наложение ареста на домен выполняется на уровне реестра, DNSSEC[19] продолжает функционировать должным образом, поскольку данное действие является модификацией содержимого DNS в источнике и поэтому, учитывая, что подписи DNSSEC восстанавливаются надлежащим образом, цепочка доверия DNSSEC не разрывается.

Однако если реестр, предоставляющий подлежащие блокированию имена, расположен в другой юрисдикции, может потребоваться содействие правоохранительных или правительственных органов из других юрисдикций. Это может оказаться проблематичным, если законодательство другой страны оказывается несовместимым или же правоохранительные

[17] См. http://news.techworld.com/personal-tech/3319654/police-take-down-2000-couk-domains-selling-counterfeit-goods/.

[18] См. http://en.wikipedia.org/wiki/Operation_In_Our_Sites_v._2.0.

[19] См. http://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions.

организации не имеют подробно разработанных договоров о взаимопомощи, соглашений о взаимодействии, сотрудничестве или координации действий, например, через Интерпол. Таким образом, прекращение деятельности домена на уровне реестра является наиболее практичным в пределах одной юрисдикции, хотя в последнее время наблюдается улучшение в сфере координации и сотрудничества между правоохранительными органами. Например, сотрудничество может быть достигнуто через обеспечение правопорядка в рамках участия в процессах заинтересованных сторон ICANN или посредством создания специальных оперативных групп в рамках организаций; примером может служить создание Европейского центра по борьбе с киберпреступностью (E3C) в рамках Европола.[20]

Блокирование DNS на уровне полномочного сервера требует от оператора этого сервера внесения изменений в зону, получаемых от реестра, без авторизации этим реестром. Если полномочные серверы находятся в ведении нескольких организаций, это может вызвать осложнения. Если операторам одного или нескольких полномочных серверов не удается отобразить одни и те же изменения в одной и той же версии зоны, для одного и того же запроса могут быть возвращены непоследовательные результаты, в зависимости от того, какие опрашивались преобразователи, какие полномочные серверы опрашивались преобразователями, когда выполнялись запросы и т.д. Кроме того, если оператор полномочного сервера не является также владельцем ключа подписи зоны (ZSK), модификации зоны, выполненные оператором полномочного сервера, не будут подписаны, что приведет к ошибкам при проверке цепочек доверия DNSSEC для распознавателей, выполняющих проверку. В результате всего этого данная форма блокирования, как правило, нецелесообразна.

Использование блокирования DNS на базе рекурсивных распознавателей позволяет избежать этих проблем с юрисдикцией, поскольку указы о прекращении деятельности адресованы поставщикам интернет-услуг или другим операторам распознавателей, находящимся в той же юрисдикции, что и орган, требующий такого прекращения. Компромисс заключается в том, что, поскольку различные сетевые операторы во всем мире работают с рекурсивными распознавателями, невозможно обеспечить полный охват без скоординированных и всеобщих усилий, направленных на фильтрацию путей данных и манипуляцию полезными данными. Кроме того, такой подход не выдержит сквозной проверки DNSSEC на уровне приложений, как описывается в следующем разделе. Однако по крайней мере в одном исследовании было показано, что в связи с явлением, известным как «восходящая фильтрация», меры по фильтрации или блокированию контента, предпринятые поставщиком интернет-услуг в одной стране, могут

[20] См. https://www.europol.europa.eu/content/press/european-cybercrime-centre-be-established-europol-1417.

привести к блокированию контента в другой стране в результате договоренностей о маршрутизации между поставщиками.[21] Непреднамеренные последствия подобного рода действий экстерриториальных руководящих органов могут проявиться в увеличении эксплуатационных расходов и снижении стабильности для всех операторов и пользователей Интернета.

7. Блокирование DNS в рекурсивных распознавателях приводит к конфликту с DNSSEC

Как обсуждалось в предыдущих разделах, реализация DNSSEC может оказывать значительное влияние на мероприятия по блокированию DNS. DNSSEC представляет собой набор расширений протокола DNS, разработанных для решения проблем, связанных с подлинностью данных в DNS. Поскольку DNSSEC-совместимые приложения еще не получили широкого распространения, потребность в таких приложениях является ключевым фактором разработки и развертывания DNSSEC. Сквозное развертывание DNSSEC необходимо для обеспечения поддержки криптографической аутентификации в действующих и разрабатываемых приложениях, чувствительных к безопасности, что необходимо для сохранения доверия общественности к глобальной сети Интернет.

Эффективное блокирование DNS через рекурсивные распознаватели входит в конфликт с целью и функционированием DNSSEC. Это происходит потому, что инициатива DNSSEC предназначена как раз для распознавания именно таких изменений, которые возникают при блокировании, хотя сам термин «блокирование» подразумевает, что изменения вносятся в соответствии с законодательством и другими нормами, оговоренными заинтересованными сторонами. Изменения, вносимые в связи с блокированием, неотличимы от тех изменений, которые призвана обнаруживать DNSSEC, например при обнаружении преступников, умышленно внедряющих ложные ответы на запросы DNS с целью перенаправления трафика на поддельные службы. Все модификации, внесенные в подписанные DNSSEC данные, выглядят идентично вредоносным попыткам «заражения» DNS, поскольку в рамках DNSSEC не существует функции или сигнала, способного сообщить получателю, что данный ответ подписан органом, отличным от владельца домена. Это верно в случаях приостановки доменов, когда целью является простой запрет веб-сайта, а также в случаях перенаправления, когда целью является отображение официального сообщения о перехвате или прекращении деятельности вместо веб-сайта и выполняется это посредством переадресации. В любом случае распознаватель конечного пользователя при проверке подписанных DNSSEC ответов сможет установить факт

[21] См. https://citizenlab.org/2012/07/routing-gone-wild/.

фальсификации, но не сможет определить ее причину. Действия распознавателя конечного пользователя при обнаружении подобных фальсификаций могут включать использование обходных путей, таких как игнорирование локального рекурсивного распознавателя, итеративно разрешающего всю цепочку доверия от корня до самого полномочного сервера.

Блокирование DNS на уровне рекурсивного распознавателя может быть использовано в качестве временной меры. В частности, если необходимость блокирования или фильтрации DNS возникает только тогда, когда либо владелец доменного имени, либо конечный пользователь не использует DNSSEC, то модифицированные данные будут приняты распознавателями конечного пользователя и использованы приложениями, такими как, например, веб-браузеры. Однако обходной путь для владельца домена, не желающего, чтобы его домен оказался заблокированным, будет заключаться в подписи данных DNS, а обходной путь для конечных пользователей, не желающих, чтобы их содержимое было заблокировано таким образом, будет заключаться в активации DNSSEC в своих распознавателях-заглушках.[22] Отсюда и определение — «временная мера».

Хотя часто считается, что проверка DNSSEC может или должна выполняться только «в сети», при этом игнорируются потребности приложений, поддерживающих DNSSEC. DNSSEC может использоваться в сети для защиты кэша DNS от зараженных данных, и в первые годы развертывания DNSSEC это была единственная область использования DNSSEC в Интернете. Однако в долгосрочной перспективе предполагается создание совершенно нового класса DNSSEC-совместимых приложений для конечных пользователей, которые будут использовать такие технологии, как Проверка подлинности именованных объектов (DANE) на базе DNS; эта работа уже ведется в Комиссии по технологиям Интернета (IETF).[23] Рабочая группа DANE в настоящее время занята стандартизацией механизма, в соответствии с которым идентичность защищенного веб-сервера и безопасность соединения между браузером и этим защищенным веб-сервером усиливается посредством DNSSEC, а не посредством устаревшей и подверженной ошибкам сети центра сертификации X.509.[24]

---

[22] Распознаватели-заглушки представляют собой минимальные распознаватели DNS, которые используют режим рекурсивного запроса для перекладывания большей части работы по разрешению DNS на рекурсивный сервер имен. Почти все интернет-устройства содержат распознаватели-заглушки, и почти все сети доступа предоставляют своим клиентам рекурсивный сервер имен. См. http://en.wikipedia.org/wiki/Stub_resolver#Stub_resolvers.

[23] См. https://datatracker.ietf.org/wg/dane/charter/.

[24] Примеры последних изменений X.509 включают компромиссные решения Diginotar (см. http://en.wikipedia.org/wiki/DigiNotar) и компромиссные решения, такие как Comodo Registration Authorities (см. http://blogs.comodo.com/it-security/data-security/the-recent-ra-compromise/).

В результате попыток использования DNSSEC в качестве общей инфраструктуры, на которой будут построены защищенные приложения, можно констатировать, что блокирование DNS на уровне рекурсивных распознавателей либо оказывает отрицательное влияние на развертывание DNSSEC, либо само оказывается неэффективным, как только реализация DNSSEC становится более широкой. В мировой экономике может существовать либо защищенное интернет-именование и в связи с этим защищенные интернет-приложения, либо эффективное блокирование содержимого через DNS Интернета, но не то и другое одновременно.

8. Другие последствия блокирования DNS

Блокирование и фильтрация DNS могут иметь и другие отрицательные последствия, помимо описанных в предшествующих разделах. Наиболее очевидные из них — это избыточное блокирование и маршрутизация трафика DNS в обход точек блокирования.

8.1 Избыточное блокирование

При использовании технологий блокирования DNS всегда существует риск возникновения ошибок в списке объектов, подлежащих блокированию. Это не зависит от того, основано ли блокирование на доменных именах или других идентификаторах, таких как IP-адрес или универсальные локаторы ресурсов (URL-адреса). В связи с этим процессы, используемые при рассмотрении элементов, подлежащих включению в тот или иной список, должны быть безопасными, надежными и допускающими возможность интенсивных проверок. Списки, используемые в примерах блокирования, описанных в настоящем отчете, происходят из различных источников: частных организаций, сотрудничающих правоохранительных органов, судов или законодательных органов. ККБС не стремится определить, какой из процессов является наилучшим, но рекомендует несколько механизмов для обеспечения технической стабильности: четкие правила, касающиеся объекта блокирования и четко определенный процесс рассмотрения и принятия решения.

Кроме того, необходимо учитывать, что если блокирование осуществляется в отношении такого домена, как, например, example.com, то при блокировании с использованием системы доменных имен будет заблокирована не только возможность поиска доменного имени при попытке доступа к контенту по заблокированному URL-адресу http://example.com/bad-content.html, но и все другие URL-адреса, использующие то же доменное имя, например *http://abc.example.com/ или http://example.com/good-content.html*. При блокировании DNS будет также заблокирован поиск доменного имени для всех других служб — электронной почты, управления сетью, передачи файлов и т.д., — которые используют тот

же домен, и, кроме того, для всех дочерних доменов *example.com* (например, *subdomain.example.com*).[25]

Наконец, в любом режиме фильтрации, будь то DNS или что-либо еще, жизненно необходимо избегать ошибок в создании объектов для блокирования. Например, опечатка при вводе данных может привести к сбою блокировки нужного домена и к случайной блокировке домена, не имеющего никакого отношения к необходимости блокирования.Интернационализированные доменные имена (ИДИ) могут быть источником повышенной опасности, поскольку два ИДИ могут выглядеть одинаково и при этом различаться внутри DNS.

8.2 Маршрутизация DNS-трафика из страны, которая осуществляет блокирование

Действия правительственных органов, которые приводят к блокировке домена, могут быть направлены на то, чтобы конечные пользователи предпринимали меры к обеспечению маршрутизации своего DNS-трафика через серверы имен, расположенные за пределами страны, например посредством использования частных виртуальных сетей или конкретных рекурсивных распознавателей, вместо тех, которые эксплуатирует поставщик услуг доступа. При такой «офшорной» маршрутизации запросов доменного имени мониторинг и управление DNS могут передаваться в другие страны, при этом срываются мероприятия, направленные на борьбу с киберпреступностью внутри страны, осуществляющей блокирование, а деятельность объектов за пределами страны, связанная с киберпреступностью, усиливается. Помимо дополнительных задержек, которые могут возникать в связи с этим, подобная внешняя маршрутизация DNS-трафика может оказать воздействие на производительность Интернета внутри блокирующей страны, поскольку многие сети доставки контента принимают решения в отношении того, какую информацию возвращать в ответ на запросы DNS, на основании IP-адреса распознавателя, отправляющего запрос. Использование нерегиональных серверов может привести к неожиданному пересечению трафиком международных каналов.

Переключение на другой сервер имен, независимо от того, является ли он частью DNS, координируемой ICANN, или принадлежит другой системе, может быть выполнено путем простой перезаписи конфигурации компьютера; этому в значительной степени способствует наличие дружественного графического интерфейса пользователя в большинстве

[25] См. http://gigaom.com/europe/orange-censors-all-blogs/, http://www.circleid.com/posts/20120917_microsoft_takedown_of_3322_org_a_gigantic_self_goal/, и http://www.techdirt.com/articles/20110220/17533013176/ice-finally-admits-it-totally-screwed-up-next-time-perhaps-itll-try-due-process.shtml

современных компьютерных систем. Даже если тот или иной человек не имеет необходимых знаний для изменения параметров DNS своего компьютера (или сети), опубликовано и доступно для загрузки множество сценариев и пользовательских приложений, автоматизирующих модификацию DNS. Одним из примеров является подключаемый модуль MAFIAAFire, опубликованный по завершении первых этапов инициативы Службы иммиграции и таможенного контроля США под названием Operation In Our Sites.[26]

8.2.1 Последствия смены пользователями распознавателей

Данные DNS дают поставщикам интернет-услуг важное и точное представление как о структуре трафика, так и об угрозах безопасности в их сетях. Эта информация позволяет поставщикам интернет-услуг выявлять увеличения и сдвиги трафика, что может оказывать влияние на принятие бизнес-решений. Еще более важным является то, что мониторинг данных DNS поддерживает сетевую безопасность, часто позволяя поставщикам интернет-услуг диагностировать атаки типа «отказ в обслуживании» и выявлять зараженные узлы, подвергшиеся атакам домены и уязвимых пользователей.

Поскольку пользователи все чаще обращаются к серверам DNS, отличным от предоставляемых их поставщиками интернет-услуг, у этих поставщиков снижается способность управлять угрозами безопасности и поддерживать эффективные сетевые операции. Сокращение использования клиентами корпоративных, локальных сетей или DNS-служб поставщиков интернет-услуг означает, что большее количество компьютеров, подвергшихся атакам, не будет идентифицировано и вылечено. Кроме того, набор атрибутов конфигурации Интернета, которые необходимо оценить при обращении клиента в службу технической поддержки оператора, будет значительно более обширным, а значит возрастет сложность и стоимость отладки.

Изложенные выше вопросы могут создавать проблемы для правительственных органов тех стран, в которых расположены поставщики интернет-услуг. Эти правительственные органы могут потерять возможность получения разведывательной информации посредством возможных соглашений об обмене данными с операторами сетей и интернет-служб, а также оказаться без информации, которая могла бы иметь доказательственную силу в расследованиях, проводимых правоохранительными органами. Например, правительство США могло бы не получить достаточных доказательств в отношении управления бот-сетями, а также структурами управления и зараженным кэшем, чтобы инициировать важное расследование, получившее

[26] См. https://addons.mozilla.org/en-US/firefox/addon/mafiaafire-redirector/ and http://en.wikipedia.org/wiki/MAFIAAFire_Redirector.

название Operation Ghost Click, в ходе которого были закрыты серверы, распространяющие вредоносную программу DNSChanger.[27]

Вопросы, связанные с правоохранительной деятельностью, встают особенно остро, когда пользователь выбирает DNS-сервер в другой стране. Возможность применения юридических процессов для решения той или иной проблемы сокращается, когда серверы находятся вне юрисдикции данного правоохранительного органа.

8.2.2 Нарушение локализации CDN при смене пользователями распознавателей

Маршрутизация DNS-трафика таким образом, что он не соответствует топологии сети, например через DNS-серверы вне данной страны, также негативно влияет на производительность сети (в пределах страны, за счет увеличения среднего времени приема-передачи и распространения) и вызывает увеличение расходов поставщиков интернет-услуг. Например, если пользователи меняют распознаватели, чтобы избежать блокирования, в результате локализация CDN может не работать и конечный пользователь будет направлен к контенту узлов CDN, расположенных на серверах за пределами его страны, а не тех, которые размещены в сети доступа пользователя и имеют прямые каналы внутренней связи.

Сети CDN обычно локализуют доставку контента распределяя одно и то же содержимое по серверам в широком спектре сетей по всему миру. Эта локализация способствует уменьшению нагрузки на каждый отдельный сервер и сводит к минимуму потребление сетевых ресурсов и перегрузок благодаря доставке контента с сервера, расположенного как можно ближе к пользователю.Многие сети CDN определяют местоположение пользователя на основе IP-адреса распознавателя DNS; при этом пользователи, которые перешли на распознаватель DNS за пределами своей страны, будут распознаваться сетью CDN как просматривающие Интернет из-за рубежа. Результат будет иметь негативное влияние на производительность и стабильность для таких пользователей CDN, а также приведет к увеличению расходов поставщиков услуг Интернета, транспортирующих соответствующий трафик.

9. Заключение и дополнительная литература

Хотя блокирование доступа к содержимому через DNS стало более распространенным, как сама тема исследования, так и ее реализация влечет за собой ряд технических проблем. Блокирование на уровне реестра DNS (непосредственно или через регистратора) связано с наименьшим

[27] См. http://www.fbi.gov/news/stories/2011/november/malware_110911.

количеством технических осложнений и совместимо с DNSSEC, однако может идти вразрез с проблемами юрисдикции или привести к долгосрочной «балканизации» пространства имен Интернета. Блокирование на уровне полномочных серверов связано с аналогичными проблемами юрисдикции, однако несовместимо с DNSSEC в тех случаях, когда оператор полномочного сервера одновременно не имеет возможности корректно подписать зону, содержащую блокируемое имя. Наконец, блокирование на уровне распознавателя, несмотря на распространенность, в лучшем случае проблематично с точки зрения DNSSEC, а в худшем — может препятствовать развертыванию DNSSEC.

Правительственные и другие органы должны учитывать эти проблемы и четко представлять себе технические последствия при разработке политик блокирования или фильтрации содержимого Интернета через DNS.

Рекомендуемые дополнительные материалы по данному вопросу включают следующие статьи:

- *Shutdowns, Suspensions, Seizures, Oh My!*, D. Piscitello, http://securityskeptic.typepad.com/the-security-skeptic/2012/08/shutdowns-suspensions-seizures-oh-my.html.
- *Preventing Access or Removing Content – Laser Scalpel or Saw?*, D. Piscitello, http://securityskeptic.typepad.com/the-security-skeptic/2012/08/preventing-access-or-removing-content-laser-scalpel-or-saw.html.
- *A Chainsaw is a Poor Choice for Surgery and for Blocking Content*, D. Piscitello, http://securityskeptic.typepad.com/the-security-skeptic/2012/08/a-chain-saw-is-a-poor-choice-for-surgery-and-for-blocking-content.html.
- *Alignment of Interests in DNS Blocking*, P. Vixie, http://www.circleid.com/posts/20110723_alignment_of_interests_in_dns_blocking/.

10. Благодарности, заявления о заинтересованности, возражения и отказы от участия

В этих разделах читателю предоставляется информация по трем аспектам нашего процесса. В разделе «Благодарности» перечислены участники, которые внесли свой вклад в подготовку настоящего документа. В разделе «Заявления о заинтересованности» содержатся ссылки на биографии членов Комитета и любые конфликты интересов (фактические, кажущиеся или потенциальные), которые могут отразиться на материалах настоящего документа. Раздел «Возражения и отказы от участия» предоставляет возможность отдельным членам выразить свое несогласие с содержанием настоящего документа или процессом его подготовки.

10.1 Благодарности

Комитет выражает свою благодарность следующим членам ККБС и другим лицам, внесшим свой вклад, за потраченное время, усилия и анализ, выполненный при подготовке настоящего отчета.

Ален Айна (Alain Aina)
Яап Аккергиус (Jaap Akkerhuis)
Дон Блюменталь (Don Blumenthal)
КС Клэффи (KC Claffy)
Дэвид Конрад (David Conrad)
Патрик Фальтстром (Patrik Fältström)
Джеймс Гэльвин (James Galvin)
Уоррен Кумэри (Warren Kumari)
Джейсон Ливингуд (Jason Livingood)
Дэнни Макферсон (Danny McPherson)
Рэм Мохан (Ram Mohan)
Пол Викси (Paul Vixie)

10.2 Заявления о заинтересованности

Биографические сведения о членах SSAC и о сферах их интересов содержатся по адресу: http://www.icann.org/en/groups/ssac/biographies-09oct12-en.htm.

10.3 Возражения и отказы от участия

Возражений и отказов от участия не поступило.