Руководство для ИТ-специалистов по идентификации и смягчению конфликтов имен

1 августа 2014 г.
Версия 1.1

Содержание

1. Введение

После ввода в корневую зону DNS нового доменного имени верхнего уровня организации могут столкнуться с тем, что запросы, которые преобразуют в адреса некоторые «внутренние» имена, специфичные для их сети, возвращают иные значения, выдавая пользователям и программам другие результаты. При этом возникают две основные проблемы: утечка «внутренних» имен в глобальный Интернет и конфликт частных пространств имен с глобальным пространством имен DNS.

Причина таких необычных результатов заключается в том, что запрос DNS, который администратор сети намеревался разрешить локально, используя внутреннее пространство имен, теперь разрешается с использованием данных о новом доменном имени верхнего уровня в глобальной системе DNS. При таких обстоятельствах, запросы, которые не должны были покинуть внутреннюю сеть, теперь получают результаты из глобальной DNS, отличающиеся от внутренних. Утечка имен, приводящая к получению других результатов, как минимум, может причинить беспокойство некоторым пользователям (например, стать причиной задержки доступа к веб-страницам). Кроме того, она может создать проблемы для безопасности (например, привести к отправке электронной почты не тем получателям).

Этот документ охватывает стратегии смягчения и предотвращения рисков для наиболее распространенных частных пространств доменных имен, используемых организациями. В настоящем документе описаны ситуации, которые могут возникнуть в организациях, столкнувшихся с утечкой внутренних имен в глобальную систему DNS, и изложены рекомендуемые практические методы смягчения отрицательных последствий. Предложенные здесь описания и рекомендации предназначены для ИТ-специалистов (сетевых администраторов, системных администраторов и сотрудников ИТ-отдела), которые в целом понимают принципы функционирования DNS и своих собственных внутренних систем имен. Читателям, которым необходимы более глубокие знания, предлагается ознакомиться с документами, перечисленными в Приложении A. В частности, читателям, заинтересованным в решении вопросов безопасности, рекомендуется ознакомиться с отчетами Консультативного комитета ICANN по безопасности и стабильности (ККБС).

Корпорация ICANN — администратор данных глобальной корневой зоны DNS — подготовила настоящий документ, проконсультировавшись с экспертами в области пространств доменных имен, чтобы помочь организациям, в которых частные пространства доменных имен могут конфликтовать с глобальной корневой зоной DNS. ICANN опубликовала и другие документы с описанием структуры глобальной системы DNS, процедуры добавления новых имен в корневую зону DNS и многого другого. Список этих документов для дополнительного чтения, посвященных многим вопросам, приведен в Приложении A. Кроме того, недавно ICANN начала помогать организациям, которые используют частные пространства имен, идентифицировать случаи возникновения соответствующих конфликтов. Об этом говорится в Разделе 1.4 и Разделе 6.

Обратите внимание, что, хотя в этом документе рассматриваются меры смягчения конфликтов имен, круг рассматриваемых проблем ограничен только теми, с которыми могут столкнуться организации при разрешении имен в адреса. В нем не рассматриваются другие проблемы, связанные с функционированием самой глобальной DNS. Например, корневым серверам имен глобальной DNS всегда поступало огромное количество запросов, которые не должны были обрабатываться глобальной DNS (см. документ *SAC 045* в Приложении A), однако корневые серверы имен всегда располагали достаточным количеством ресурсов для обработки этих лишних запросов. Соответствующие проблемы, касающиеся корневых серверов имен, не рассматриваются в настоящем документе. В нем рассматриваются только последствия непреднамеренной утечки запросов на общедоступные серверы корневой зоны DNS.

ICANN создала веб-страницу, на которой представлены информационные материалы о конфликтах имен: http://www.icann.org/namecollision. На этой странице также представлена процедура информирования об очевидном причинении серьезного вреда в результате конфликтов имен, причиной которых являются новые родовые домены верхнего уровня (рДВУ).

1.1 Конфликты имен

Глобальная DNS является иерархическим пространством имен, а имена в DNS состоят из одной или нескольких меток, формирующих полное имя. На верхнем уровне этой иерархии находится корневая зона DNS, содержащая группу таких имен, как com, ru, asia и другие; это глобальные ДВУ (домены верхнего уровня), которые часто называют просто «ДВУ» или «TLD». Примером полного доменного имени (которое часто называют *полностью определенным доменным именем* или *FQDN*) является www.ourcompany.com.

Почти все частные пространства имен также являются иерархическими. Есть три основных типа частных пространств имен:

- **Пространства имен, являющиеся ответвлением глобальной DNS.** Корневым элементом частного пространства имен, являющегося ответвлением глобальной DNS, служит имя, которое можно преобразовать в адрес глобальной DNS. Однако управление всей структурой каталогов под этим именем осуществляется локально с использованием имен, которые ИТ-администраторы не планируют делать видимыми в глобальной DNS. В качестве примера можно привести частное пространство имен, корневым элементом которого является winserve.ourcompany.com: управление именами в этом частном пространстве имен (winserve) осуществляет частный сервер имен, и эти имена не видны в глобальной DNS.

- **Пространства имен, использующие собственные корневые узлы с частными ДВУ.** Корневым элементом такого частного пространства имен служит одиночная метка, которая не является глобальным ДВУ. Управление всей структурой каталогов, включая частный ДВУ, осуществляют частные серверы имен, которые не видны в глобальной DNS. Например, если корневым элементом частного пространства имен служит метка ourcompany, то частные серверы имен также отвечают за управление доменами www.ourcompany, region1.ourcompany, www.region1.ourcompany и так далее. Существует множество разных видов пространств имен, использующих.собственные корневые элементы с частными ДВУ. В качестве примеров можно привести Active Directory компании Майкрософт (в некоторых конфигурациях), многоадресную систему DNS (RFC 6762) и старые службы каталогов ЛВС, которые все еще используются в некоторых уголках Интернета.

- **Пространства имен, которые создаются путем использования списков поиска.** Списком поиска называется функция локального определителя имен (для частного пространства имен или рекурсивного определителя для глобальной DNS). Список поиска позволяет пользователю вводить более короткие имена для удобства; во время разрешения сервер имен добавляет указанные при настройке имена справа от имени в запросе. (Эти указанные при настройке имена также называются *суффиксами*.)

Пространства имен, являющиеся ответвлением глобальной DNS, создают конфликты имен только в сочетании со списками поиска. Любой запрос, в котором указано полное доменное имя из глобальной DNS, по определению никогда не создаст конфликта с другим именем в глобальной DNS. Такой запрос может стать причиной только тех конфликтов имен, которые непреднамеренно созданы путем использования списков поиска.

Понятие «частные пространства имен» приводит в замешательство многих людей, которые привыкли главным образом к обычному применению Интернета, то есть тех людей, которые знакомы только с глобальной системой присвоения имен DNS и, возможно, с удивлением узнают, что некоторые запросы на разрешение имен не адресованы и не должны быть адресованы глобальной DNS. Возможно, они удивятся еще больше, когда узнают, что некоторые запросы на преобразование имен, намеренно созданные для частного пространства имен, в итоге попадают в глобальную DNS. Одной из возможных причин возникновения конфликтов имен является то, что запросы, предназначенные для сервера имен, находящегося в частном пространстве имен, вместо этого начинают обрабатываться в глобальной DNS.

1.2 Конфликты имен из-за частных ДВУ

Конфликты имен возникают в результате двух событий. Во-первых, запрос на разрешение полного доменного имени, размещенного в частном ДВУ, в результате утечки попадает из частной сети в глобальную DNS. Во-вторых, в глобальной DNS по запросу удается найти имя, которое точно совпадает с именем, существующим в частной сети в пространстве имен частного ДВУ.

Распространенная причина таких конфликтов имен — использование в системах, аналогичных Active Directory компании Майкрософт, имени, которое не является ДВУ в глобальной DNS на момент настройки системы, но впоследствии добавлено в глобальную DNS. Конфликты имен этого вида уже многократно возникали ранее, и ожидается, что они по-прежнему будут наблюдаться по мере внедрения новых ДВУ в глобальную DNS (см. документ *Введение в программу внедрения новых рДВУ* в Приложении А).

1.3 Конфликты имен из-за списков поиска

Другой причиной конфликтов имен является обработка списков поиска. Если в запросе не указано полное доменное имя — FQDN, то такое имя называется *кратким неполным именем*. Список поиска содержит один или несколько суффиксов. Они последовательно добавляются с правой стороны запроса. Если определитель не может выполнить разрешение краткого неполного имени, он добавляет суффиксы из списка при каждой попытке преобразовать доменное имя в адрес до тех пор, пока не будет найдено подходящее имя. Список поиска — полезная функция; однако обработка этого списка предусматривает использование кратких неполных имен, которые не являются FQDN и в силу этого непреднамеренно создают пространства имен, не размещенные в глобальной DNS. В этом случае конфликт имен возникает тогда, когда строка, которую пользователь намерен использовать как краткое неполное имя, вместо этого дополняется через список поиска и разрешается в адрес как полное доменное имя.

Предположим, например, что у определителя имен есть список поиска, содержащий суффиксы ourcompany.com и marketing.ourcompany.com. Предположим также, что пользователь вводит в программу, которая обращается к определителю, имя www. При этом вначале определитель будет искать имя www, но если это не даст результата, то он может начать поиск имен www.ourcompany.com и www.marketing.ourcompany.com.

Обратите внимание на слово «может» в описании данного примера. Правила применения списков поиска при выполнении операций разрешения имен меняются в зависимости от операционной системы и приложений. Некоторые системы перед применением списка поиска всегда попытаются выполнить разрешение имени либо в частном пространстве имен, либо в глобальной DNS. Однако другие системы сначала будут использовать список поиска, если искомая строка не содержит символа «.». Также есть системы, которые будут использовать список поиска, если искомая строка заканчивается символом «.». Правила применения списков поиска рядом операционных систем и приложений (например, веб-браузерами) неоднократно

менялись. Поэтому невозможно прогнозировать, когда списки поиска будут или не будут использоваться, что можно и что нельзя считать кратким неполным именем, и, следовательно, есть ли вероятность утечки кратких неполных имен в глобальную DNS. См. документ *Проблемы новых рДВУ: имена без точки и конфликты имен* в Приложении А, чтобы получить более подробную информацию о многообразии обработки списков поиска.

Это описание списков поиска может стать сюрпризом для некоторых читателей, потому что эти списки весьма распространены в таких местах, которые на первый взгляд, вроде бы не создают «частных пространств имен». Каждый суффикс в списке поиска определяет еще одно пространство имен, к которому можно обратиться в процессе разрешения имен. Это приводит к созданию частного пространства имен, надежно функционирующего только тогда, когда клиент направляет запросы только конкретным определителям этого пространства имен. В зависимости от реализации списков поиска, некоторые определители имен даже могут попытаться преобразовать краткое неполное имя, введенное пользователем или настроенное в программном обеспечении, перед добавлением любого из имен, включенных в список поиска. Например, ввод www.hr в одном месте Интернета может привести к получению одного результата от определителя DNS, однако ввод этой же строки в другом месте может привести к получению другого результата. Когда такое происходит, одно из этих пространств имен является «частным» по отношению к другому.

Использование списков поиска вместо разрешения полных имен (FQDN) через глобальную DNS повышает неопределенность результатов разрешения доменных имен. Конфликты имен, возникающие по причине использования списков поиска, трудно прогнозировать, потому что эти списки получили очень широкое распространение. Они являются частью программного обеспечения определителей имен во многих операционных системах, сетевом оборудовании, серверах и других компонентах. Программное обеспечение определителей имен функционирует по-разному в зависимости от используемой системы, различных версий одной и той же операционной системы и даже функции определения операционной системой или приложением источника сетевого запроса. Развертывание службы разрешения имен, которая осуществляет преобразование имен в адреса с использованием только глобальной DNS, служит лучшей гарантией устранения такой неопределенности и непредсказуемости результатов.

1.4. Помощь в определении конфликта имен в новых рДВУ

Начиная с 18 августа 2014 г. и далее при делегировании рДВУ из корневой зоны DNS ему необходимо ввести услугу *управляемого прерывания* сроком на 90 дней. В течение периода управляемого прерывания на различные DNS-запросы в отношении новых рДВУ полномочные серверы выдают легко определяемые ответы. Эти ответы нужны для того, чтобы предупредить организации, у которых возникнет конфликт имен, о том, что им необходимо предпринять немедленные действия для предотвращения возможного ущерба в связи с утечкой запросов.

Кроме того, начиная с той же даты некоторые рДВУ, уже присутствующие в корневой зоне, перед тем как делегировать определенные имена второго уровня в глобальную DNS, должны реализовать услугу управляемого прерывания сроком на 90 дней. Этим преследуется та же цель, что и выше: предупредить организации, допускающие утечку частных запросов о том, что им необходимо как можно скорее принять меры для смягчения возможного ущерба.

Обратите внимание, что эти правила применимы только к рДВУ, а не к национальным ДВУ (обычно называемым «нДВУ»). При добавлении нДВУ в корневую зону его оператор может принять решение о применении управляемого прерывания, но не обязан этого делать.

2. Проблемы, возникающие из-за конфликтов имен

Конфликты имен, причиной которых является утечка запросов из частных сетей в глобальную DNS, могут привести ко многим непредвиденным последствиям. Если на запрос получен положительный ответ, но при этом ответ поступил из глобальной DNS вместо ожидаемого ответа из частного пространства имен, отправившее запрос приложение попытается подключиться к системе, которая не входит в частную сеть, и эта попытка может оказаться успешной. Такое подключение может создать досадные помехи (стать источником задержки при разрешении имен). Оно также может создать проблемы для безопасности, например, уязвимость, которой можно будет воспользоваться в злонамеренных целях, в зависимости от операций, выполняемых приложением после подключения.

2.1 Направление на непредусмотренные веб-сайты

Предположим, что находящийся в частной сети пользователь вводит в адресной строке своего веб-браузера https://finance.ourcompany, и в этой сети есть пространство имен, частным ДВУ которого является ourcompany. Если запрос браузера на разрешение имени finance.ourcompany выполняется так, как ожидалось, то браузер получит IP-адрес внутреннего веб-сервера финансового отдела. Однако представим, что ДВУ ourcompany также входит в состав глобальной DNS, и у этого ДВУ есть доменное имя второго уровня (SLD) finance. Если произойдет утечка запроса, то после выполнения операции разрешения имени будет получен не такой IP-адрес, как в случае обработки запроса в частном пространстве имен. Теперь представим, что по этому другому IP-адресу может находиться веб-сервер. Браузер попытается подключиться к веб-серверу, расположенному в сети общего пользования — Интернете, а не к веб-серверу в частной сети.

Как было продемонстрировано ранее, точно такая же проблема может возникнуть даже в тех сетях, где нет частных ДВУ, но используются списки поиска. Рассмотрим браузер, который используется стандартным образом в сети, где у пользователей есть список поиска с именем ourcompany.com и пользователь вводит имя www.finance, чтобы попасть на узел www.finance.ourcompany.com. Теперь представим, что браузер использует с мобильного устройства сотрудник, находящийся в кафе. Если произойдет утечка этого запроса в Интернет и там есть ДВУ с именем financeто в результате запроса имя буде преобразовано в иной IP-адрес, например, в адрес совершенно другого узла, имеющего в глобальной DNS имя www.finance. Этот запрос может стать причиной попытки браузера подключиться к веб-серверу, находящемуся в совершенно другой части общедоступного Интернета, вместо веб-сервера, который был бы найден в случае поступления запроса на определитель частной сети.

Обычно при таком развитии событий пользователь понимает, что попал не на тот веб-сайт и немедленно покидает его. Однако браузер может передать веб-серверу большое количество данных, если «доверяет» ему по причине того, что этот веб-сервер имеет такое же доменное имя и считается узлом, который ранее просматривался в этом браузере. Браузер может автоматически ввести имя пользователя, используемое для входа в систему, или другие конфиденциальные данные, делая тем самым эту информацию доступной для захвата и анализа за пределами организации. При других обстоятельствах (например, в случае тщательно спланированной атаки на организацию) браузер может подключиться к сайту, который содержит вредоносный код, устанавливающий на компьютер опасные программы.

Обратите внимание, что использование протокола TLS и цифровых сертификатов может оказаться бесполезным для предотвращения ущерба из-за конфликтов имен; фактически, это даже способно усугубить ситуацию, создав у пользователя ложное ощущение безопасности. Многие центры сертификации (ЦС), которые выдают сертификаты для проверки подлинности имен в глобальной DNS, также выдают сертификаты для проверки подлинности кратких неполных имен в частных адресных пространствах, поэтому возможна ситуация, когда направленный не на тот сайт пользователь все-таки будет видеть действующий сертификат. Для получения более подробных сведений о сертификатах имен в частных пространствах имен см. документ *SAC 057* в Приложении A.

2.2 Отправка электронной почты не тем адресатам

Возможные последствия конфликтов имен не ограничиваются веб-браузерами. Электронная почта, предназначенная одному адресату, может быть отправлена другому адресату, если имена их узлов совпадают; например, электронное письмо, отправленное по адресу chris@support.ourcompany может быть доставлено пользователю с совершенно другой учетной записью, если ourcompany станет ДВУ в глобальной DNS. Даже в том случае, когда сообщение не доставлено конкретному пользователю электронной почты, могут быть предприняты попытки его отправки, способные сделать содержание почтового сообщения доступным для захвата или анализа за пределами организации.

Многие сетевые устройства — брандмауэры, маршрутизаторы и даже принтеры — можно настроить на отправку уведомлений или регистрацию данных в журнале по электронной почте. Если имя адресата, указанное для отправки уведомлений по электронной почте, впоследствии начнет конфликтовать с именем в глобальной DNS, уведомление может быть доставлено совершенно не тому адресату, которому оно предназначалось. Может произойти утечка находящихся в теле сообщения сведений о событиях или данных журнала, раскрывающих конфигурацию сети и поведение узлов, к непредусмотренному получателю. Выполняемый ИТ персоналом повседневный анализ параметров сети или трафика может быть нарушен, если целевому получателю не доставляются данные журнала или события, ставшие причиной отправки уведомления, невозможно расследовать или устранить.

2.3 Снижение безопасности

Конфликты имен, последствия которых не были смягчены, могут приводить к непредсказуемому поведению или ущербу для систем в частных сетях. Системы, функционирование которых определяется разрешением имен, выполняющие также функции обеспечения безопасности, *могут* надежно работать при использовании полных имен (FQDN) и разрешении этих имен через глобальную DNS.

Например, в брандмауэрах правила безопасности часто основаны на определении источника или места назначения потока пакетов. В качестве источника и места назначения пакетов используются адреса IPv4 или IPv6, однако многие брандмауэры также позволяют вводить их как доменные имена. Если используется краткое неполное имя, разрешение которого выполняется не так, как ожидалось, эти правила могут не обеспечить выполнение функций блокирования или пропуска трафика в соответствии с намерениями администратора. Аналогичным образом, в журналах брандмауэра часто используются доменные имена; при этом использование кратких неполных имен, которые преобразуются в адреса непредсказуемым образом, может помешать отслеживанию событий, анализу и реагированию. К примеру, анализирующий журналы ИТ-персонал способен недооценить важность события, потому что указанное в журнале краткое неполное имя может определять разные узлы, в зависимости от места создания журнала (то есть в одно и то же краткое неполное имя в журнале может быть

связано с двумя или несколькими разными IP-адресами). Данную проблему может усугубить тот факт, что большинство брандмауэров способно выступать в качестве самостоятельных определителей DNS или позволять администраторам использовать или настраивать списки поиска.

2.4 Системы, на которые конфликты имен оказывают влияние

Подключенные к сети системы следует проверять на предмет использования имен узлов, для которых корневым является частный ДВУ, или имен узлов, в основе которых находятся списки поиска. Во всех случаях такое «использование» необходимо заменить на использование полных имен (FQDN) из глобальной DNS. Ниже приведен неполный перечень систем или приложений, подлежащих проверке:

- **Браузеры.** Веб-браузеры позволяют пользователям указывать местоположение прокси-серверов HTTP, которые очень часто находятся в частных сетях. Проверьте, не созданы ли пользователями или сотрудниками ИТ-отдела персональные начальные страницы, закладки или поисковые системы: эти компоненты могут содержать ссылки на серверы частной сети. Кроме того, конфигурация некоторых браузеров позволяет задать источники получения информации об отзыве сертификатов SSL/TLS, в качестве которых могут быть указаны имена узлов частной сети.

- **Веб-серверы.** Веб-серверы позволяют получить содержимое HTML, в котором есть ссылки и метаданные, содержащие имена узлов. Проверьте, нет ли на веб-серверах частной сети содержимого с краткими неполными именами. Проверьте, не указаны ли в файлах конфигурации веб-серверов краткие неполные имена или другие узлы частной сети.

- **Пользовательские агенты электронной почты.** У всех почтовых клиентов, таких как Outlook и Thunderbird, есть параметры конфигурации, в которых указаны узлы получения электронной почты по протоколам POP или IMAP и узлы отправки электронной почты по протоколу SUBMIT; в качестве всех этих параметров могут использоваться имена узлов частной сети. Проверьте, не настроены ли эти приложения на получение информации об отзыве сертификатов SSL/TLS от узлов, которым присвоены краткие неполные имена.

- **Серверы электронной почты.** Проверьте, нет ли у серверов электронной почты конфигураций с перечнем кратких неполных имен или других локальных узлов, таких как шлюзы резервного копирования электронной почты, серверы автономных хранилищ и так далее.

- **Сертификаты.** Проверьте, не содержат ли приложения, использующие сертификаты X.509, например программы для телефонной связи и мгновенного обмена сообщениями, данные конфигурации, в которых в качестве места получения информации об отзыве сертификатов SSL/TLS указаны краткие неполные имена.

- **Другие приложения.** У пользовательских приложений может быть множество параметров конфигурации, хранящих имена узлов. Наиболее очевидным местом их хранения являются файлы конфигурации, но имена узлов также могут входить в состав многих видов данных приложения, ссылок на социальные сети или вики-сайты, и даже могут быть встроены в состав исходного кода приложения. Проверьте, нет ли среди этих данных конфигурации кратких неполных имен.

- **Сетевые устройства.** Проверьте входящие в состав сетевой инфраструктуры устройства — брандмауэры, системы защиты информации и управления событиями (SIEM), маршрутизаторы, коммутаторы, устройства мониторинга сети, системы обнаружения и предотвращения вторжений, VPN-серверы, DNS-серверы, DHCP-серверы, серверы журналов — на предмет наличия в их параметрах конфигурации кратких неполных имен других устройств частной сети.

- **Администрирование клиентов.** Проверьте средства централизованного администрирования клиентов, например инструменты настройки рабочих станций и сетевых устройств организации, на предмет наличия кратких неполных имен в конфигурациях (в частности, в списках поиска), текущее и исходное состояние которых контролируют эти системы.

- **Мобильные устройства.** Пользовательские устройства, например мобильные телефоны и планшеты, могут иметь параметры конфигурации, аналогичные параметрам некоторых перечисленных выше приложений, и в силу этого могут содержать в конфигурации краткие неполные имена узлов локальной сети.

Среди данных конфигурации всех этих устройств необходимо найти хранящиеся краткие неполные имена, чтобы обеспечить возможность изменения таких имен в случае изменения корневого узла частного пространства имен или в случае отказа от использования списков поиска.

3. Когда следует принимать меры по смягчению конфликтов имен

Иногда в глобальную корневую зону DNS добавляются новые имена, например в случае изменения названия страны или в случае регистрации корпорацией ICANN новых рДВУ. Оба типа доменов верхнего уровня добавлялись почти ежегодно в течение более чем двадцати лет. В 2013 г. и 2014 г. также были добавлены новые ДВУ, и совершенно очевидно, что в последующие годы их станет еще больше.

Исторические данные свидетельствуют о том, что при добавлении ДВУ в DNS возникали конфликты имен. Кроме того, исторические данные свидетельствуют об утечке имен из частных пространств в течение многих лет, которая в некоторых случаях имеет очень большую интенсивность. Для получения более подробных сведений см. документ *SAC 045* в Приложении A. История наглядно демонстрирует, что изоляция пространств имен и разрешения имен, которое должно осуществляться в рамках частных сетей, никогда не была такой тщательной, какой ее считают администраторы, и запросы на разрешение имен, которые по замыслу администраторов должны обрабатываться внутренними серверами имен, вместо этого иногда отправляются определителям в глобальной DNS.

Сетевые администраторы иногда принимают решения о выборе имен, исходя из предположений о неизменности списка имен в корневой зоне глобальной DNS, однако на самом деле этот список менялся и будет меняться с течением времени. Например, когда почти 25 лет тому назад был добавлен ДВУ cs, являющийся доменом Чехословакии, многие университеты использовали списки поиска, позволявшие пользователю ввести имя, заканчивающееся суффиксом cs, для поиска факультета информатики в составе полного доменного имени университета, и эти решения привели к неопределенности разрешения имен после добавления нового ДВУ в корневую зону, потому что теперь заканчивающиеся на cs имена стали полными доменными именами (FQDN) в глобальной DNS. Сетевые администраторы нередко забывают о необходимости постоянно иметь актуальную информацию об именах, находящихся в корневой зоне глобальной DNS, даже в том случае, когда эти имена не пересекаются с именами в частных пространствах имен (будь то частный ДВУ или список поиска).

ИТ-отделу рекомендуется как можно скорее начать работу по минимизации последствий конфликтов имен. Позиция «мы просто улучшим работу своих брандмауэров» может привести к устранению некоторых конфликтов, однако она никогда не позволит избавиться от всех конфликтов. Аналогичным образом, те, кто говорит «мы убедимся в том, что пользователи обращаются к нашим серверам имен» или «мы переведем удаленных сотрудников на использование сетей VPN», вероятно сократят количество конфликтов, но при этом оставшиеся конфликты будет еще труднее диагностировать.

Конфликты имен могут возникать независимо от используемых в имени символов; однако применение символов не из набора ASCII, таких как ä, 中 и й, в частных ДВУ усложняет анализ конфликтов. Определители могут отправлять запросы на разрешение подобных имен труднопредсказуемым образом, и эти запросы могут не соответствовать стандартам Интернета, поэтому выявление ситуаций, в которых возникнут конфликты имен, становится намного более трудной задачей.

Хотя корневая зона глобальной DNS в конечном итоге станет крупнее, чем в предыдущие годы, добавление в нее новых имен на самом деле вовсе не является необычным событием. При добавлении каждого нового ДВУ есть вероятность возникновения конфликтов имен с теми частными пространствами имен, в которых утечка в Интернет преимущественно остается без внимания. Организации используют имена и берут на себя риск конфликтов в течение многих лет.

Обратите внимание, что добавление новых имен в корневую зону DNS не является и никогда не станет проблемой для организаций, уже использующих в своей сети полные имена (FQDN) из глобальной DNS. Эти организации не столкнутся с необходимостью изменения принципов использования имен DNS, поскольку в их случае конфликты имен отсутствуют. Проблемы возникают только у организаций, которые используют частные ДВУ, или у организаций, которые используют списки поиска, позволяющие вводить краткие неполные имена, когда само сокращенное имя является допустимым именем в глобальной DNS.

3.1 Определение возможности конфликтов

Чтобы определить, возникнут или нет конфликты имен в частном пространстве имен вашей организации, вам необходимо идентифицировать и систематизировать все используемые организацией частные пространства имен и списки поиска DNS, а затем на основе этих источников составить перечень имен верхнего уровня. В большинстве организаций, как правило, существует одно пространство имен с единственным именем верхнего уровня, однако в некоторых организациях, особенно в тех, которые были объединены с другими организациями, также использовавшими частные пространства имен (например, в результате слияния или расширения бизнеса), есть несколько частных имен верхнего уровня.

Затем вам необходимо определить как текущее, так и ожидаемое содержимое корневой зоны глобальной DNS. Список имен, которые в настоящее время есть в корневой зоне глобальной DNS, находится по адресу http://data.iana.org/TLD/tlds-alpha-by-domain.txt. Чтобы выяснить, рассматривается ли вопрос о предоставлении имени, используемого в частном пространстве имен, в рамках текущей программы внедрения новых рДВУ, выполните следующие действия:

1. Перейдите по адресу https://gtldresult.icann.org/application-result/applicationstatus
2. Нажмите стрелку в столбце «String» («Строка»)
3. Просматривайте страницы, пока не найдете группу строк, содержащую имя из вашего частного пространства имен

Если составленный вами перечень частных ДВУ пересекается со списком имен в корневой зоне DNS, есть вероятность возникновения в будущем конфликтов имен. Поэтому необходимо срочно принять меры по смягчению ситуации.

Обратите внимание, что после ввода в корневую зону тех новых ДВУ, которые рассматриваются в текущем раунде программы, могут быть предложены новые домены верхнего уровня; в частности, список новых ДВУ может меняться и при этом могут возникнуть конфликты между именами из частных пространств имен и будущими новыми ДВУ. Кроме того, организации, использующие двухбуквенные частные ДВУ (например, ab), должны понимать, что двухбуквенные доменные имена верхнего уровня зарезервированы для использования в качестве кодов стран (национальных доменов), которые вводятся в корневую зону согласно совершенно другой процедуре.

3.2. РДВУ глобальной DNS, делегирование которых откладывается на неопределенный срок

ICANN заявила, что на неопределенное время откладывает делегирование трех ДВУ: .corp, .home и .mail. Эти рДВУ по-прежнему широко используются в частных пространствах имен, и поэтому представляют намного более высокий риск с точки зрения конфликтов, чем другие рДВУ. Не гарантируется, что эта отсрочка будет вечной, поэтому любая организация, использующая одно из таких имен в качестве частного пространства имен, должна по-прежнему соблюдать указания в Разделе 4 и Разделе 5 в отношении перехода из частного пространства имен. Однако такие организации будут располагать большим количеством времени для перехода, чем организация, использовавшая другое имя, которое может появиться в корне глобальной DNS в обозримом будущем.

4. Этапы смягчения проблем, связанных с частным ДВУ

Уже несколько десятилетий не рекомендуется использовать частные ДВУ. Фактически, в течение многих лет инструкции по применению Active Directory компании Майкрософт и серверных продуктов явным образом не поощряют использование частных ДВУ. Наиболее эффективной мерой по смягчению конфликтов имен, возникающих по причине утечки имен частных ДВУ в глобальную DNS, является переход от использования частного ДВУ к использованию домена, находящегося в глобальной DNS.

Описанные в настоящем разделе действия распространяются на любую сеть, в которой по субъективным причинам решено использовать в качестве корневого узла частный ДВУ или применять списки поиска для разрешения кратких неполных имен, вместо размещения пространства имен в рамках глобальной DNS и использования запросов на разрешение полных доменных имен, обрабатываемых в глобальной DNS. Настоящий раздел касается всех организаций, использующих частные ДВУ, а не только тех, где уже наблюдается утечка запросов на разрешение имен в глобальный Интернет. Если ваша организация использует то, что вы считаете «безопасным» частным ДВУ, то есть имя, на которое еще не подана заявка, или имя, делегирование которого в корневую зону глобальной DNS еще не утверждено, вам все равно следует серьезно рассмотреть возможность его замены на доменное имя, размещенное в глобальной DNS. Если вы работаете в крупной организации, имеющей несколько частных ДВУ (например, в компании, которая объединилась с другой компанией, но не произвела слияния двух пространств имен), то описанные в настоящем разделе меры необходимо принять в отношении каждого частного ДВУ.

По всей вероятности, когда организация принимала решение об использовании частного ДВУ, она подразумевала применение конкретного соглашения о присвоении имен. Предлагаемые здесь меры могут противоречить этой первоначальной модели. Чтобы гарантированно смягчить проблемы, связанные с конфликтами имен из-за наличия частных ДВУ, как пользователям, так и системам необходимо изменить принципы использования доменных имен, а конфигурацию локальных серверов имен необходимо поменять таким образом, который некоторые пользователи могут счесть неудобным. Для повышения осведомленности и содействия признанию предлагаемых мер среди вашего сообщества пользователей используйте описания непредвиденных или нежелательных последствий, способных повлиять на деятельность вашей организации.

Важное замечание. Одновременно выполнением описанных в настоящем разделе действий вам, возможно, потребуется смягчить конфликты имен, вызванные применением списков поиска, которые рассмотрены в разделе 5. Многие из описанных в указанном разделе мер аналогичны рассматриваемым в настоящем разделе и могут быть приняты одновременно с ними.

4.1. Мониторинг запросов, поступающих полномочным серверам имен

Чтобы смягчить проблемы, причиной которых является частный ДВУ, составьте список всех компьютеров, сетевого оборудования и любых других систем, использующих существующий частный ДВУ для каких-либо запросов. После изменения используемых имен потребуется обновить конфигурацию всех устройств, автоматически использовавших старые частные имена.

Существует три широко распространенных способа выполнения такого мониторинга и подготовки списка систем:

- У полномочных серверов (например, Active Directory) может быть функция ведения журналов. Включите эту функцию, чтобы собрать сведения обо всех запросах на разрешение частных имен.

- Многие современные брандмауэры также можно настроить на обнаружение и регистрацию в журналах запросов на разрешение частных имен. Это может оказаться не столь эффективной мерой, как ведение журналов в самой системе присвоения имен, в зависимости от топологии вашей сети. Например, если запрос не проходит через брандмауэр, то брандмауэр его не увидит, и поэтому данный запрос будет пропущен.

- Если нельзя использовать ни один из описанных выше способов, осуществляйте мониторинг и сбор входящего и исходящего трафика полномочных серверов имен при помощи программы для захвата пакетов, такой как Wireshark. Однако этот способ требует программной обработки захваченных данных для поиска только тех запросов, которые относятся к частным именам.

Некоторые организации захотят (и должны) принять несколько из вышеописанных мер для повышения вероятности обнаружения всех запросов. Обратите внимание, что выполнение этого этапа может привести к сбивающим с толку результатам. На таких устройствах, как компьютеры и телефоны, установлены приложения, предусматривающие ввод имен пользователем; эти устройства будут обнаружены в ходе анализа, даже несмотря на то, что в них отсутствуют какие-либо сохраненные варианты старых частных имен. Чтобы выполнить этот этап, необходимо знать только все места вашей сети, где старые частные имена хранятся и используются приложениями.

4.2. Составление перечня всех систем, использующих частные ДВУ в автоматическом режиме

Вам потребуется сводная информация из журналов, полученных на предыдущем этапе. Этой сводной информацией должен стать перечень всех устройств и всех указываемых в запросах имен, а не полный перечень всех случаев отправки запросов устройствами. Необходимость списка всех имен, содержащихся в запросах, обусловлена тем, что на некоторых устройствах может быть установлено несколько приложений, каждое из которых придется правильно настроить. Таким образом, эта сводная информация должна содержать как список всех систем, так и список всех установленных в каждой системе приложений, использующих частный ДВУ. Эта сводка станет перечнем устройств, конфигурацию которых необходимо изменить.

4.3. Определение лиц, занимающихся администрированием ваших имен в глобальной DNS

Наверняка, у вашей организации уже есть имя в глобальной DNS, и этот домен можно использовать для корневой зоны вашего частного пространства имен. Вам необходимо определить, кто отвечает за ваши имена DNS и какая процедура используется для создания и обновления имен в DNS. Эти задачи могут выполняться в рамках вашего ИТ-отдела или через поставщика услуг (которым часто является компания, обеспечивающая ваше подключение к Интернету).

4.4. Замена корневого домена вашего частного пространства имен на доменное имя из глобальной DNS

Распространенной стратегией использования имени из глобальной DNS в качестве корневого имени вашего частного пространства имен является получение в глобальной DNS общедоступного имени с последующим применением имеющегося у вашей организации полномочного сервера для администрирования всех имен, расположенных ниже. Например, если у вашей компании есть глобальное доменное имя ourcompany.com, в качестве корневого имени можно использовать ad1.ourcompany.com.

Если у вашей организации есть несколько доменных имен в глобальной DNS, вам следует разместить свои имена в той корневой зоне, которой сотрудникам ИТ-отдела вашей организации будет проще управлять. В некоторых случаях дополнительные имена контролируют другие субъекты, например отдел маркетинга. Если это возможно, лучше всего размещать корневое имя под именем, которое уже контролирует ИТ-отдел вашей организации.

Этапы такого изменения зависят от программного обеспечения частных серверов имен, которое у вас имеется, конкретной версии этого программного обеспечения, топологии серверов имен в вашей частной сети и существующей конфигурации серверов имен. Эти сведения выходят за рамки настоящего документа, однако они должны быть охвачены в инструкциях поставщика вашей текущей системы. Кроме того, во многих организациях это изменение потребует утверждения на некоторых уровнях управления, в частности, если схема управления именами глобальной DNS отличается от схемы управления частным пространством имен.

В рамках этого этапа, если у вас имеются сертификаты на какие-либо узлы, для которых используются имена из частного пространства имен, вам потребуется получить сертификаты на эти использование для этих узлов новых (полных) имен. Этапы получения этих сертификатов зависят от вашего ЦС и, таким образом, выходят за рамки настоящего документа.

4.5. Выделение узлам новых IP-адресов, если это необходимо

Если у вас есть сертификаты TLS, в основе которых лежит старое имя вашего частного ДВУ, вам потребуется получить новые сертификаты для новых имен. Если ваш веб-сервер не поддерживает расширение Server Name Indication (SNI) протокола TLS, которое позволяет обслуживать через TLS несколько доменных имен по тому же IP-адресу, вам потребуется добавить к узлам IP-адреса, чтобы узел поддерживал старое частное имя по первоначальному IP-адресу и новое имя по новому IP-адресу. В качестве альтернативы можно обновить программное обеспечение вашего веб-сервера до той версии, которая корректно обрабатывает расширения SNI.

4.6. Создание системы для мониторинга соответствия между новыми и старыми частными именами

После перенастройки всех частных имен на использование нового корня вы по-прежнему будете обслуживать адреса и регистрировать в журналах запросы, относящиеся к вашим старым частным именам, чтобы обнаружить системы, которые не вошли в перечень и не были обновлены и настроены на использование имен, находящихся в DNS. Поэтому вам потребуется убедиться в том, что у новых и старых частных имен одинаковые значения IP-адресов.

Ряд программ для обслуживания частных пространств имен позволяет поддерживать параллельно два дерева каталогов, но если у вас установлено более старое программное обеспечение или несколько полномочных серверов, то, возможно, придется осуществлять мониторинг соответствия с использованием специализированных средств. Эти специализированные средства должны часто направлять запросы на разрешение всех имен как в старом, так и в новом пространстве имен, и сообщать обо всех несовпадениях адресов, позволяющих определить, какие системы были изменены без параллельного изменения другой системы.

Если на предыдущем этапе вам потребовалось добавить IP-адреса из-за наличия сертификатов SSL/TLS, такие несовпадения необходимо разрешить в программном обеспечении для мониторинга соответствия.

4.7. Обучение пользователей и системных администраторов использованию нового имени

Помимо изменения систем, у которых имена введены в конфигурацию, вам необходимо изменить образ мышления пользователей, чтобы они начали использовать новые имена вместо старых частных имен. Это обучение должно предшествовать реализации последующих этапов, чтобы у пользователей было время привыкнуть к новым именам, однако во время обучения необходимо четко дать понять, что предстоящие изменения неизбежны, и вскоре придется перестраиваться на использование новых имен. Это также удачное время для обучения пользователей применению полных доменных имен (FQDN). Для повышения осведомленности и содействия признанию предлагаемых мер используйте описания непредвиденных или нежелательных последствий, способных повлиять на деятельность вашей организации.

4.8. Перевод всех затрагиваемых систем на новые имена

Этот тот момент, когда переход к использованию в сети новых имен вместо старых частных имен становится реальностью для всех систем (ПК, сетевых устройств, принтеров и так далее). Частные имена заменяются поочередно в каждой системе новыми именами DNS. В программном обеспечении системы необходимо обнаружить и заменить на новое имя DNS все экземпляры старого частного имени. Одновременно с этим следует прекратить использование кратких неполных имен в списках поиска.

Мониторинг, который был начат на предыдущем этапе, на данном этапе обретает исключительную важность. Маловероятно, что человек сможет обнаружить во всех системах все приложения, в которые встроены старые частные имена. Вместо этого после изменения каждой системы следует обращаться к данным мониторинга, чтобы узнать, не поступают ли по-прежнему из этой системы запросы на разрешение старых частных имен.

Во многих системах после их первоначального включения запускаются некоторые приложения для инициализации. В эти приложения могут быть встроены системные имена, обнаружение которых сопряжено с трудностями. После замены в системе всех старых частных имен на новые имена DNS перезагрузите эту систему и воспользуйтесь программным обеспечением для мониторинга, чтобы отследить операции поиска имен. Если система пытается найти какие-либо старые частные имена, вам необходимо определить программу, которая направляет этот запрос, и перенастроить ее на использование новых имен. Для выполнения этой процедуры и полной настройки системы надлежащим образом может потребоваться несколько перезагрузок.

4.9. Начало мониторинга использования старых частных имен на сервере имен

Вам необходимо настроить свой полномочный сервер имен так, чтобы начать мониторинг всех имен, имеющих старый корень. Так как ваши пользователи больше не должны использовать эти имена, созданный на этом этапе мониторинга журнал, возможно, не будет слишком большим; но если это не так, придется повторить некоторые из описанных выше этапов для конкретных систем вашей сети.

4.10. Настройка долгосрочного мониторинга по периметру для отслеживания старых частных имен

Во время предыдущих этапов необходимо было обнаружить подавляющее большинство случаев использования старых частных имен, но несколько (возможно ключевых) систем по-прежнему могут использовать старые частные имена, только крайне редко. Одним из способов обнаружения подобных запросов на разрешение имен является добавление в конфигурацию всех расположенных по периметру сети брандмауэров правил, обеспечивающих поиск любой утечки запросов. Этим правилам необходимо назначить высокий приоритет и настроить таким образом, чтобы создавались уведомления о событиях, позволяющие быстро оповестить ИТ-персонал. В качестве альтернативы можно просматривать журналы брандмауэров для поиска событий, но при этом высока вероятность пропуска. Оповещения в случае отправки запросов позволят сотрудникам обнаружить эти события, которые, как следует надеяться, теперь будут происходить редко. Некоторые брандмауэры поддерживают такой тип правил только как дополнительную платную функцию; если ваш брандмауэр относится к их числу, следует оценить целесообразность дополнительных расходов на обнаружение редких запросов.

4.11. Переадресация всех имен из старой корневой зоны на неработающий адрес

После обучения пользователей наиболее эффективным способом прекратить использование старых частных имен перед их удалением является переход на использование для разрешения всех старых частных имен сервера, который игнорирует любые запросы на обслуживание. Это также поможет очистить все системы, которые все еще используют старое пространство имен, но не были обнаружены на более ранних этапах.

Используемый адрес должен указывать на тот сервер, где гарантированно не запущена ни одна служба. Таким образом, исключается вероятность того, что какая-то система, использующая старые частные имена, получит неверную информацию. При этом приложения будут выдавать сообщения об ошибках, которые пользователи смогут легко обнаружить и понять; в рамках обучения следует рекомендовать пользователям сообщать ИТ-персоналу о любых ошибках подобного рода. По мере выполнения данного этапа, описанная выше система мониторинга, контролирующая соответствие между старыми и новыми именами, должна поддерживаться в актуальном состоянии в соответствии с вносимыми изменениями.

Имена следует заменять поочередно с интервалом по крайней мере в несколько часов между каждым изменением или группой изменений. На этом этапе скорее всего в ИТ-отдел будут поступать обращения, поэтому разделение изменений на этапы поможет сбалансировать количество таких обращений из-за того, что имена, которые еще используются, перестают функционировать.

4.12. Аннулирование всех сертификатов, которые были выданы для узлов со старыми частными именами

Если вашей организации были выданы сертификаты SSL/TLS для любых серверов сети, использующих старые частные имена, эти сертификаты следует аннулировать. Это достаточно просто сделать, если ваша организация является собственным ЦС. Если при получении сертификатов для частного пространства имен вы воспользовались услугами коммерческого ЦС, необходимо выяснить процедуру отправки в этот ЦС просьбы об аннулировании; разные ЦС могут предъявлять разные требования к таким просьбам.

4.13. Длительное использование нового имени

Обратите внимание, что старое частное имя и его подчиненные домены по-прежнему обслуживаются и будут обслуживаться до тех пор, пока функционирует сервер имен. Нет никаких причин для их удаления, а во многих системах, например в Active Directory, достаточно сложно удалить первое имя, которое было указано в настройках системы.

На самом деле, есть убедительная причина сохранить старое имя: это позволит обнаружить остаточные следы старого частного имени в системах вашей сети. Пока все адреса, связанные со всеми именами в этом частном ДВУ, указывают на узел, где не запущены никакие службы, вы можете использовать и журналы сервера имен (и, для дополнительного удобства, системные журналы входящего трафика на этом сервере) для определения того, насколько тщательно удалось удалить старое частное имя.

5. Этапы смягчения конфликтов имен, связанных со списками поиска

Чтобы гарантированно смягчить проблемы, связанные с конфликтами имен из-за наличия списков поиска, как пользователям, так и системам необходимо изменить принципы использования доменных имен. Может принести пользу заблаговременная подготовка пользователей посредством уведомления об изменениях, программ повышения осведомленности и обучения.

Обратите внимание, что если вы уже осуществляете централизованное администрирование, такие действия могут оказаться менее трудными, чем кажется. Многие из тех, кто обычно использует списки поиска, знают, что они также могут вводить в случае необходимости полные имена (например, когда они получают доступ к серверу, находясь за пределами частной сети организации), и такие пользователи в меньшей степени нуждаются в обучении по сравнению с теми, кто умеет применять только краткие неполные имена.

5.1. Мониторинг запросов, поступающих серверам имен

Чтобы смягчить проблемы, причиной которых являются списки поиска, вам нужно знать все компьютеры, сетевое оборудование и любые другие системы, использующие для каких-либо запросов списки поиска. Потребуется обновить конфигурацию всех устройств, автоматически использовавших списки поиска.

Существует три широко распространенных способа выполнения такого мониторинга и подготовки списка систем:

- У рекурсивного сервера имен (например, у Active Directory), возможно, есть функция ведения журналов, и ее можно включить для получения сведений обо всех запросах, в которых указаны краткие неполные имена.

- Многие современные брандмауэры также можно настроить на обнаружение и регистрацию в журналах запросов на разрешение всех имен. Это может оказаться не столь эффективной мерой, как ведение журналов в самой системе присвоения имен, в зависимости от топологии вашей сети. Например, если запрос не проходит через брандмауэр, то брандмауэр его не увидит, и поэтому данный запрос будет пропущен.

- Если нельзя использовать ни один из описанных выше способов, мониторинг сервера имен можно осуществлять при помощи программы для захвата пакетов, такой как Wireshark. Однако этот способ требует программной обработки захваченных данных для поиска только тех запросов, которые относятся к кратким неполным именам.

Обратите внимание, что выполнение этого этапа может привести к сбивающим с толку результатам. На таких устройствах, как компьютеры и телефоны, могут быть установлены приложения, предусматривающие ввод имен пользователем; эти устройства будут обнаружены в ходе анализа, даже несмотря на то, что в них отсутствуют какие-либо сохраненные варианты кратких неполных имен. Чтобы выполнить этот этап, необходимо знать только все места вашей сети, где краткие неполные имена хранятся и используются приложениями.

5.2. Составление перечня всех систем, использующих краткие неполные имена в автоматическом режиме

Вам потребуется сводная информация из журналов, полученных на предыдущем этапе. Этой сводной информацией должен стать перечень всех устройств и всех указываемых в запросах кратких неполных имен, а не полный перечень всех случаев отправки запросов устройствами. Необходимость списка всех имен, содержащихся в запросах, обусловлена тем, что на некоторых устройствах может быть установлено несколько приложений, которые придется правильно настроить. Эта сводка станет перечнем устройств, конфигурацию которых необходимо изменить.

5.3. Обучение пользователей и системных администраторов использованию полных имен (FQDN)

Помимо изменения систем, у которых есть краткие неполные имена в какой-либо конфигурации (либо в конфигурации всей системы, либо в конфигурации отдельного приложения), вам необходимо изменить образ мышления пользователей, чтобы они начали использовать полные имена вместо кратких. Для повышения осведомленности и содействия признанию предлагаемых мер используйте описания непредвиденных или нежелательных последствий, способных повлиять на деятельность вашей организации.

5.4. Перевод всех затрагиваемых систем на использование полных доменных имен

Краткие неполные имена заменяются поочередно в каждой системе полными доменными именами (FQDN). В программном обеспечении системы необходимо обнаружить и заменить полными доменными именами все экземпляры краткого неполного имени.

Мониторинг, который был начат на предыдущем этапе, на данном этапе обретает исключительную важность. Маловероятно, что человек сможет обнаружить во всех системах все приложения, в которые встроены краткие неполные имена. Вместо этого после изменения каждой системы следует обращаться к данным мониторинга, чтобы узнать, не поступают ли по-прежнему из этой системы запросы на разрешение кратких неполных имен.

Во многих системах после их первоначального включения запускаются некоторые приложения для инициализации. В эти приложения могут быть встроены системные имена, в основе которых лежат списки поиска, и обнаружение таких имен сопряжено с трудностями. После замены в системе всех имен на полные доменные имена (FQDN) перезагрузите эту систему и воспользуйтесь программным обеспечением для мониторинга, чтобы отследить операции поиска имен. Если система пытается найти какие-либо краткие неполные имена, вам необходимо определить программу, которая направляет этот запрос, и перенастроить ее на использование полных имен. Для выполнения этой процедуры и полной настройки системы надлежащим образом может потребоваться несколько перезагрузок.

5.5. Отключение списков поиска на общих определителях имен

Этот тот момент, когда переход к использованию в сети полных имен вместо кратких неполных имен становится реальностью для всех систем (ПК, сетевых устройств, принтеров и так далее). Списки поиска могут существовать в любой системе, выполняющей операции разрешения имен или определяющей конфигурацию других систем, например сервера DHCP. Эти системы часто представляют собой автономные серверы имен, однако они также могут быть брандмауэрами или другими сетевыми устройствами. Независимо от типа системы, необходимо отключить списки поиска в каждой из них, чтобы предотвратить попытки ввода пользователями кратких неполных имен в данном пространстве имен.

5.6. Начало мониторинга использования кратких неполных имен на серверах имен

Вам необходимо настроить свой сервер имен так, чтобы начать мониторинг всех запросов на разрешение имен, для выполнения которых необходимы списки поиска. Если вы заблаговременно проинформировали и обучили пользователей, они больше не должны использовать эти имена, поэтому созданный на данном этапе мониторинга журнал, возможно, не будет слишком большим; но если это не так, вероятно, придется повторить некоторые из описанных выше этапов для конкретных систем вашей сети.

5.7. Настройка долгосрочного мониторинга по периметру для отслеживания кратких неполных имен

Во время предыдущих этапов необходимо было обнаружить подавляющее большинство случаев использования старых частных имен, но несколько (возможно ключевых) систем по-прежнему могут использовать краткие неполные имена, только крайне редко. Лучшим способом обнаружения подобных запросов на разрешение имен является добавление в конфигурацию всех расположенных по периметру сети брандмауэров правил, обеспечивающих поиск любой утечки запросов. Этим правилам необходимо назначить высокий приоритет и настроить таким образом, чтобы создавались уведомления о событиях, позволяющие быстро оповестить ИТ-персонал. В качестве альтернативы можно просматривать журналы брандмауэров для поиска событий, но при этом высока вероятность пропуска. Оповещения в случае отправки запросов позволят сотрудникам обнаружить эти события, которые, как следует надеяться, теперь будут происходить редко. Некоторые брандмауэры поддерживают такой тип правил только как дополнительную платную функцию; если ваш брандмауэр относится к их числу, следует оценить целесообразность дополнительных расходов на обнаружение редких запросов.

6. Определение конфликта имен новых рДВУ

Начиная с 18 августа 2014 г. ICANN требует, чтобы новые рДВУ, делегированные в корневую зону, помогали организациям выявлять те случаи, когда они допускают утечку запросов в глобальную DNS в отношении имен, подпадающих под категорию новых ДВУ. Такая поддержка будет оказываться на протяжение 90 дней: скорее всего, в первые дни после появления нового рДВУ в корневой зоне, после чего новые рДВУ будут функционировать, как любые другие ДВУ в корневой зоне. Эта поддержка оказывается в форме услуги «управляемого прерывания», которая описывается в этом разделе.

Безусловно, организация, которой необходимо смягчить конфликты имен между своими частными пространствами имен и глобальной DNS, должна сделать это до того, как соответствующий новый ДВУ войдет в корневую зону: ждать начала указанного 90-дневного периода не следует. (Это особенно касается организаций, которые выбрали в качестве имени двухбуквенный ДВУ, поскольку от этих имен не требуется выполнение управляемого прерывания. Управляемое прерывание предназначено в качестве последнего предупреждения организации, которой нужно быстро снизить риск, до того как ДВУ начнет выдавать «настоящие» ответы на запросы.

В этом разделе описывается механизм реализации управляемого прерывания на полномочном сервере имен и то, как это будет отражаться в ответах на запросы. Кроме того, здесь рекомендуется тем организациям, которые имеют частные пространства имен, определять, связаны ли наблюдаемые эксплуатационные изменения результатом управляемого прерывания, рассказывается, как поступать в отношении этих изменений, если речь идет именно о таком случае.

6.1. Описание управляемых прерываний

Услуга управляемого прерывания, которую согласно требованиям ICANN необходимо применять в отношении новых рДВУ, добавляемых в корневую зону после 18 августа 2014 г., должна обеспечивать прерывание на устройствах, с которых в глобальную DNS происходит утечка запросов в отношении имен в частном пространстве имен. В настоящее время, когда происходит утечка такого запроса DNS в глобальную DNS, корневые серверы имен возвращают ответ с кодом, который означает, что данный домен не существует. (С технической точки зрения, речь идет о установке в поле RCODE заголовка запроса значения 3, что мнемонически определяется как ответ «NXDOMAIN»).

В период действия управляемого обслуживания домена в ответе на запрос вместо ошибки NXDOMAIN указание на ошибку вообще отсутствует, но содержатся данные, которые имеют наиболее высокие шансы быть замеченными системой, направившей запрос. Невозможно придумать ответ, который обязательно будет замечен системой, из-за большого разнообразия типов ПО, используемого для запросов DNS. Вместе с тем, требуемое ICANN управляемое прерывание будет заметно на системах с адекватной регистрацией ошибок и в сетях, где сетевые администраторы имеют возможность следить за трафиком DNS.

Те рДВУ, которые работают в режиме управляемого прерывания, будут предсказуемо отвечать на широкий спектр DNS-запросов. В Разделе 6.2 разъясняется, как следить за поведением систем, которые получают ответы с управляемым прерывание на такие запросы DNS.

- Безусловно, чаще всего направляются запросы DNS в отношении A-записей, то есть адресов IPv4, связанных с доменным именем. Теперь в ответах на такие запросы будет указываться IPv4-адрес 127.0.53.53. Это кольцевой адрес для хоста, пославшего запрос. Таким образом, если приложение использует этот адрес для установления контакта, то пошлет сообщение самому себе. Разумеется, сделать это, скорее всего не получится,

поскольку почти все программы, которые выполняют DNS-поиск, должны использовать этот адрес в ответе для контакта с другим сервером.

- Еще один распространенный запрос DNS — это запрос на записи, содержащие текст, известные как «TXT-записи». В условиях действия услуги управляемого прерывания в ответе с TXT-записью будет обязательно содержаться строка «Вам необходимо срочно обратить внимание на вашу конфигурацию DNS, см. https://icann.org/namecollision» (“Your DNS configuration needs immediate attention see https://icann.org/namecollision”). Система, отображающая такие текстовые записи, позволяет увидеть информацию о конфликте имен.

- В случае с запросами DNS, которые направляются на почтовые серверы (с технической точки зрения, на системы обмена электронной почтой для получения MX-записей), служба управляемого прерывания выдаст ответ: «доменное имя вам-срочно-нужно обратить-внимание-на-вашу-dns.<ДВУ> (domain name your-dns-needs-immediate-attention.<TLD>), где «<ДВУ>» — это ДВУ, указанное в DNS-запросе. Это доменное имя может отражаться в сообщениях об ошибке от почтового клиента или почтового сервера. При обращении по адресу «доменное имя вам-срочно-нужно обратить-внимание-на-вашу-dns.<ДВУ>» придет ответ 127.0.53.53.

- Служба управляемого прерывания, получив запрос на служебные (SRV)-записи, даст ответ «доменное имя вам-срочно-нужно обратить-внимание-на-вашу-DNS.<ДВУ>». Запросы на SRV-записи не так распространены, как запросы на IPv4-адреса, текстовые записи и имена почтовых серверов, но становятся все более популярными для более новых приложений, таких как мгновенный обмен сообщениями и голосовая связь.

Если рДВУ добавлено в корневую зону до 18 августа 2014 г., то для него также можно использовать службу управляемого прерывания для подмножества возможных доменов второго уровня в ДВУ. Ответы в отношении таких имен в режиме управляемого прерывания будут точно такие же, как и описанные выше. Согласно требованиям ICANN некоторые домены второго уровня должны быть блокированы от ДВУ, и такие имена, возможно, смогут стать активными после окончания 90-дневного периода управляемого прерывания для доменов второго уровня.

6.2 Идентификация управляемых прерываний

Важно отметить, что нет никакой гарантии, что приложение, получившее ответ в режиме управляемого прерывания, визуально будет вести себя иначе, чем до этого. Однако вероятность того, что приложение поведет себя иначе, весьма высока, и разница эта, скорее всего, будет выражаться в сбое. Можно надеяться, что такой сбой будет сопровождаться сообщением об ошибке, а пользователь приложения сообщит об этом системному администрацию, отвечающему за такие случаи. Если в сообщении об ошибке содержится IPv4-адрес 127.0.53.53, то это является очень весомым указанием на то, что программа использует имя из частного пространства имен, которое в результате утечки попало в общий Интернет.

Ошибки, связанные с использованием службы управляемого прерывания, возникают, когда программа, которая ранее в ответ на запросы получала ответы NXDOMAIN, начинает получать реальные ответы. Разумеется, такие ошибки появились бы позднее при выдаче новым рДВУ ответов с реальными данными, при том, что услуга управляемого прерывания, скорее всего будет действовать на протяжении 90 дней, требуемых ICANN. В течение этого периода ошибки будут более очевидными, поскольку сообщения об ошибке будут содержать IPv4-адрес 127.0.53.53, текст «Вам необходимо срочно обратить внимание на вашу конфигурацию DNS, см. https://icann.org/namecollision», или доменное имя, содержащее строку «доменное имя вам-срочно-нужно обратить-внимание-на-вашу-dns».

Управляемое прерывание также можно отслеживать в сети организации, если сетевой администратор активно ищет сообщения DNS, которые содержат такие ответы. Такой поиск можно проводить через сетевой тест-порт в соответствующих точках входа или же через брандмауэр. В основе такого рода контроля не лежит визуальное слежение за сообщениями об ошибке в соответствующем компьютере: в данном случае сетевой администратор сможет определить компьютер, входящий в сеть организации, с которого происходит утечка запросов в отношении имен в частном пространстве имен.

Независимо от того, как проявится управляемое прерывание в конкретном случае, главное, чтобы в результате компьютер, получающий ответы в этом режиме, был переконфигурирован таким образом, чтобы он мог посылать запросы DNS только на сервер имен организации, а не глобальной DNS. Стандартного способа, который позволял бы указать такие настройки, не существует, хотя настройки — это нормальная составляющая операционной системы. Если компьютер получает свои сетевые настройки от сервера в сети организации, называемого обычно «сервером DHCP», то тогда нужно изменить настройки этого сервера, чтобы DNS-запросы направлялись на сервер имен организации, а не глобальной DNS.

Любой сигнал о том, что компьютер получает ответы в режиме управляемого прерывания, является признаком того, что другие компьютеры сети этой организации также могут их получать. Системному администратору необходимо сразу же проверить настройки DNS для всех компьютеров в этой сети, даже если эти компьютеры не демонстрируют признаков того, что получают ответы в режиме управляемого прерывания. Помните, что период управляемого прерывания длится только 90 дней, поэтому время на то, чтобы найти компьютеры с неправильными настройками DNS, ограничено.

Конечно, внесение таких изменений является лишь временной мерой для смягчения риска возникновения основной проблемы конфликта имен. В разделе 4 и 5 настоящего документа представлены указания о том, как принять постоянные меры для смягчения риска.

7. Резюме

Конфликты имен способны привести к неожиданным последствиям для организаций, использующих частные пространства имен. В настоящем документе перечислены некоторые из этих потенциальных последствий и описаны передовые практические методы изменения принципов использования в организациях частных пространств имен. В документе также описывается управляемое прерывание как инструмент, позволяющий определить те случаи, в которых последствия конфликтов имен могут проявляться со всей очевидностью.

Для тех пространств имен, где используется частный ДВУ, который становится (или уже стал) ДВУ в глобальной DNS, наилучшим способом смягчения ситуации является переход к использованию пространства имен, корневой узел которого находится в глобальной DNS. Для тех пространств имен, где используется сокращение имен при помощи списков поиска, смягчить ситуацию можно только в том случае, если полностью отказаться от применения списков поиска. В состав этапов принятия этих смягчающих мер также входит долгосрочный мониторинг частной сети, позволяющий убедиться, что все экземпляры имен, способные стать причиной конфликтов, больше не используются. Организации получат средства, позволяющие определить наличие конфликта имен при делегировании в корневую зону некоторых новых ДВУ.

Всеобъемлющий способ устранения проблем, связанных с конфликтами имен, заключается в использовании полных имен (FQDN) везде, где используются доменные имена. В сети, где уже используется глобальная DNS, это означает отказ от применения списков поиска. В сети, где используется частное пространство имен, это означает, что корневой узел данного частного пространства имен должен быть размещен в глобальной DNS и необходимо отказаться от применения списков поиска.

Приложение A. Дополнительная литература

Перечисленные ниже документы были подготовлены различными организациями, входящими в состав ICANN. Кроме того, могут принести пользу документы других организаций. Наиболее важной может оказаться ценная информация, опубликованная поставщиком программного обеспечения вашего сервера имен и/или оборудования на своем веб-сайте технической поддержки.

A.1. Введение в программу внедрения новых рДВУ

На этой странице описана история, ход и последовательность реализации программы добавления сотен новых рДВУ в глобальную DNS.
http://newgtlds.icann.org/en/about/program

A.2. Конфликты имен в DNS

ICANN поручила компании Interisle Consulting Group, LLC подготовить этот исчерпывающий доклад о потенциальных конфликтах имен. В нем представлены общие сведения о конфликтах имен, данные по не существующим сейчас ДВУ, которые в настоящее время указываются в запросах к серверам корневой зоны, а также содержится огромное количество справочной информации о проблемах, к которым могут привести конфликты имен.
http://www.icann.org/en/about/staff/security/ssr/new-gtld-collision-mitigation-05aug13-en.pdf

A.3. План управления конфликтами имен в рамках программы ввода новых рДВУ

Это утвержденный корпорацией ICANN план управления конфликтами имен, возникающими между новыми рДВУ и частными пространствами имен. В нем также содержится много ссылок на комментарии, которые были получены ICANN в ответ на более ранние предложения, относящиеся к конфликтам имен в корневой зоне.
http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-annex-1-07oct13-en.pdf

A.4. Рамочный план действий в случае конфликта имен

Настоящий документ является составной частью Рамочного плана действий в случае конфликта имен. В нем определяются особенности услуги управляемого прерывания для рДВУ, которые делегируются в корневую зону DNS начиная с 18 августа 2014 г.
http://www.icann.org/en/system/files/files/name-collision-framework-30jul14-en.pdf

A.5. Проблемы новых рДВУ: имена без точки и конфликты имен

В разных системах списки поиска могут приводить к очень разным результатам, в зависимости от указанного в запросе краткого неполного имени. Основной темой данной статьи являются списки поиска для доменов без точки (ДВУ с адресными записями у своей вершины), однако описание обработки списков поиска также представляет ценность и во многих других отношениях.
https://labs.ripe.net/Members/gih/dotless-names

A.6. SAC 045: недопустимые запросы доменов верхнего уровня на корневом уровне системы доменных имен

В этом отчете ККБС ICANN описаны типы запросов ДВУ, которые наблюдались на корневых серверах на момент подготовки указанного документа.
http://www.icann.org/en/groups/ssac/documents/sac-045-en.pdf

A.7. SAC 057: Информационное сообщение ККБС в отношении сертификатов внутренних имен

В этом отчете ККБС ICANN описаны последствия использования сертификатов, содержащих частные (внутренние) имена, для безопасности и стабильности. В нем определены практические методы работы ЦС, которыми могут воспользоваться злоумышленники и которые создают существенный риск для конфиденциальности и целостности системы безопасного обмена информацией через Интернет.
http://www.icann.org/en/groups/ssac/documents/sac-057-en.pdf