RU

SAC 032
Предварительный отчет по модификации ответов на запросы DNS

ПРИМЕЧАНИЯ К ПЕРЕВОДАМ

Исходная версия данного документа на английском языке доступна по следующему адресу http://www.icann.org/committees/security/sac032.pdf. Если существуют противоречия в переводе или заметные различия между данным документом и исходным текстом, исходная версия имеет приоритетное значение.

Рекомендации Консультативного комитета по вопросам безопасности и стабильности (SSAC) ICANN
Июнь 2008 г.

Предисловие

Поле «Код ответа» (RCODE) протокола DNS[1] обеспечивает серверу имен возможность передавать сигналы и описывать проблемы, возникающие при попытке ответа на запрос клиента (распознаватель). Полномочный сервер имен возвращает код RCODE, установленный для значения *Name Error*, чтобы указать, что доменное имя из запроса не существует. Стандарты Интернета также используют термины *несуществующий домен* или *ответ NXDomain* для описания этого сообщения об ошибке[2].

Значение Name Error имеет смысл только в ответах от полномочного сервера имен. В некоторых случаях владельцы регистрации доменов поручают работу с их полномочной службой имен внутреннему персоналу; в других случаях работу по управлению DNS выполняют внешние организации. SSAC называет их доверенными агентами служб имен или просто Доверенными агентами. Обычно клиенты DNS не отправляют запрос полномочному серверу напрямую. Вместо этого большинство запросов DNS обрабатываются промежуточными системами, называемыми *итеративными распознавателями*. Частные итеративные распознаватели могут использоваться любой организацией. Также существуют общедоступные итеративные распознаватели, создаваемые поставщиками услуг, которые предоставляют клиентам услуги хостинга службы имен или предлагают механизм разрешения доменных имен своим подписчикам. Хотя владельцы регистрации обычно устанавливают с доверенными агентами деловые отношения и отношения доверия, как правило, такие отношения не устанавливаются со всеми операторами итеративных распознавателей. Поэтому в данном докладе при обсуждении этого класса поставщиков услуг используется термин *третья сторона*.

В этом предварительном отчете описываются способы изменения ответов на запрос DNS доверенными агентами и третьими сторонами. В первом случае доверенный агент получает запрос DNS по имени. Доверенный агент определяет, что имя из запроса не существует в зоне, которую он поддерживает для владельца регистрации, но вместо возвращения ответа на запрос DNS с указанием, что имя *не существует*, доверенный агент возвращает ответ, в котором указывается, что такое имя существует, и сопоставляется IP-адрес и указанное в запросе имя по выбору агента. Во втором случае третья сторона, управляющая итеративным распознавателем, получает ответы NXDomain, генерируемые полномочным сервером имен, и изменяет их содержимое, заменяя ответ «*несуществующее имя*» на ответ, указывающий, что *имя существует,* и вставляя вместо него сопоставление IP-адреса и запрошенного имени, произвольно выбираемое третьей стороной.

[1] См. RFC 1035, Внедрение и спецификация системы доменных имен, http://rfc.net/rfc1035.html и реестр IANA http://www.iana.org/assignments/dns-parameters
[2] RFC 2308, NXDomain, http://rfc.net/rfc2308.html

Это поведение может называться по-разному: перенаправление субдоменов, перенаправление NXDomain, перезапись NXDomain, перехват NXDomain, перехват субдоменов, разрешение ошибок и маркетинг ошибок. Эти названия указывают на то, что данные действия используются в коммерческих целях и являются спорными.

Цель этого отчета – описать воздействие изменений ответов на запросы DNS на владельцев регистрации доменных имен, операторов DNS и пользователей Интернета, а также исследовать возможности использования этих методов злоумышленниками. В этом начальном отчете основное внимание уделяется объяснению эффектов и непредвиденных последствий таких действий для пользователей, владельцев регистрации и тех, кто полагаются на ответы о несуществующих доменах для создания отчетов об ошибках и в административных целях.

Что такое изменение ответа на запрос DNS?

Изменение ответа на запрос DNS – это деятельность, при которой поставщик услуг сервера имен возвращает ответ DNS, в котором указывается, что *имя существует,* вместо указания на несуществующее имя в случае, когда выполняется запрос имени, но это имя не опубликовано в сведениях о зоне владельца регистрации домена. В некоторых случаях доверенный агент владельца регистрации домена использует возможность, возникающую благодаря тому, что имя не существует в домене (например, при ошибке набора – www.example.com вместо www.example.com), чтобы возвратить *синтезированный ответ,* то есть сопоставление запрошенного имени и IP-адреса по собственному выбору агента. Доверенный агент может использовать общее сопоставление или сопоставление по умолчанию IP-адресов и запрашиваемых имен, которые не опубликованы в файле зоны: это называется *синтезом шаблона.*

В других случаях итеративный распознаватель, управляемый третьей стороной, исследует ответы на запросы DNS, которые он пытался разрешить для своих клиентов. При обнаружении ответа на запрос DNS, содержащего код ответа со значением *Name Error (Ошибочное имя)*, настроенный третьей стороной итеративный распознаватель изменяет[3] содержимое этого ответа на запрос DNS перед перенаправлением сообщения клиенту, от которого поступил запрос. Это означает, что итеративный распознаватель заменяет код ответа, указывающий, что имя не существует, на ответ, сообщающий, что имя существует. Затем поставщик услуг настраивает распознаватель на изменение содержимого ответа, вставляя сопоставление IP-адреса и запрошенного имени; особенно важно то, что это сопоставление не опубликовано в файле зоны владельца регистрации домена, а является произвольно выбранным третьей стороной.

[3] Мы называем это поведение *тайным изменением*, так как итеративный распознаватель не предоставляет каких-либо явных сведений в протоколе, указывающих, что содержимое было изменено, клиенту или полномочному имени.

Перенаправление на уровне реестра DNS

SSAC и Совет по архитектуре Интернета ранее публиковали свои комментарии о перенаправлении и синтезе DNS на уровне реестра DNS[4, 5, 6]. SSAC не приводит в этом отчете дальнейших комментариев или рекомендаций. Однако для полноты раскрытия темы мы приводим ниже базовую схему *синтезированного ответа от оператора TLD.*

1) Клиент направляет запрос DNS на преобразование доменного имени *example.tld* в IP-адрес итеративному распознавателю *A*.
2) Итеративный распознаватель A начинает процесс преобразования, перенаправляя запрос корневому серверу имен.
3) Корневой сервер имен возвращает список серверов имен, способных преобразовать имена для *tld*.
4) Итеративный разрешитель *A* отправляет запрос на преобразование имени *example.tld* одному из серверов имен *tld,* указанных корневым сервером имен.
5) Сервер имен зоны *tld* определяет, что имени *example* не соответствует конкретное имя в файле зоны *tld*. Вместо возвращения ответа на запрос DNS с кодом ответа, имеющим значение *Name Error*, сервер имен зоны *tld* формирует и возвращает итеративному распознавателю A ответ на запрос DNS, в котором *example.tld* преобразовывается в выбранный им IP-адрес.
6) Итеративный распознаватель A направляет сообщение с положительным ответом клиенту, от которого поступил запрос (а также может поместить этот ответ в кэш).

[4] SAC 006 Перенаправление в доменах COM и NET (9 июля 2004) http://www.icann.org/committees/security/ssac-report-09jul04.pdf
[5] SAC 015 Почему доменам корневого уровня не следует использовать шаблонные записи ресурсов (10 ноября 2006) http://www.icann.org/committees/security/sac015.htm
[6] SAC 013 Ответ SSAC на письмо ICANN: Tralliance предлагает новую службу реестра, http://www.icann.org/committees/security/sac013.htm

Синтезируемые ответы на запросы DNS от Доверенных агентов

В этом примере описывается, как доверенный агент может синтезировать ответ на запрос DNS для домена, на примере *example.tld*.

1) Клиент направляет запрос DNS на преобразование доменного имени *service.example.tld* в IP-адрес итеративному распознавателю *A*.
2) Итеративный распознаватель A начинает процесс преобразования, перенаправляя запрос корневому серверу имен.
3) Корневой сервер имен возвращает список серверов имен, способных преобразовывать имена для *tld*.
4) Итеративный распознаватель *A* отправляет запрос на преобразование имени *service.example.tld* одному из серверов имен *tld,* указанных корневым сервером имен.
5) Сервер имен зоны *tld* возвращает список серверов имен, способных преобразовывать имена для зоны *example.tld*.
6) Итеративный распознаватель *A* продолжает процесс преобразования имени, отправляя запрос на преобразование имени *service.example.tld* одному из серверов имен зоны *example.tld,* указанных сервером имен зоны *tld*.
7) Сервер имен *example.tld* определяет, что имени *service* не соответствует какое-либо имя в файле зоны *example.tld*. Сервер имен *example.tld* формирует и возвращает итеративному распознавателю A ответ на запрос DNS, в котором имя *service.example.tld* преобразовывается в IP-адрес по умолчанию, определенный в файле зоны.
8) Итеративный распознаватель A направляет сообщение с положительным ответом клиенту, от которого поступил запрос (а также может поместить этот ответ в кэш).

На рис. 1 показан этот вариант изменения ответа на запрос DNS.

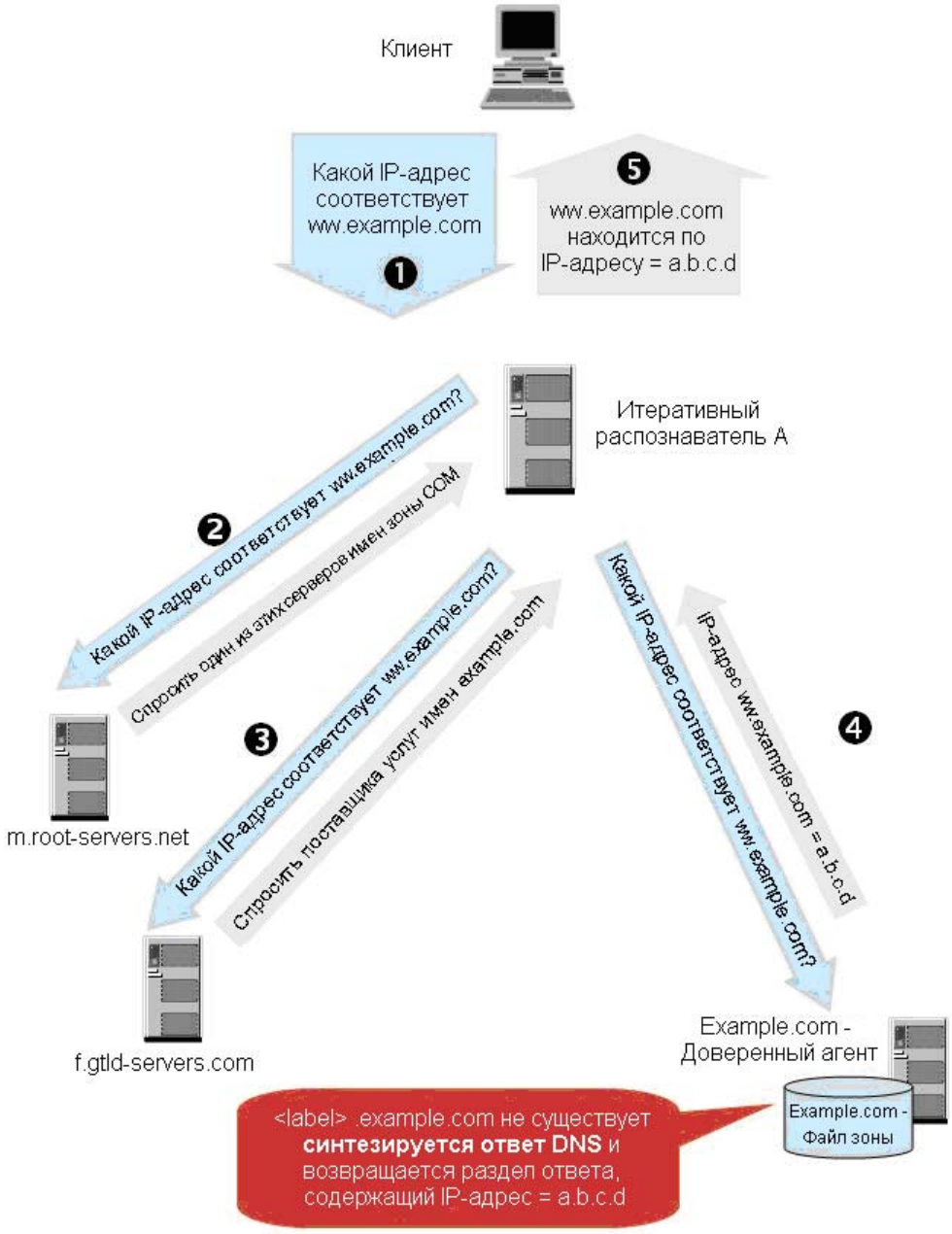

Рис. 1. Ответ NXDomain изменяется доверенным агентом

Изменение ответа NXDomain поставщиками служб имен третьей стороны

Любая третья сторона, управляющая сервером имен с итеративным распознавателем, участвующим в процессе преобразования конкретного имени, может выполнить изменение ответа NXDomain. Например:

1) Клиент направляет запрос DNS на преобразование доменного имени *service.example.tld* в IP-адрес итеративному распознавателю *A*.
2) Итеративный распознаватель A начинает процесс преобразования, перенаправляя запрос корневому серверу имен.
3) Корневой сервер имен возвращает список серверов имен, способных преобразовывать имена для *tld*.
4) Итеративный распознаватель *A* отправляет запрос на преобразование имени *service.example.tld* одному из серверов имен *tld,* указанных корневым сервером имен.
5) Сервер имен зоны *tld* возвращает список серверов имен, способных преобразовывать имена для зоны *example.tld*.
6) Итеративный распознаватель *A* продолжает процесс преобразования имени, отправляя запрос на преобразование имени *service.example.tld* одному из серверов имен зоны *example.tld,* указанных сервером имен зоны *tld*.
7) Сервер имен e*xample.tld* определяет, что имя *service* отсутствует в файле зоны *example.tld* и возвращает итеративному распознавателю A ответ на запрос DNS с кодом ответа, равным *Name Error.*
8) Итеративный распространитель *A* обнаруживает, что сервер имен *example.tld* возвратил сообщение с ответом, указывающим на несуществующее имя. Вместо передачи этого ответного сообщения клиенту итеративный распознаватель *A* заменяет RCODE в сообщении ответа DNS на RCODE, указывающий, что имя найдено (*name found*) и вставляет в запрос ответ, сопоставляющий *service.example.tld* с IP-адресом, произвольно выбираемым третьей стороной, управляющей сервером имен, перед перенаправлением ответа клиенту.

Важно заметить, что на практике любая сторона, участвующая в процессе преобразования, может выполнять перенаправление NXDOMAIN для *любого* имени, которое она определит, как несуществующее, или об отсутствии которого она осведомлена, вне зависимости от того, возвращает ли полномочный сервер NXDOMAIN.

На рис. 2 показан этот вариант изменения ответа на запрос DNS.

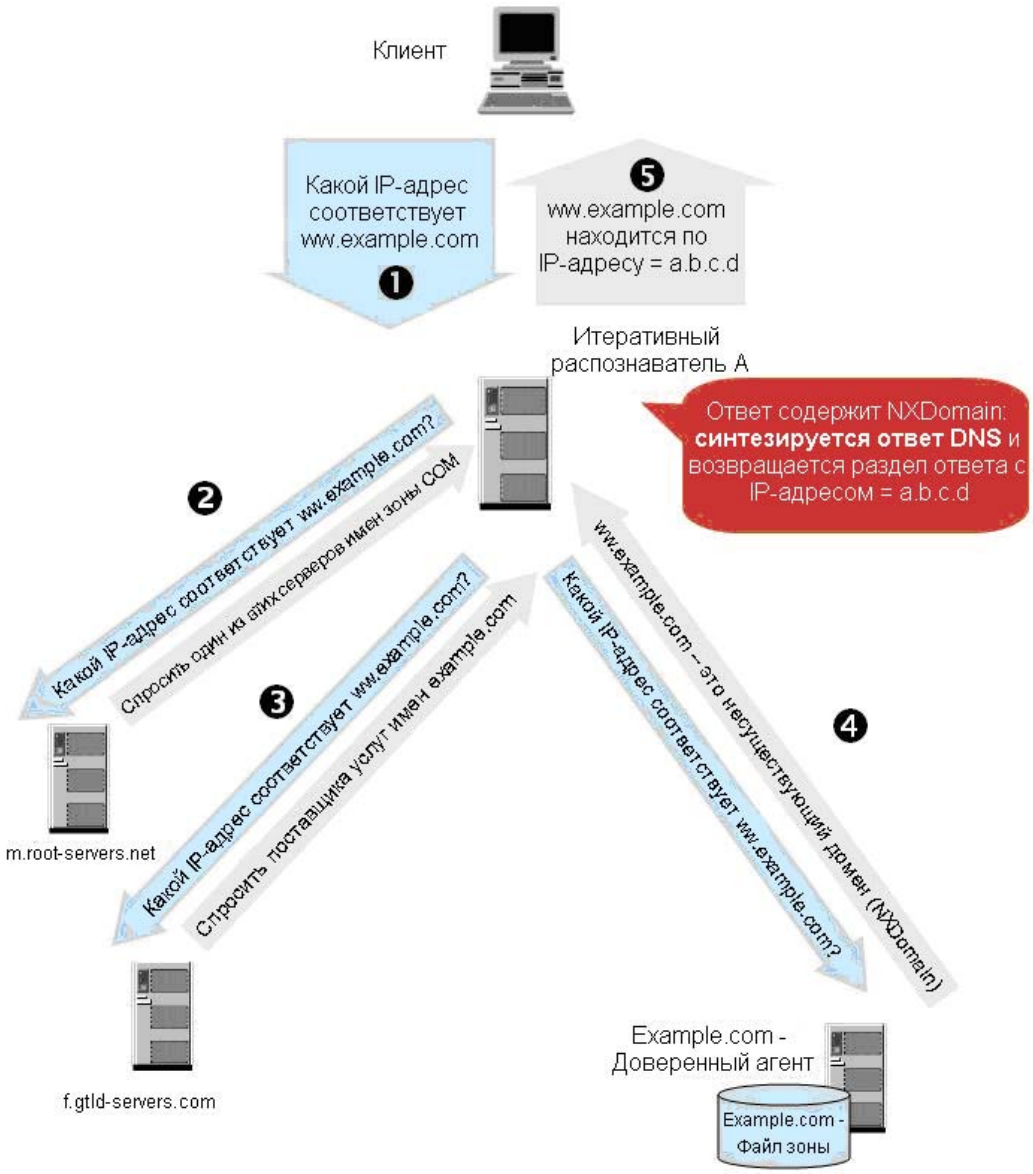

Рис. 2. Ответ NXDomain изменяется доверенным агентом

Кто может изменять сообщения ответов на запросы DNS?

В примерах из предыдущего раздела указаны некоторые из сторон, которые могут перенаправлять сообщения ответа NXDomain. В этот список входят доверенные агенты и третьи стороны.

Доверенные агенты. Сотрудники владельца регистрации имен могут являться доверенной стороной и управлять сведениями о зоне владельца регистрации. Поддерживающий доменное имя регистратор, поставщик услуг Интернета или внешние поставщики услуг DNS (компании, размещающие за плату DNS организации) также могут выступать в качестве доверенной стороны и размещать сведения о зоне владельца регистрации.

Третьи стороны. Любая сторона, управляющая итеративным распознавателем, который участвует в процессе преобразования для заданного запроса DNS, имеет возможность обрабатывать сообщения DNS, направляемые полномочным сервером имен инициатору запроса, в том числе:

- общедоступные поставщики услуг DNS, получающие доход за счет
    - сбора и продажи аналитических сведений о трафике DNS или
    - продажи рекламных площадей на страницах, размещаемых по адресам, которые вставляются в изменяемые ими ответы DNS;
- Поставщики услуг Интернета или их агенты (компании, поддерживающие DNS для поставщиков услуг Интернета за плату), которые обеспечивают преобразование имен для подписчиков, или, в общем, для любой стороны, использующей службы имен поставщика услуг Интернета.
- Поставщики услуг, предлагающие разрешение имен в сочетании с услугами веб-прокси.

Злоумышленники также могут изменять ответы DNS для осуществления злоумышленной или преступной деятельности.

Этот список также показывает, что существует множество мотивов для изменения ответов на запросы DNS. Они будут рассмотрены в следующем разделе.

Зачем изменять ответы NXDomain?

Несколько причин, по которым стороны могут решить изменять ответы на запросы DNS, определены и описаны SSAC. Например, вместо доставки ответа NXDomain, возвращенного полномочным сервером имен, третья сторона может перехватить и тайно изменить содержимое ответа DNS, чтобы он содержал IP-адрес веб-страницы, с помощью которой выполняется следующая деятельность.

- **Получение дохода**. На целевой странице размещается реклама или другое содержимое, обеспечивающее доход для домена и субдоменов зарегистрированных доменов.
- **Способствование работе пользователя в Интернете**. На целевой странице пользователю сообщается (потенциальному клиенту), что запрошенное им доменное имя недоступно, и предоставляется возможность устранить ошибку, например, пользователь может исправить ошибку, воспользовавшись (спонсируемой) формой поиска, доступной на целевой странице.
- **Обеспечение соблюдения политики**. На целевой странице содержится уведомление, что содержимое страниц в домене, к которому он попытался получить доступ, нарушает политику допустимого использования. На целевой странице может быть указан конкретный тип содержимого или приведена копия правил политики допустимого использования для просмотра пользователем.
- **Предоставление обучающих материалов**. На целевой странице сообщается, что домен, к которому пользователь пытался получить доступ, был определен как фишинговый домен, и обслуживание сайта было приостановлено. Пользователь может просмотреть антифишинговые образовательные материалы на целевой странице.
- **Поддержка несанкционированной или преступной деятельности**. На целевой странице по имени, относящемуся к домену, но не созданному регистратором, размещается различное опасное загружаемое содержимое, способствующее преступной деятельности (фишингу, краже личных данных, мошенничеству и т.д.)

Является ли изменение ответов DNS проблемой безопасности и стабильности?

Некоторые характеристики изменения ответов DNS заслуживают внимания. SSAC обнаружил в описанные ниже особенности поведения доверенных агентов и третьих сторон, участвующих в изменении ответов DNS.

1) Предполагается, что доверенные агенты действуют по поручению владельца регистрации домена. С точки зрения деятельности вносимые доверенным агентом изменения допустимы в модели данных DNS. Вопрос разрешения создания синтезированных ответов доверенным агентом должен решаться агентом и владельцем регистрации. Владелец регистрации может воспользоваться услугами другого агента для размещения зоны, если доверенный агент окажется недостойным доверия.
2) По самой природе DNS любая третья сторона, предоставляющая итеративный распознаватель, участвующий в процессе разрешения, является посредником и имеет потенциальную возможность изменять получаемые от полномочного сервера имен сообщения перед их перенаправлением клиенту. Изменение ответов NXDomain третьими сторонами в процессе разрешения может находиться вне области коммерческих взаимоотношений, в которых участвует владелец регистрации.
3) Третьи стороны, изменяющие семантику и содержимое ответов DNS, могут делать это в собственных интересах, без уведомления и получения согласия владельца регистрации домена или пользователя, от которого получен запрос.
4) Третьи стороны, изменяющие ответные сообщения NXDomain, предоставляют сведения о домене, отличающиеся от сведений, которые намерен распространять владелец регистрации домена, в нескольких значительных аспектах. Ответ предполагает, что имя (субдомен) было создано в домене и сопоставляется с конкретным IP-адресом. С точки зрения владельца регистрации домена это имя в его зоне отсутствует. Такой ответ является неправильным и неверно представляет намерения владельца регистрации.
5) Третьи стороны влияют на последующие действия пользователя, который формулировал запрос, исходя из своих предположений о связи домена с владельцем регистрации доменного имени. Если третья сторона намерена получать выгоду от подразумеваемых отношений между третьей стороной и владельцем домена, то, вероятно, это является мошенничеством, введением в заблуждение или несанкционированным использованием бренда либо торговой марки.
6) Изменения ответов DNS могут повлиять на другие приложения, помимо веб-приложений, и, в частности, могут нарушать работу электронной почты, интернет-телефонии и других служб в Интернете.
7) Изменения ответов на запросы DNS могут приводить к непредсказуемым результатам (обычно это затрагивает вопросы стабильности, но также возможна атака типа «отказ в обслуживании»).

Далее рассматривается влияние этих проблем безопасности и стабильности на владельцев регистрации доменов.

Как изменение ответов на запросы DNS влияет на владельцев регистрации доменных имен?

Когда ответы NXDomain изменяются без явного согласия и осведомленности владельца регистрации доменных имен, ответное сообщение не передает точно рабочее состояние домена, предполагаемое владельцем регистрации.

1) Клиент, отправляющий запрос, должен получить сообщение об отсутствии имени в файле зоны. Доверенный агент или третья сторона, тайно изменяющие передаваемое клиенту сообщение, должны возвратить код ответа *Name Error*, но они не делают этого.

2) Ресурсная запись типа A помещается в раздел ответа возвращаемого сообщения. Сопоставление имени и адреса, описываемое в этой записи, не существует в опубликованном файле зоны владельца регистрации домена.

При более внимательном рассмотрении это является не только альтернативным вариантом обработки ошибочного состояния, но изменением содержимого. Если доверенный агент владельца регистрации домена создает сообщение ответа на запрос DNS, каким бы ни был ответ, агент и владелец регистрации имеют все причины ожидать от посредников, что те попытаются доставить содержимое без его изменений. Если это предположение окажется неверным, то интересы владельца регистрации домена могут быть затронуты в любом из следующих аспектов.

Ответ не содержит информацию, которую он должен был содержать. Работа приложений и выполнение деятельности по управлению, которые зависят от ответов NXDomain, обеспечивающих их работу или являющихся сигналом для вмешательства, нарушаются для всех имен в домене, которые перенаправляются.

Ответ разрушает обычную модель доверия доменов. Обычно организации принимают решения по вопросам безопасности, исходя из подразумеваемой модели доверия: родительский домен доверяет субдоменам, расположенным в этом домене. Это подразумеваемое доверие основано на предположении, что администрирование хостов, имена которых относятся к домену организации, выполняется специалистами по обслуживанию домена или назначенными и доверенными агентами. Измененный ответ NXDomain направляет пользователей к службам, работающим на хостах вне административного контроля и вне домена безопасности владельца регистрации домена.

Ответы усложняют проведение проверок на соответствие и аудита. Организации, которые выполняют проверку безопасности, особенно если они выполняют проверку для подтверждения соответствия правовым нормам, должны принимать во внимание, что третьи стороны могут произвольно добавлять узлы, которые будут казаться располагающимися в домене, но эти узлы не будут находиться под административным контролем владельца зоны, а их имена не будут опубликованы в зоне.

Ответ может вызывать нестабильность функционирования DNS. При разрешении имен, выполняемом напрямую с помощью полномочного сервера имен домена или через итеративный распознаватель, не изменяющий ответы NXDomain, будут возвращаться ответы, соответствующие намерениям владельца регистрации, но тот же запрос может возвращать другой ответ в случае, если он обрабатывается третьей стороной, изменяющей ответы NXDomain, или проходит через итеративный распознаватель или распознаватель-заглушку, в кэше которого содержится измененный ответ. Та же ситуация может возникнуть и в случае, если владелец регистрации домена пользуется услугами двух доверенных агентов для размещения файла зоны. Один доверенный агент может опубликовать файл зоны владельца регистрации с записью-шаблоном, а другой может опубликовать настоящий (не измененный) файл зоны.

Важна возможность существования конфликтующих сопоставлений адресов. Владелец регистрации домена может добавить ресурсную запись типа A для имени (ww.example.com) в собственный файл зоны, обнаружив после этого, что третья сторона (или, возможно, несколько сторон) уже сопоставили IP-адрес с этим именем. [Примечание: в большинстве случаев это истинно для любого вида запрашиваемой клиентом записи.]

Хосты домена подвергаются любым рискам, которыми можно воспользоваться с хоста перенаправления или при использовании этого хоста. Даже в ситуациях, когда упоминаемый в измененном ответе NXDomain хост управляется законопослушной компанией (например, он используется для рекламы или продвижения услуг), этот хост может быть подвержен атакам на веб-сервер и веб-приложения, перекрестным атакам на сценарии сайтов (XSS) или атакам с использованием слабых мест операционной системы; в частности, злоумышленники могут внедрить содержимое в одну из систем владельца регистрации домена через хост, упоминаемый в измененном ответе NXDomain. Эти атаки существуют не только в теории. Исследователи вопросов безопасности открыто продемонстрировали возможность внедрения сценариев в сайты родительского домена через хосты, упоминаемые в измененных ответах NXDomain (серверы внедрения рекламы)[7, 8].

[7] h0h0h0h0, автор – Дэн Камински (Dan Kaminsky), http://www.doxpara.com/DMK_Neut_toor.ppt
[8] Взлом страниц сообщений об ошибках ISP, Брюс Шнайер (Bruce Schneier), http://www.schneier.com/blog/archives/2008/04/hacking_isp_err.html

Ответ добавляет в домен хосты, а администратор владельца регистрации домена не может управлять содержимым этих сайтов. Хосты, упоминаемые в измененных третьими сторонами ответах NXDomain, получают преимущества за счет использования принадлежащих владельцу регистрации домена брендов, репутации, популярности сайта и ссылок, а также соглашений о спонсировании ссылок с поисковыми системами. Владелец регистрации не получает никакой выгоды от такой деятельности, а в определенных ситуациях она может причинить ему вред или ущерб. Ниже приведены примеры такого вреда.

- Третья сторона может публиковать рекламу на хосте, на который ссылается измененный ответ NXDomain. Реклама может содействовать продаже услуг или товаров, предлагаемых конкурентами владельца регистрации доменного имени.
- Компания, реклама которых публикуется на хосте, на который ссылается измененный третьей стороной ответ NXDomain, получает преимущества от спонсируемых ссылок, связанных с доменным именем и ключевыми словами, которые ассоциируются поисковыми системами с компанией владельца регистрации.
- У владельца регистрации может осуществлять собственную рекламную деятельность, и реклама, публикуемая на хосте, который упоминается в измененном третьей стороной ответе NXDomain, может подрывать эффективность рекламы, которую владелец регистрации домена публикует на собственных веб-хостах, или конкурировать с ней. Это затрагивает владельца регистрации домена, чье сотрудничество с поставщиком услуг рекламы подвергается опасности, и рекламируемых партнеров, чьи возможности получения прибыли перехватываются.
- Хост, упоминаемый третьей стороной в измененном ответе NXDomain, может публиковать материалы недоброжелательных рекламных кампаний или публиковать неточные либо вводящие в заблуждение сведения, ориентированные на причинение вреда репутации владельца регистрации.

Изменение ответов NXDomain не ограничивается ресурсными записями типа A. Третья сторона не ограничивается заменой ответов NXDomain, которые предположительно должны были разрешать имена хостов, используемых при соединениях по протоколу HTTP, поскольку ответ NXDomain может относиться к запросу любой ресурсной записи, выполняемому любым приложением – распознаватель DNS определяет в запросе лишь имя и тип записи. Третьи стороны теоретически могут изменять ответы NXDomain на любой запрос (MX, SRV, NAPTR); например, запросы DNS, используемые для поиска номеров IP-телефонии (например, запросы, возвращающие ресурсную запись NAPTR), могут перенаправляться на сервер обработки вызовов по выбору третьей стороны.

Ответ создает возможность злоупотребления и осуществления атак. Следующие атаки могут проводиться с помощью поддельных ответов.

- **Фишинг с помощью внедрения фальшивых сайтов через поддельные субдомены**. Злоумышленники могут воспользоваться сценариями, находящимися на хосте, который упоминается в измененном ответе NXDomain, и атаковать системы владельца регистрации домена через эти сценарии. Например, злоумышленник может найти сценарий, который принимает входные данные, но не выполняет проверку их соответствия определенным параметрам этого сценария. Внедрив собственный исполняемый код в этот уязвимый параметр, злоумышленник может обмануть посетителей сайта, заставив их заполнить поддельную версию формы входа или оплаты на этом сайте[9]. Злоумышленники могут использовать схожие методы для публикации баннеров, в которых пользователям предлагается загрузить опасное программное обеспечение, или для создания всплывающих окон, в которых пользователю предлагается выполнить обновление приложений или операционной системы, но эти обновления содержат опасный код и являются поддельными.
- **Извлечение данных**. Хост перенаправления может отслеживать трафик и собирать веб-статистику по перенаправляемым пользователям, во многом подобно деятельности компаний по отслеживанию воздействия рекламы.
- **Получение произвольных cookie-файлов**. Хост перенаправления может перехватывать и копировать cookie-файлы, отправляемые клиенту веб-сервером владельца регистрации домена. Это может привести к раскрытию личных сведений, сведений о кредитных картах или данных для входа в учетную запись.
- **Атаки, направленные против брендов**. Многие владельцы регистрации доменных имен защищают бренды и торговые марки, предупредительно регистрируя находящиеся в TLD имена, которые являются оскорбительными, клеветническими, обманчиво схожими с оригинальными или имеют схожее написание. Те же имена могут быть реализованы в виде субдоменов злоумышленником, использующим внедрение шаблона. При этом все запросы таких имен вместо возврата сообщения о несуществующем домене могут перенаправляться на искаженный исходный веб-сайт.

Кроме этих вопросов функционирования и безопасности, SSAC также отмечает, что перенаправление субдоменов может поднимать вопросы, связанные с интеллектуальной собственностью и защитой торговых марок. Эти вопросы, находящиеся вне области компетенции SSAC, возможно, заслуживают рассмотрения компетентными сторонами при дальнейшем изучении проблемы.

[9] *Структура атаки XSS: использование, влияние и противодействие, Русс МакРи (*Russ McRee), ISSA Journal, июнь 2008, стр. 12–14.

Перехват перезаписи

Измененный ответ DNS и сам может быть изменен. Краткое описание данного явления, называемого *перехватом перезаписи*, приводится ниже:

1) Пользователь, Фред, регистрирует домен *example.tld* через регистратора *X*.
2) Владелец регистрации *example.tld* использует службы DNS, предлагаемые регистратором *X,* для размещения файла зоны *example.tld*.
3) На компьютере Фреда по умолчанию используется сервер имен *NS1.mylocalisp.tld*.
4) Фред открывает окно браузера на компьютере ПК1 и пытается перейти на *ww.example.tld*. Он допустил ошибку при наборе имени *www.example.tld,* имени хоста, используемого владельцем регистрации как адреса для подключения к веб-серверу по протоколу HTTP.
5) Сервер имен *NS1.mylocalisp.tld* выполняет процесс разрешения для преобразования имени *ww.example.tld*. Сначала корневому серверу имен направляется запрос имени *tld,* затем серверу имен *tld* направляется запрос имени *example.tld* и, наконец, выполняется запрос к серверу имен регистратора X относительно имени *ww.example.tld*
6) Сервер имен регистратора X возвращает положительный ответ на запрос DNS вместо ответа NXDomain для имени *ww.example.tld.* Этот ответ содержит в разделе ответа запись A, которая сопоставляет *ww.example.tld* с *a.b.c.d.*
7) Сервер имен *NS1.mylocalisp.tld* перехватывает ответ DNS регистратора *X* и сопоставляет адрес перенаправления *a.b.c.d* с рекламной страницей, используя данные выполненного ранее анализа трафика DNS.
8) Сервер имен *NS1.mylocalisp.tld* заменяет информацию перенаправления и возвращает положительный ответ DNS, содержащий в разделе ответа запись A, которая сопоставляет *ww.example.tld* с *a.x.y.z.*
9) Открыв окно браузера на ПК1, Фред пытается подключиться к сайту *ww.example.tld* по адресу *a.x.y.z.*

Предварительные результаты исследования

SSAC предлагает следующие предварительные сведения и наблюдения относительно изменения ответов на запросы DNS.

1) Ответы NXDomain могут изменяться поставщиками услуг третьих сторон на любом из итеративных распознавателей между клиентом и полномочным сервером имен. Доверенные агенты могут включать в файл зоны владельца регистрации записи шаблонов и возвращать такое сопоставление адресов вместо сообщения *Name Error*.

2) Изменение ответов NXDomain третьими сторонами создает проблемы функционирования и безопасности для владельцев регистрации доменов, которые нельзя легко устранить даже при использовании собственной службы имен.

3) Изменение ответа NXDomain и синтезированные ответы могут представлять собой проблемы безопасности для владельцев регистрации доменов. В частности, нельзя полагаться на отношения доверия между родительским доменом и его субдоменами. Разрушение отношений доверия может негативно влиять на аудит безопасности и проверки на соответствие.

4) Изменение записей NXDomain и синтезированные ответы могут создавать возможность атак против владельца регистрации домена, а также давать злоумышленникам возможность использовать активы, связанные с доменом владельца регистрации, в злонамеренных или преступных целях.

5) Измененяемые ответы NXDomain и синтезированные ответы могут изменяться третьими сторонами, которые модифицируют получаемые ими ответы NXDomain.

6) Доверенные агенты, которые синтезируют ответы, и третьи стороны, изменяющие ответы NXDomain существуют в действительности и могут быть идентифицированы. Некоторые третьи стороны изменяют ответы NXDomain непосредственно или через *партнеров по разрешению ошибок*[10].

7) Доверенные агенты и третьи стороны могут скрывать, что они изменяют ответы DNS, отказываясь открыто признать этот факт, а в случаях, когда они признают подобные действия, они могут скрывать их возможное неблагоприятное воздействие на интересы владельца регистрации домена. Некоторые поставщики услуг сообщают, что они пользуются правом выполнять разрешение или перенаправление ошибок согласно соглашению о предоставлении услуг, и не дают владельцу регистрации иного способа отказаться от этой практики, кроме выбора другого поставщика услуг.

[10] Некоторые участники этой деятельности оценивают всемирный ежегодный рынок ошибок в более чем 1 млрд. долл. США http://barefruit.com/services.htm

8) Ответы NXDomain не просто передают сведения об ошибке от владельца регистрации домена, но передают информацию, относящуюся к записям файла зоны. К этому содержимому следует относиться так же, как и к содержимому любых других приложений.
9) Изменение ответов влияет не только на веб-приложения. Замена и внедрение содержимого могут широко использоваться и в других областях, особенно в сфере электронной почты и IP-телефонии.
10) Изменение ответов на запросы DNS может поднимать вопросы, связанные с интеллектуальной собственностью и торговыми марками.

Предварительные рекомендации

SSAC предоставляет следующие предварительные рекомендации.

1) SSAC ранее многократно рекомендовал не синтезировать ответы DNS на уровне TLD. Подобные действия не рекомендуется выполнять и на уровне субдоменов.

2) Владельцы регистрации могут управлять тем, каким образом доверенные агенты отвечают на запросы имен, отсутствующих в файле зоны, за счет доверия и укрепления деловых отношений. Владелец регистрации должен определять, будут ли его полномочные сервера имен возвращать Name Error или синтезированные ответы.

3) Владельцам регистрации следует запрашивать своих доверенных агентов о способе работы с их незарегистрированными субдоменами. SSAC сходится во мнении с IAB, рекомендуя доверенным агентам не использовать шаблоны DNS в зонах без уведомления владельцев регистрации доменов о рисках, описанных в этом Отчете и в других источниках. Доверенным агентам не следует создавать шаблоны и синтезированные ответы без основанного на осведомленности владельцев регистрации согласия. Доверенным агентам следует реализовать механизм отказа, позволяющий клиентам получать исходные ответы DNS на свои запросы.

4) Третьим сторонам следует сообщать о том, что они вносят изменения в ответы NXDomain, и предоставлять возможность отказа от этой практики для своих клиентов.

5) Организациям, которые полагаются на точную передачу NXDomain для обеспечения стабильности функционирования, следует выбирать доверенных агентов, которые гарантируют передачу неизменных ответов DNS в договорах об оказании услуг.

6) Владельцам регистрации следует исследовать возможности предоставления конечным пользователям подтвержденных доказательств отсутствия субдоменов, например расширения безопасности DNSSEC[11,12,13,14]. Организациям следует стремиться к уменьшению степени подверженности изменению ответов NXDomain, выбирая доверенные стороны, которые предоставляют итеративные распознаватели, чтобы запросы клиентов организаций не направлялись через произвольных поставщиков разрешения имен, которые могут применять перенаправление субдоменов

[11] RFC 4033 Краткое описание и требования к безопасности DNS, http://rfc.net/rfc4033.html
[12] RFC 4034 Ресурсные записи для расширений безопасности DNS, http://rfc.net/rfc4034.html
[13] RFC 4035 Изменения протокола для расширений безопасности DNS, http://rfc.net/rfc4035.html
[14] RFC 5155 Хэшируемое подтверждаемое отрицание существования в безопасном DNS (DNSSEC), http://rfc.net/rfc5155.html

Последующие действия

Влияние перенаправления субдоменов на коммерческую и экономическую деятельность, безопасность и обеспечение функционирования заслуживает дополнительного внимания. Согласно нашим сведениям изменение ответов DNS большей частью ограничивается веб-приложениями, а вопрос воздействия подобного изменения на другие IP-службы требует дальнейшего изучения. SSAC поддерживает более детальное рассмотрение сообществом последствий обращения отрицательных ответов в возможности получения прибыли без учета влияния данных действий на функционирование систем и без учета пожеланий владельцев регистрации и клиентов данных DNS. По существу, разрешение ошибок и «рынки ошибок», создаваемые такими действиями, вызывают беспокойство и приводят к неоднозначности и изменчивости традиционных моделей управления ошибками и доверия. Не ясно, могут ли такие действия применяться к службам электронной почты, IP-телефонии и совместной работы или даже к адресации, маршрутизации и другим ключевым аспектам функционирования Интернета. Также не ясно, насколько сильное воздействие они могут оказывать на IP-коммуникацию.