Qué esperar durante el traspaso de la KSK de la Raíz

Oficina del Director de Tecnologías de la ICANN

22 agosto de 2018

Resumen Ejecutivo

Tras el inicio del traspaso de la KSK de la raíz (actualmente planificado para el 11 de octubre de 2018), se prevé que un porcentaje muy pequeño de usuarios de Internet tenga problemas para resolver algunos nombres de dominio. En la actualidad, existe un pequeño número de Extensiones de Seguridad del Sistema de Nombres de Dominio (DNSSEC) que validan resolutores recursivos que están configurados incorrectamente y algunos de los usuarios que dependen de estos resolutores tendrán problemas. Este documento describe qué usuarios tendrán problemas y, entre ellos, qué tipo de problemas tendrán en diferentes momentos.

- Los usuarios que se basan en un resolutor que no realiza la validación de DNSSEC no verán ningún efecto a causa del traspaso.
- Los usuarios que se basan en un resolutor que tiene la nueva KSK no verán ningún efecto a causa del traspaso.
- Si ninguno de los resolutores de los usuarios tiene la nueva KSK en su configuración de anclaje de confianza, el usuario probablemente comenzará a ver los efectos en algún momento dentro de las 48 horas después de que ocurra el traspaso.
- Es imposible predecir en qué momento los operadores de los resolutores afectados notarán fallas de validación.
- Según el análisis de los datos pertinentes, más del 99% de los usuarios cuyos resolutores están validando no se verá afectado por el traspaso de la KSK.

1. Introducción

La organización de la ICANN lleva varios años anunciando el próximo traspaso de la KSK de la zona raíz del DNS.[1] Durante los comentarios públicos recientes sobre los planes revisados del traspaso,[2] muchos miembros de la comunidad solicitaron más detalles sobre este proceso. La organización de la ICANN acordó publicar más materiales para ayudarles a prepararse para el traspaso.[3] Este documento es parte de esa iniciativa.

En varias comunidades, surgió cierta confusión acerca de lo que sucederá (o lo que no sucederá) una vez que se produzca el traspaso. Este documento aporta detalles sobre lo que se espera a partir del momento en que se produzca el traspaso.

Este documento está dirigido a diversos tipos de público. Entre ellos, se destacan los siguientes tres grupos:

- Operadores de resolutores de validación que desean saber dónde focalizar su atención una vez que ocurra el traspaso.

[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

- Periodistas no especializados en temas técnicos y demás personas que deseen escribir sobre el traspaso antes y durante este acontecimiento.
- Investigadores que estarán a cargo de monitorear el DNS para detectar indicaciones de fallas en los resolutores una vez ocurrido el traspaso.

Cabe señalar que el presente documento probablemente sea de poco interés para quienes utilizan al menos un resolutor que está listo para el traspaso. Después de que se produzca el traspaso, estos usuarios no verán cambios al usar el DNS o Internet en general. Lo mismo se aplica a los usuarios cuyos resolutores no validan DNSSEC. Según las estimaciones actuales, dos tercios de los usuarios recurren a resolutores que aún no validan DNSSEC.

El traspaso está programado para el 11 de octubre de 2018. La fecha del traspaso de la KSK aún debe ser ratificada por la Junta Directiva de la ICANN con antelación a este acontecimiento. El traspaso se planificó originalmente para el 11 de octubre de *2017*, pero se pospuso debido a que se recibieron datos poco claros justo antes de la fecha programada.[4]

Las secciones 2 y 3 de este documento describen lo que sucederá después del traspaso con los resolutores de validación que están preparados, como también con aquellos que no lo están. La sección 4 describe lo que podrían ver los investigadores que monitorean el tráfico hacia el sistema de servidores raíz del DNS. A lo largo de este documento, hay expresiones no deterministas que se usan para describir lo que sucederá después del traspaso. Esta redacción se utiliza porque no hay forma de que otra persona que no sea el operador de un resolutor pueda determinar con exactitud qué software está ejecutando el resolutor, y no hay forma de saber si un resolutor incluso está configurado correctamente para el traspaso.

Nota importante para los operadores de resolutores: todos los operadores de resolutores de validación que lean este documento deben verificar de inmediato si están preparados para el traspaso mediante la verificación de sus anclajes de confianza actuales.[5] Si los operadores no están listos, deben actualizarlos con los últimos anclajes de confianza en la primera oportunidad que tengan.[6] Los operadores de resolutores que no están realizando validación de DNSSEC ya están preparados para el traspaso.

1.1 Definición del traspaso de la KSK de la Raíz

La zona raíz del DNS se firmó con DNSSEC en 2010. La zona raíz del DNS tiene dos tipos de claves; las claves para la firma de la zona (ZSK) que firman los datos principales en la zona raíz y las claves para la firma de la llave (KSK) que firman solo el conjunto de claves de la raíz (tanto ZSK como KSK) en la zona raíz. Cada tres meses, se publica una nueva ZSK. Cada nueva ZSK está firmada por una KSK de mayor duración.

El traspaso se produce cuando se modifica la KSK de la raíz y la nueva KSK comienza a firmar la clave de la raíz configurada para la zona. En el momento del traspaso, se retirará la KSK original y se utilizará la nueva KSK. La primera KSK se llama KSK-2010 (todavía en uso en la actualidad). La nueva KSK se llama KSK-2017. Después del traspaso, la KSK-2010 ya no firmará el conjunto de claves de la raíz: en su lugar, lo firmará la KSK-2017.

[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

1.2 Anclajes de confianza

Para poder comprender cómo ocurrirá el traspaso, también es importante comprender cómo el resolutor de validación confía en la KSK de la raíz. Cada resolutor de validación se configura con un conjunto de *anclajes de confianza*, que son copias de las claves o identificadores de clave que coinciden con la KSK de la raíz. Los anclajes de confianza suelen configurarse automáticamente mediante proveedores de software o mediante resolutores que están configurados para actualizar automáticamente los anclajes de confianza utilizando el proceso descrito en el documento RFC 5011,[7] o mediante el operador de resolutores que agrega de forma manual una nueva KSK al repositorio de anclajes de confianza del resolutor.

Antes de que existiera la KSK-2017, todos los resolutores de validación solo tenían la KSK-2010 configurada como anclaje de confianza. Después de que se creó y publicó la KSK-2017, la mayoría de los operadores de resolutores agregaron manualmente la KSK-2017 a la configuración de anclajes de confianza de su resolutor, o el cambio lo hacía su software (como con el proceso de actualización automatizado que se describe en el documento RFC 5011) o su proveedor de software. Sin embargo, algunos operadores de resolutores no actualizaron su configuración, y ahora no están preparados para el traspaso porque todavía tienen la KSK-2010 como anclaje de confianza. Cuando se produzca el traspaso, estos operadores de resolutores no tendrán anclajes de confianza válidos.

2. Resolutores que están preparados para el traspaso

Los resolutores que están preparados para el traspaso ya tienen la KSK-2017 configurada como anclaje de confianza. Cuando se produzca el traspaso, estos resolutores continuarán funcionando igual que antes del traspaso porque la nueva KSK de la raíz ya es confiable para firmar el conjunto de claves de la raíz. Algún software de resolutores podría observar en los registros operacionales que se produjo un traspaso, pero es poco probable que se vean esas entradas de registro (si es que existen) a menos que el operador las esté buscando específicamente.

Los usuarios de resolutores que están preparados para el traspaso no verán ninguna diferencia cuando ocurra el traspaso. Las respuestas que obtienen a las consultas normales serán idénticas antes y después del traspaso. De acuerdo con una investigación reciente del APNIC,[8] más del 99 % de los usuarios cuyos resolutores realizan validación de DNSSEC utilizan resolutores que están preparados para el traspaso.

La mayoría de los usuarios de Internet tienen configurado más de un resolutor del DNS. Si alguno de los resolutores que un usuario ha configurado está preparado para el traspaso, el software del usuario debería encontrar ese resolutor después del traspaso y continuar usándolo. Esto puede reducir la velocidad de la resolución del DNS, ya que su sistema sigue intentando utilizar el resolutor que no está preparado antes de cambiar al resolutor que está preparado, pero el usuario aún obtendrá la resolución del DNS.

[7] https://datatracker.ietf.org/doc/rfc5011/
[8] http://www.potaroo.net/ispcol/2018-04/ksk.html

3. Resolutores que no están preparados para el traspaso

Si un resolutor solo tiene la KSK-2010 configurada como anclaje de confianza, después del traspaso, comenzará a dejar de validar las respuestas que obtiene de los servidores autoritativos. Sin embargo, el momento en que esa falla comience a suceder no es predecible.

Aunque la publicación en el DNS es una acción instantánea, puede haber un retraso hasta que un resolutor vea un registro recientemente publicado. Cada registro en el DNS tiene un "tiempo de vida útil" (generalmente denominado *TTL*) durante el cual un resolutor no intentará obtener una versión más nueva del registro. Después del momento del traspaso, un resolutor probablemente todavía tenga una versión almacenada en la memoria caché de la firma realizada por la KSK-2010 y, por lo tanto, continuará validando sin problemas, al menos durante un tiempo.

3.1 La falla comienza cuando la ZSK no se puede validar

Cada vez que un resolutor de validación obtiene una respuesta de un servidor de nombre autoritativo, verifica la firma en esa respuesta. Guarda el estado de validación de la firma de cada nombre en su memoria caché. Para validar la firma en un nombre como "www.ejemplo.com", el resolutor debe validar las firmas en la raíz, en ".com", en "ejemplo.com" y "www.ejemplo.com". Los resolutores normalmente almacenan estas validaciones en la memoria caché para no tener que hacerlo con cada nombre. La mayoría de los resolutores solo realizan validaciones cuando el estado de validación puede haber cambiado.

El TTL para los registros de KSK y ZSK es de 48 horas. Si un resolutor obtiene el conjunto de claves de la raíz y lo valida *justo* antes de que ocurra el traspaso, ese resolutor no se enterará del traspaso durante casi dos días, porque el resolutor no obtendrá una nueva KSK hasta que obtenga la primera consulta después de que el TTL del conjunto de claves de la raíz haya caducado. En un resolutor normal con solo unos pocos usuarios, esa consulta de activación ocurrirá en unos minutos (o incluso segundos) después de que haya caducado el TTL de los registros de DNSKEY. En un resolutor con un solo usuario, el tiempo antes de la primera consulta podría ser de horas, o incluso días, después de que haya caducado el TTL del conjunto de claves de la raíz.

Tenga en cuenta que esta descripción es un poco más simple de lo que realmente sucede. Por ejemplo, algunos resolutores imponen una duración máxima en los TTL, lo que podría hacer que esos resolutores vean el traspaso de la clave en un período de tiempo más corto. Otras opciones de configuración también pueden afectar el momento en que el resolutor ve el traspaso por primera vez.

3.2 Qué verán los usuarios cuando fallen todos sus resolutores

En algún momento dentro de las 48 horas posteriores al momento del traspaso, las consultas del DNS de algunos usuarios comenzarán a fallar porque harán que el resolutor obtenga nuevamente la clave la raíz. Como se explicó anteriormente, no se puede predecir cuándo fallarán los primeros resultados durante ese período de 48 horas.

Cuando ocurra esta falla, si el usuario tiene múltiples resolutores configurados (como lo hacen la mayoría de los usuarios), el software de su sistema probará los otros resolutores que el usuario haya configurado. Esto puede reducir la velocidad de la resolución del DNS ya que su sistema sigue intentando utilizar el resolutor que no está preparado antes de cambiar al resolutor que está preparado, pero el usuario aún obtendrá la resolución del DNS y puede que ni siquiera note la reducción de velocidad. Sin embargo, si ninguno de los resolutores del usuario está preparado para el traspaso (como sucede cuando todos los resolutores son gestionados por una organización y esa organización no tiene listo ninguno de sus resolutores), el usuario comenzará a ver el error en algún momento dentro de las 48 horas posteriores al traspaso.

Los usuarios verán diferentes síntomas de falla en función del programa que estén ejecutando y cómo ese programa reaccione ante las búsquedas fallidas del DNS. En los navegadores, es probable que una página web no esté disponible (o posiblemente que solo dejen de aparecer las imágenes en una página web ya visualizada). En los programas de correo electrónico, es posible que el usuario no pueda recibir correo nuevo o que partes de los cuerpos de mensajes muestren errores. Las fallas se propagarán en cascada hasta que ningún programa pueda mostrar nueva información de Internet.

Tenga en cuenta que el término "usuarios" en este documento no solo indica seres humanos. Los sistemas automatizados que también estén utilizando resolutores no preparados para su resolución del DNS comenzarán a fallar, posiblemente de manera catastrófica.

Una vez que el operador del resolutor corrija la imposibilidad de validar (agregando la KSK-2017 como anclaje de confianza o desactivando la validación), la experiencia de Internet de los usuarios debería volver a la normalidad casi de inmediato.

3.3 Cómo sabrán los operadores de resolutores que hay una falla

El operador de un resolutor que ha configurado su software de monitoreo del sistema para buscar errores significativos será alertado inmediatamente después de que el resolutor busque una nueva copia del conjunto de claves de la raíz y no pueda ser validado. Dicho monitoreo ofrece al operador la mejor posibilidad de detectar y recuperarse rápidamente de los errores.

Si el operador no monitorea de forma activa los errores significativos, probablemente no se enterará de la validación fallida hasta que los sistemas automáticos que se basan en el resolutor comiencen a fallar, o los usuarios comiencen a llamarlos por interrupciones. Si el operador solo está utilizando resolutores con configuraciones de anclaje de confianza incorrectas, es posible que no pueda recibir los mensajes de correo electrónico que se le envían y que solo se entere de los problemas mediante llamadas telefónicas.

3.4 Recuperación ante la falta de preparación

Tan pronto como los operadores descubran que la validación de DNSSEC de su resolutor está fallando, deberían cambiar la configuración del resolutor para deshabilitar temporalmente la validación de DNSSEC. Esto debería lograr que los problemas se detengan inmediatamente.

Posteriormente, y a la brevedad posible, el operador debe instalar la KSK-2017 como anclaje de confianza y activar nuevamente la validación de DNSSEC. La organización de la ICANN

brinda instrucciones para actualizar los anclajes de confianza para el software de resolutores comunes.[9]

4. Qué verán los operadores de servidores raíz

Después del traspaso, los operadores de servidores raíz comenzarán a ver muchas más consultas de los resolutores que no están preparados para el traspaso. Esas consultas probablemente serán para la DNSKEY de la raíz (./IN/DNSKEY), y también probablemente incluirán consultas para el registro DS de la zona .net (.net/IN/DS). Además, dado que las respuestas no se pueden validar correctamente, no se almacenarán en la memoria caché, lo cual generará un aumento general del tráfico de estos resolutores de validación. De forma similar, los operadores de resolutores que permiten que otros resolutores reenvíen a través de ellos probablemente comenzarán a ver un aumento en los conteos de estas solicitudes después del traspaso.

Los investigadores ya están monitoreando el tráfico de los servidores raíz para las solicitudes de DNSKEY con el fin de obtener una referencia de la cantidad típica de consultas por minuto. 11 de las 12 organizaciones de servidores raíz informan estas estadísticas a la ICANN casi en tiempo real (una vez por minuto). La ICANN continuará monitoreando esas estadísticas una vez que comience el traspaso y notificará los resultados a los operadores de servidores raíz y al resto de la comunidad técnica del DNS.

Apéndice A. Dónde obtener más información sobre el traspaso

Esta es la fuente principal de información sobre el traspaso:
http://www.icann.org/kskroll
Esa página contiene una Guía rápida sobre el traspaso de la KSK y un extenso conjunto de recursos sobre DNSSEC. En la página también se indica el motivo por el cual la comunidad eligió realizar un traspaso y los planes para llevarlo a cabo. La página se encuentra disponible en inglés, español, francés, ruso, árabe, chino, portugués, coreano y japonés.

Suscríbase a esta lista de correo electrónico para participar en los debates sobre el traspaso:
https://mm.icann.org/listinfo/ksk-rollover

Apéndice B. Glosario

DNSSEC: extensiones del DNS que permiten que un servidor autoritativo firme criptográficamente registros del DNS para que un resolutor pueda estar seguro de que los datos en los registros no se alteraron.[10]

KSK: clave para la firma de la llave de la zona raíz; la clave que se utiliza para firmar todas las llaves en una zona.

[9] https://www.icann.org/dns-resolvers-updating-latest-trust-anchor
[10] https://meetings.icann.org/en/marrakech55/schedule/sun-dnssec-everybody

Traspaso: cambio de clave para la firma de la llave en una zona de una clave existente a una clave nueva.

TTL: el "tiempo de vida útil" para un conjunto de registros en el DNS. Cuando un resolutor obtiene un conjunto de registros de un servidor autoritativo, por lo general conserva esos registros en su memoria caché durante la cantidad de segundos indicada en el TTL.

Validación: validación de las firmas en los registros en una zona que está protegida por DNSSEC. Los resolutores realizan la validación para asegurarse de que los registros que reciben de un servidor autoritativo sean correctos.

ZSK: clave para la firma de la llave de la zona; la clave que se utiliza para firmar todos los registros en una zona distinta de las claves (que están firmadas por la clave para la firma de la llave).