Чего ожидать во время обновления ключа KSK корневой зоны?

Офис технического директора ICANN

22 августа 2018 года

Основные положения

Ожидается, что после начала процедуры смены ключа KSK корневой зоны (в настоящее время запланированной на 11 октября 2018 года) очень небольшой процент интернет-пользователей столкнется с проблемами при разрешении некоторых доменных имен. В данный момент небольшое количество валидирующих рекурсивных резолверов расширений безопасности системы доменных имен (DNSSEC) настроено неправильно, и у части пользователей, обслуживаемых этими резолверами, возникнут проблемы. В настоящем документе описано, какие пользователи столкнутся с проблемами и какого рода проблемы будут периодически возникать.

- Обновление ключа не затронет пользователей, чьи резолверы не выполняют валидацию DNSSEC.
- Смена ключа не затронет пользователей, обслуживаемых резолверами, настроенными на новый KSK.
- Если у всех резолверов пользователя в конфигурации якорей доверия отсутствует новый KSK, вполне возможно, что этот пользователь в течение 48 часов после смены ключа в какой-то момент столкнется с негативными последствиями.
- Нет возможности предсказать, когда операторы резолверов, на которых отразится обновление заметят, что у них прекратилась валидация.
- Результаты анализа позволяют заключить, что более 99% пользователей, обслуживаемых резолверами, выполняющими валидацию, от смены ключа KSK не пострадают.

1. Введение

Корпорация ICANN уже много лет обращает внимание общественности на предстоящее обновление ключа KSK корневой зоны DNS.[1] Во время последнего общественного обсуждения уточненной процедуры обновления ключа[2] многие члены сообщества попросили предоставить дополнительную информацию о процедуре смены ключа. Корпорация ICANN обещала опубликовать дополнительные материалы, чтобы помочь в подготовке к обновлению ключа.[3] Настоящий документ подготовлен в рамках данного обещания.

В ряде сообществ отсутствовало ясное понимание того, что произойдет (и чего не произойдет) при смене ключа. В настоящем документе представлены подробные сведения об ожидаемом развитии ситуации с момента обновления ключа.

[1] http://www.icann.org/kskroll
[2] https://www.icann.org/public-comments/ksk-rollover-restart-2018-02-01-en
[3] https://www.icann.org/en/system/files/files/report-comments-ksk-rollover-restart-23apr18-en.pdf

У данного документа широкая целевая аудитория. В первую очередь он предназначен для трех групп. Это:

- Операторы валидирующих резолверов, которые хотят понимать, на что им следует обратить внимание после обновления ключа.
- Журналисты без технической специализации, а также другие лица, которые планируют освещать в СМИ процедуру обновления ключа до, во время и после самого события.
- Исследователи, которые будут наблюдать за DNS для выявления сбоев в работе резолверов после осуществления процедуры смены ключа.

Следует отметить, что данный документ вероятно не представляет большого интереса для тех, кто использует хотя бы один резолвер, готовый к смене ключа. После смены ключа эти пользователи не заметят никаких изменений в использовании DNS и интернета в целом. То же справедливо и для пользователей, обслуживаемых резолверами, не выполняющими валидацию DNSSEC. Согласно текущим оценкам приблизительно две трети пользователей обслуживается резолверами, в которых еще не включена валидация DNSSEC.

В настоящее время смену ключа планируется осуществить 11 октября 2018 года. Дата произведения процедуры обновления ключа еще подлежит ратификации Правлением ICANN, что должно произойти до наступления самой даты. Первоначально ключ планировалось сменить 11 октября *2017* года, но эта дата была перенесена в связи с получением неоднозначных данных накануне указанного срока.[4]

В разделах 2 и 3 настоящего документа описано, что произойдет с готовыми и не готовыми к смене ключа валидирующими резолверами после осуществления процедуры обновления. В разделе 4 указано, какие явления могут заметить исследователи, наблюдающие за трафиком в системе корневых серверов DNS. Для описания того, что произойдет после обновления ключа, в настоящем документе используются недетерминированные формулировки. Это делается в связи с тем, что никто, кроме оператора резолвера, не может сообщить, какое именно программное обеспечение установлено на резолвере, и с невозможностью определить, правильно ли настроен резолвер для целей обновления ключа.

Важное примечание для операторов резолверов: Все операторы валидирующих резолверов, читающие этот документ, должны незамедлительно убедиться, что они готовы к обновлению ключа, проверив состояние своих текущих якорей доверия.[5] Если операторы не готовы к смене ключа, им следует как можно скорее указать в настройках конфигурации резолверов новейшие якоря доверия.[6] Операторы резолверов, не выполняющих валидацию DNSSEC, уже готовы к обновлению ключа.

[4] https://www.icann.org/news/announcement-2017-09-27-en
[5] https://www.icann.org/dns-resolvers-checking-current-trust-anchors
[6] https://www.icann.org/dns-resolvers-updating-latest-trust-anchor

1.1 Определение понятия «обновление ключа KSK корневой зоны»

Корневая зона DNS была подписана при помощи DNSSEC в 2010 году. В корневой зоне DNS есть два вида ключей. Это ключи подписания зоны (ZSK), которые применяются для подписания основных данных в корневой зоне, и ключи для подписания ключей (KSK), которые применяются только для подписания комплекта ключей корневой зоны (как ZSK, так и KSK). Новый ZSK публикуется раз в три месяца и подписывается KSK, имеющим более длительный срок действия.

Обновление ключа происходит при изменении KSK корневой зоны, когда для подписания комплекта ключей корневой зоны начинает использоваться новый KSK. В момент смены ключа первый KSK выводится из эксплуатации и начинает использоваться новый KSK. Первый KSK называется KSK-2010 (продолжает использоваться сегодня). Новый KSK называется KSK-2017. После осуществления процедуры смены ключа использование KSK-2010 для подписания комплекта ключей корневой зоны будет прекращено: вместо этого комплект ключей корневой зоны будет подписываться с помощью KSK-2017.

1.2 Якоря доверия

Чтобы понять, как произойдет обновление ключа, важно также понять принципы использования якорей доверия KSK корневой зоны валидирующими резолверами. В конфигурации каждого валидирующего резолвера определена совокупность *якорей доверия*, которые являются копиями ключей или идентификаторов ключей, соответствующими KSK корневой зоны. Как правило, якоря доверия автоматически настраиваются поставщиками программного обеспечения, резолверами, в которых настроено автоматическое обновление якорей доверия при помощи процесса, описанного в RFC 5011,[7] или оператором резолвера, который добавляет новый KSK в хранилище якорей доверия резолвера вручную.

До появления KSK-2017 в конфигурации всех валидирующих резолверов в качестве якоря доверия был указан только KSK-2010. После создания и публикации KSK-2017 большинство операторов резолверов либо вручную настроили якоря доверия своих резолвера на KSK-2017, либо это изменение было сделано программным обеспечением резолвера (например, при автоматическом обновлении, описанном в RFC 5011), либо соответствующим поставщиком программного обеспечения. Надо отметить, что некоторые операторы резолверов не изменили конфигурацию своих устройств и в данный момент не готовы к смене ключа, поскольку продолжают использовать в качестве якоря доверия только KSK-2010. Когда произойдет обновление ключа, у этих операторов резолверов будут отсутствовать валидные якоря доверия.

2. Резолверы, готовые к обновлению ключа

В конфигурации резолверов, готовых к обновлению ключа, KSK-2017 уже указан в качестве якоря доверия. После смены ключа эти резолверы будут работать, как и раньше, поскольку новый KSK корневой зоны уже включен в состав ключей, которые разрешено использовать для подписания комплекта ключей корневой зоны. Программное

[7] https://datatracker.ietf.org/doc/rfc5011/

обеспечение некоторых резолверов фиксирует в журнале событий факт обновления ключа, однако маловероятно, что эти записи в журнале (если они вообще существуют) будут замечены, если оператор не приложит конкретных усилий, чтобы их найти.

Когда произойдет обновление ключа, пользователи готовых к обновлению резолверов никаких изменений не заметят. Ответы, которые они будут получать на стандартные запросы после обновления ключа, ничем не будут отличаться от ответов, получаемых до его обновления. Согласно результатам недавно проведенного APNIC исследования,[8] более 99% пользователей резолверов, настроенных на валидацию DNSSEC, обслуживаются резолверами, готовыми к обновлению ключа.

Большинству интернет-пользователей доступно несколько правильно настроенных резолверов DNS. Если хоть один из доступных пользователю резолверов готов к обновлению ключа, программное обеспечение этого пользователя должно найти его после смены ключа и перейти на его использование. Это может замедлить процесс разрешения DNS, поскольку система пользователя будет пытаться использовать резолвер, не готовый к смене ключа перед тем, как переключиться на резолвер, готовый к смене ключа, но разрешение DNS в результате все-таки произойдет.

3. Резолверы, не готовые к обновлению ключа

Если в конфигурации резолвера в качестве якоря доверия указан только KSK-2010, то после обновления ключа этот резолвер не сможет подтверждать достоверность ответов, получаемых им от авторитативных серверов. При этом невозможно предсказать, в какой именно момент возникнет этот сбой.

Хотя публикация в DNS — событие мгновенное, резолвер может увидеть опубликованную новую запись с отставанием по времени. У каждой записи в DNS есть «время существования» (известное под названием *TTL*), в течение которого резолвер не делает попыток получить более новую версию записи. После обновления ключа в кэше резолвера вероятнее всего будет сохраняться версия подписи с использованием KSK-2010, в связи с чем операции по подтверждению достоверности будут продолжать успешно выполняться еще некоторое время.

3.1 Сбои начнут возникать, когда станет невозможно выполнять валидацию ZSK

Каждый раз при получении ответа от авторитативного DNS-сервера, валидирующий резолвер проверяет подлинность подписи этого ответа. Результат проверки подлинности или статус валидации подписи по каждому имени сохраняется в кэше резолвера. Для валидации подписи такого имени, как «www.example.com», резолверу необходимо выполнить валидацию подписей в корневой зоне, в «.com», «example.com» и «www.example.com». Обычно резолверы кэшируют результат подобных операций по валидации, чтобы не выполнять их для каждого имени. Большинство резолверов

[8] http://www.potaroo.net/ispcol/2018-04/ksk.html

выполняет валидацию только при возникновении вероятности изменения статуса валидации.

TTL для записей KSK и ZSK составляет 48 часов. При получении резолвером комплекта ключей корневой зоны и выполнении их валидации *непосредственно* перед моментом обновления ключа, этот резолвер в течение практически двух суток не будет располагать информацией о том, что ключ обновился, так как не будет делать попуток получить новый KSK до поступления первого запроса по истечении TTL комплекта ключей корневой зоны. На обычный резолвер, которым пользуется лишь несколько пользователей, подобный триггерный запрос поступает в течение нескольких минут (или даже секунд) после истечения TTL записей DNSKEY. На резолвер с одним пользователем, первый запрос может поступить через несколько часов (или даже дней) после истечения TTL комплекта ключей корневой зоны.

Следует учесть, что представленное здесь описание немного упрощено по сравнению с тем, что происходит в действительности. Например, для некоторых резолверов определена максимальная продолжительность TTL, что может заставить их быстрее заметить, что произошло обновление ключа. Другие параметры конфигурации также могут повлиять на момент обнаружения резолвером факта смены ключа.

3.2 Что увидит пользователь в случае отказа всех обслуживающих его резолверов

В какой-то момент в течение 48 часов после смены ключа запросы некоторых пользователей к DNS начнут выполняться с ошибками, потому что они будут заставлять резолвер снова запросить комплект ключей корневой зоны. Как было разъяснено выше, нельзя предсказать, когда именно в течение этих 48 часов возникнет первый сбой.

При возникновении этого сбоя, если пользователь обслуживается несколькими настроенными резолверами (что можно сказать о большинстве пользователей), системное программное обеспечение попытается направить запрос другим настроенным пользователем резолверам. Это может замедлить процесс разрешения DNS, поскольку система пользователя будет продолжать пытаться использовать неготовый к смене резолвер перед переходом на готовый к смене резолвер, хотя для пользователя тем не менее разрешение DNS произойдет, и он даже может не заметить снижения в темпе работы. При этом, если ни один резолвер пользователя не готов к обновлению ключа (например, если они все находятся под управлением одной организации, не подготовившей ни один из своих резолверов к смене ключа), в какой-то момент в течение 48 часов после смены ключа в работе пользователя произойдет сбой.

Пользователи заметят различные симптомы сбоев, в зависимости от программы, с которой они работают и ее реакции на ошибки, возникающие при отправке запросов к DNS. В браузерах вероятнее всего станут недоступными веб-сайты (или на уже отображаемой веб-странице прекратят отображаться только изображения). В почтовых клиентах пользователь, возможно, перестанет получать новые письма или при отображении некоторых частей текста сообщения начнут возникать ошибки. Количество подобных сбоев будет постепенно нарастать до тех пор, пока ни одна программа не сможет отображать новую информацию из интернета.

Обратите внимание, что понятие «пользователи» в данном контексте относится не только к людям. Автоматизированные системы, которые тоже используют неподготовленные к смене ключа резолверы для разрешения DNS, начнут давать сбои, возможно, катастрофические.

После того, как оператор резолвера устранит невозможность валидации (либо добавив KSK-2017 в качестве якоря доверия, либо отключив валидацию), нормальный режим работы пользователей в интернете должен восстановиться практически мгновенно.

3.3 Как операторы резолверов узнают об отказе

Оператор резолвера, настроивший программу для мониторинга системы на отслеживание ошибок в системе, получит предупреждение сразу после извлечения резолвером новой копии комплекта ключей корневой зоны и возникновения ошибок при валидации. Подобный мониторинг дает оператору наилучшую возможность быстро обнаружить и устранить сбой.

Если оператор не осуществляет активный мониторинг серьезных ошибок, вероятнее всего он не узнает о сбоях при валидации до тех пор, пока не начнут выходить из строя автоматизированные системы, использующие этот резолвер, или не поступят жалобы от пользователей на перебои в работе. Кроме того, если на всех резолверах оператора используется неправильная конфигурация якорей доверия, ему не будет доставляться электронная почта, и он сможет узнать о возникших проблемах только по телефону.

3.4 Восстановление после сбоя, возникшего из-за отсутствия готовности

Как только оператор обнаруживает, что его резолвер перестал выполнять валидацию DNSSEC, ему следует изменить конфигурацию своего резолвера, временно отключив валидацию DNSSEC. Это должно привести к немедленному исчезновению проблемы.

Затем оператору следует максимально быстро установить KSK-2017 в качестве якоря доверия и снова включить валидацию DNSSEC. Корпорация ICANN подготовила инструкции по обновлению якорей доверия для наиболее распространенного вида программного обеспечения резолверов.[9]

4. Что увидят операторы корневых серверов

После обновления ключа операторы корневых серверов увидят, что количество запросов от резолверов, не подготовленных к обновлению, существенно возрастет. Скорее всего, это будут запросы DNSKEY корневой зоны (./IN/DNSKEY), а также запросы записи DS зоны .net (.net/IN/DS). Кроме того, поскольку правильная валидация ответов невозможна, они не будут кэшироваться, что приведет к общему увеличению объема трафика, исходящего от этих резолверов. Аналогичным образом, операторы резолверов, которые

[9] https://www.icann.org/dns-resolvers-updating-latest-trust-anchor

позволяют другим резолверам перенаправлять трафик через них, вероятно будут наблюдать рост количества подобных запросов после обновления ключа.

Исследователи уже следят за объемом трафика, связанного с запросами DNSKEY корневой зоны, чтобы получить исходные данные о типичном количестве подобных запросов в минуту. 11 из 12 организаций-операторов корневых серверов передают эти статистические данные корпорации ICANN практически в режиме реального времени (ежеминутно). ICANN будет продолжать следить за этой статистикой после начала процедуры смены ключа и передавать информацию о результатах операторам корневых серверов и остальной части технического сообщества DNS.

Приложение А. Где получить дополнительную информацию о процедуре обновления ключа

Основной источник информации о процедуре обновления ключа:
http://www.icann.org/kskroll
На этой странице размещено «Краткое руководство о процедуре обновления ключа KSK», множество ресурсов о DNSSEC, описание причин, по которым сообщество приняло решение обновить ключ, и описание процедуры обновления ключа. Страница доступна на английском, арабском, испанском, китайском, корейском, португальском, русском, французском и японском языках.

Подпишитесь на лист рассылки для обсуждения вопроса смены ключа:
https://mm.icann.org/listinfo/ksk-rollover

Приложение Б. Глоссарий

DNSSEC — расширения безопасности DNS, которые позволяют авторитативному серверу подписывать записи DNS при помощи криптографического ключа, чтобы резолвер мог убедиться в отсутствии изменений данных в записях.[10]

KSK — ключ для подписания ключей. Это ключ, который используется для подписания всех ключей в зоне.

Обновление ключа — замена существующего ключа для подписания ключей в зоне на новый ключ.

TTL — «время существования» группы записей в DNS. При получении резолвером набора записей от авторитативного сервера, они обычно сохраняются в кэше резолвера в течение количества секунд, определенного значением TTL.

Валидация — подтверждение подлинности подписей записей в зоне, защищенной DNSSEC. Резолверы выполняют валидацию, чтобы убедиться в подлинности записей, получаемых ими от авторитативных серверов.

[10] https://meetings.icann.org/en/marrakech55/schedule/sun-dnssec-everybody

ZSK — ключ подписания зоны. Это ключ, который используется для подписания всех записей в зоне, не являющихся ключами (последние подписываются ключом для подписания ключей).