YEŞIM NAZLAR: Buenos días, buenas tardes y buenas noches. Bienvenidos a esta llamada de resumen de At-Large sobre la clave para la firma de la llave del DNSSEC de la zona raíz y su implementación por parte de la ICANN, el día miércoles 19 de octubre de 2016, a las 19:00 UTC.

No vamos a pasar asistencia, pero quiero recordarles a todos los participantes que se encuentren conectados telefónicamente que por favor silencien sus micrófonos o los parlantes de las computadoras mientras no estén tomando la palabra. Para la transcripción y para que también los intérpretes puedan identificarlos en el canal lingüístico correspondiente al momento de tomar la palabra mencionen sus nombres por favor. Contamos con interpretación al francés y al español. Muchas gracias por su participación.

Le doy la palabra ahora al señor Tijani Ben Jemaa. Adelante por favor.

TIJANI BEN JEMAA: Muchas gracias, Yesim. Buenos días, buenas tardes y buenas noches a todos. Muchas gracias por participar de este seminario web.

Como saben, la ICANN está cambiando la clave para la firma de la llave del DNSSEC y pensamos que sería un evento importante sobre el cual ustedes quisieran conocer un poco más.

Voy ahora a darle la palabra al personal para que haga algunos anuncios y luego vamos a dar comienzo al seminario. Yesim, adelante por favor.

YEŞIM NAZLAR: Muchas gracias, Tijani.

Vemos que hay una presentación en pantalla que muestra la sala de Adobe Connect. Vamos a tener un pod de preguntas y respuestas durante el seminario. Entonces si tienen preguntas, los invitamos a que coloquen esas preguntas en esta parte y luego se van a responder. También vamos a tener un cuestionario de preguntas y respuestas y una evaluación después de la presentación, así que estén preparados para responder estas preguntas de evaluación. Muchas gracias.

Así que, Tijani, le cedo nuevamente la palabra.

TIJANI BEN JEMAA: Muchas gracias, Yesim.

Como dije, este es un evento importante y la comunidad de At-Large desea recibir información porque cuenta con muchos usuarios finales. Nuestro presentador del día de hoy es una persona muy importante en materia de la firma de la llave. Es el vicepresidente de investigación para la ICANN. Va a dar una presentación sobre esta clave para la firma de la llave del DNSSEC.

La clave para la firma de la llave de la zona raíz KSK es una clave criptográfica muy importante en las cuestiones de seguridad o de extensiones de seguridad del DNS o DNSSEC. El DNSSEC protege a los usuarios finales de recibir información falsa y evita ataques que puedan llevar a una dirección errónea o a un sitio web que sea malicioso. Por esta razón, hemos invitado a Matt para que nos cuente un poco más al respecto y nos diga quienes pueden estar alcanzados por esta cuestión. Así que, Rod, adelante por favor.

MATT LARSON: En realidad mi nombre es Matt Larson. Soy vicepresidente de investigación de la oficina de la ICANN. Muchas gracias a todos por la invitación. Voy a comenzar con mi presentación.

Ustedes habrán escuchado que hay un cambio, que la ICANN está a punto de cambiar un parámetro de configuración muy importante en el DNSSEC. Y para los operadores de red, esto puede dar lugar a la necesidad de tomar acción. Entonces en este debate vamos a informarles de cómo funciona el DNS y luego vamos a hablar de qué es lo que va a suceder y cuándo se va a llevar a cabo este cambio. Las preguntas las voy a responder al final de mi presentación.

Vamos a comenzar en primer lugar a hablar sobre cómo funciona el DNS. Creo que ya todos están familiarizados con el DNS. Aquí vemos un muy breve ejemplo de una dirección de IP, que representa un nombre de dominio, como por ejemplo .com. Esto es la dirección traducida. El DNSSEC lo que hace es agregar una firma criptográfica a esta firma adicional que se ya existe.

Entonces qué es la validación del DNSSEC? Es un proceso de inspeccionar la firma digital y los datos para verificar que la respuesta sea apropiada y también para verificar la coherencia de esos datos. Para validar la firma se requiere una llave pública. Una llave privada genera una firma y una llave pública es necesaria para validar esa firma.

La razón por la cual tenemos el DNSSEC es que los protocolos del DNS en algunas oportunidades son un tanto ingenuos y fáciles de falsificar. Entonces si no se utiliza el DNSSEC básicamente uno tiene que confiar

en los anclajes que tiene. Y no hay manera de saber si la respuesta que está recibiendo realmente proviene de la persona o lugar ante el cual uno emitió una consulta, si son respuestas verdaderas o no o si es información real o verdadera. Durante los años se ha debatido el tema y algunos desarrolladores estuvieron un tanto paranoicos sobre esta cuestión.

Pero el hecho de tener DNSSEC no implica una protección absoluta. Con el DNSSEC podemos confiar esta información que existe dentro del DNS de una manera más segura porque tenemos una prueba criptográfica de que los datos que se reciben son los mismos datos que los miembros han enviado y que estos datos no son modificados conforme van pasando de un servidor a otro o de un servidor al cliente. No solamente el DNS sirve para esto, sino que también se puede utilizar para extensiones para asegurar por ejemplo la transferencia de correo electrónico. Una forma de asegurar la transferencia de correo electrónico seria mediante el DNSSEC y también mediante el agregado de un certificado de operaciones mediante certificado X509.

El DNSSEC tiene tres tipos de registros que mantienen los datos de la llave criptográfica. Creo que si tenemos estos tres. Quizás no todos tengan el mismo formato, pero para cada zona del DNS que se afirma y está protegida con el DNSSEC, tiene dos claves importantes. Una es la clave para la firma de la llave. Esta llave engloba todas las llaves de la zona. Otra implica la llave para la firma de la zona que es la que produce firmas especificas o todas las firmas que van a ser luego validadas. Luego vamos a tener un firmante de la delegación. Este es un puntero a la llave. Lo bueno es que el DNS de esta manera está protegido, pero también tenemos una mala noticia que es que no siempre las

operaciones terminan siendo del todo protegidas. No obstante, este tema lo vamos a tratar en alguna otra presentación.

Les voy a dar más detalles en las próximas diapositivas, pero quiero darles un ejemplo sencillo y simplificado con esta diapositiva. Aquí mostramos de qué manera se valida una firma. Tenemos datos del DNS en la parte superior. Este sería un registro con una dirección de IPBv6, por ejemplo www.ejemplo.com. Tiene una firma digital y para eso vamos a necesitar la creación de una llave pública. Entonces una vez que tenemos toda esta información se puede validar esa firma. Y si es legitima se valida, y si no es legitima significa que los datos no pueden ser validados. En color naranja tenemos la clave para la firma de la zona para poder hacer la validación. La pregunta es de qué manera o cómo podemos confiar en esta información.

Entonces para esto llegamos a esta diapositiva y llegamos a la situación actual donde hablamos de la firma de la zona. El DNS requiere un cambio para poder incrementar la confianza. Y para poder confiar en la llave es necesario comenzar con una llave en la cual uno confíe y para eso es necesario implementar anclajes de confianza. En la zona raíz, por ejemplo KSK, esto sería el anclaje de confianza que vamos a utilizar como ejemplo. Cuando uno habla de un anclaje de confianza quiere decir que el validador del DNS confía en esto y se confía en la información y le decimos al validador que confiamos plenamente en lo que esto contiene. El proceso de validación del DNS entonces comienza con esta clave y luego se valida la clave para la firma de la zona y la validación para .com apunta a .com KSK.

No voy a leer toda la diapositiva, pero como pueden ver esto da un cambio en la confianza y en la firma. Al implicar este cambio de confianza se puede hacer un seguimiento de la firma y también confiar en la clave para la firma. Una vez que esto sucede se puede utilizar esta clave y también incluir por ejemplo el registro que tenemos aquí con la dirección de IP que sería en nuestro ejemplo www.ejemplo.com. Sé que hay mucha información contenida en esta diapositiva, pero es importante ilustrarlo. Y lo importante aquí es que la clave para la firma de la llave de la zona raíz es un punto de partida para la validación. Se firman muchos TLD, por tanto hay muchísima información en la zona raíz. Y lo importante es que esto refuerza lo que dije anteriormente en cuanto a que el KSK es un punto de partida para todos aquellos que contengan el DNSSEC.

Ahora bien, como dije anteriormente, el anclaje de confianza es una clave específica, en el cual uno tiene plena confianza a los fines de la verificación o para verificar respuestas. Uno puede tener confianza en este anclaje de confianza porque está diseñado con un software particular y uno confía en esto, o quizás uno mismo configuró este anclaje de confianza. Pero de una manera u otra, independientemente de la confianza que tengamos, es importante tenerlo en cuenta.

Hay diferentes anclajes de confianza. Se pueden poner diferentes claves. Esto no sería del todo común, pero el anclaje de confianza de la raíz es un paso importante, en el cual me quiero focalizar ahora. Vamos a hablar ahora un poco de las especificidades del DNSSEC en la zona raíz. La administración de la zona raíz es un tanto complicada, dado que hay múltiples organizaciones que cooperan con la gestión de la zona raíz. La ICANN es responsable de la operación de la clave para la firma

de la zona raíz y VeriSign es responsable de la operación de la clave para la firma de la zona raíz.

El ZKF necesita ser verificado cuando cambia el DNS. Y cuando cambie esto tiene que ser verificado nuevamente. Por eso se verifica el KSK y esto se hace a través de una ceremonia para la firma de la llave. Estas son actividades que están coordinadas, pero se realizan de manera separada. La clave KSK actual fue creada en el 2010. Esta almacenada en lo que denominamos módulos de seguridad de hardware en dos instalaciones de gestión de la clave diferentes, en la cual la ICANN conoce y que están muy bien protegidas y que tienen muchos niveles y procesos de seguridad en relación al acceso a estas instalaciones. Esto por supuesto da lugar a todo un debate respecto de cómo se maneja la KSK. Pero por el momento voy a decir que la KSK está muy bien protegida y es un proceso que se lleva a cabo de manera muy cuidadosa.

Hay diferentes formas de lograr la KSK de la zona raíz. Tenemos lo que se denomina las consultas al DNS. Pero esto sería similar a otros casos. No estaría protegido. Lo importante aquí es que la KSK de la raíz es un punto de partida, un punto de verificación. Uno puede obtener esta KSK de la raíz mediante el sitio web que se muestra en la diapositiva. También los anclajes de confianzas pueden utilizarse y de esta manera obtener certificados. De una manera u otra, la idea es garantizar la KSK de la raíz.

Otra forma es confiar en la información que uno obtiene cuando por ejemplo se resuelven las validaciones del DNS. Así que hay un plan para cambiar esta clave para la firma. Dado que es la primera vez que lo

cambiamos (la primera KSK fue creada hace 6 años), este plan no tiene precedentes porque hay diferentes partes involucradas que interactúan y que van a tener un impacto. Todos los que utilizan la validación del DNS van a tener que efectuar este cambio en la KSK. Esto será parte de un proceso. Básicamente el cambio será automáticamente, pero es importante que uno esté al tanto de todos los cambios que se van a realizar, especialmente si uno opera software de validación del DNS porque hay que garantizar que, incluso aunque la clave cambie automáticamente, todo lo demás se cambie correctamente. Y también es imposible saber si todo el mundo hace validación del DNSSEC. No es posible obtener esa información, por ejemplo en los nombres de servidores recursivos. Así que lo que la ICANN está tratando de hacer es diseminar información de este estilo para que la comunidad sepa qué es lo que está sucediendo y también para crear conciencia.

Es por eso que cuando se cambia la primera vez la KSK no solo tiene que ver con lo que sucede en la KSK de la raíz. No se trata de una debilidad que tenga, sino que tiene que ver con una buena higiene criptográfica operativa porque los secretos no permanecen así para siempre. Entonces es importante cambiar cada tanto.

También queremos tener un plan porque queremos cambiarlo por distintas circunstancias. No queremos hacerlo cuando haya una situación donde sí pudiera existir un problema, sino que la idea es hacer un cambio repentino. No queremos hacerlo sobre todo la primera vez, sino que lo queríamos hacer en operaciones normales. Tener un plan, poder implementarlo fase por fase. Tampoco lo podemos hacer de forma privada porque todos los que hagan validación DNSSEC no van a poder participar.

Mencioné que había mucha gente de hecho involucrada. Si alguien no recibe el mensaje y no actualiza el software con la nueva clave, el software va a creer entonces o va a dar cada una de las respuestas como invalidas, como que se trata de un ataque que está cambiando todas las respuestas que dé porque no hay ninguna firma que coincida. Entonces no va a poder seguir la cadena de confianza porque no va a funcionar desde el punto de partida. Entonces van a caer todas las resoluciones del DNS.

Vamos a hablar ahora del proyecto en sí mismo. Es importante, sobre todo si están realizando validación del DNSSEC. [Incomprensible], que es una investigadora en IPNIC, ha realizado una investigación y publicó estadísticas donde dice que alrededor del 15% del tráfico del DNS en el mundo está haciendo validación. Yo querría señalar que en lo que hace la firma del DNSSEC no se verá afectado porque realmente es una gran parte del DNSSEC. Tenemos la parte de la firma del DNSSEC, donde la información del DNSSEC se publica y está en los servidores, que necesita ser firmada. Y después tenemos la información del DNS que se busca en los servidores, y en ese caso debe ser validada. Estamos hablando entonces de esta porción de la validación hoy. La firma del DNSSEC no se ve afectada por esto, sino que lo que vamos a sacar es la validación en el DNS cuando buscamos información. Entonces si alguien hace validación del DNSSEC pueden ver cuál es la configuración. Como no lo hicimos nunca anteriormente, digamos que todos debemos estar atentos a este plan y al cambio.

Acá tenemos algo de antecedentes. La ICANN reunió a expertos de la comunidad y personal de la ICANN para desarrollar un plan para cambiar la KSK y se publicó un informe en marzo de 2016. El personal de

la ICANN entonces empezó a desarrollar el proyecto para desarrollar el plan siguiendo las recomendaciones y se han hecho muy pocos cambios.

Entonces para ser transparentes, a principios de julio publicamos todos los planes en el url que pueden ver acá en pantalla. Tenemos todos estos planes publicados, así que quienes estén interesados en el plan, obviamente van a encontrar acá mucho más detalle sobre todo lo que tiene que ver en el cambio de la clave KSK. Pero creo que esta es la imagen más importante que tengo en toda mi presentación porque acá sí que estamos hablando de la KSK de la zona raíz, cuando se va a utilizar la nueva KSK, cuándo va a dejar de funcionar la KSK actual. Y como pueden ver, tenemos una fecha que habla del 11 de octubre de 2017. Sé que falta mucho tiempo; estamos hablando de casi un año; pero debido a la importancia de que reviste el tema y porque hay mucha gente que se va a ver afectada, estamos empezando con bastante anticipación para que todos sepan qué es lo que va a pasar, qué es lo que va a suceder. No voy a hablar de muchos detalles sobre el plan realmente, cuánto va a demorar, pero sí que vamos a ir lento. No tenemos ninguna ceremonia específica en este caso como sucede trimestralmente en la ceremonia para la firma de la llave porque no hay ningún apuro. La verdad no tenemos ningún apuro en hacerlo, entonces vamos a tomar el plan con mucha cautela y seguirlo paso por paso.

Los planes no hablan de ningún cambio en ninguna configuración que tiene que ver con la criptografía actual. No cambia el tamaño de la clave ni el algoritmo criptográfico. Estamos cambiando la clave de forma tal que el protocolo que se llama actualizaciones automáticas de los anclajes de confianza del DNSSEC siga funcionando. Esto lo pueden ver en la RCS 5011. Es el mecanismo que mencioné anteriormente, que

tenía que ver con la actualización de los anclajes de confianza. Brevemente es la forma en que esto funciona es que cuando uno publica un anclaje de confianza tiene el anclaje anterior y firma un nuevo anclaje. Entonces el validador del DNSSEC va a ver que el anclaje de confianza está firmando un nuevo anclaje de confianza. Y entonces, después de 30 días, el validador va a decir que el nuevo anclaje de confianza es el legítimo y va a desechar el anterior. Pero es algo bueno para este proyecto porque todo los validadores de DNSSEC que también siguen este protocolo, el de actualizaciones automáticas, ese validador tiene que ser capaz automáticamente de hacer la validación con el nuevo anclaje de confianza.

Antes estaba publicado el DNSSEC. Lo tenía que ver un validador. Y entonces, después de 30 días, ese validador se va a dar cuenta de que el anclaje de confianza era el valido y lo tenía que configurar. Pero ahora esperamos que para mucha gente ya no tenga que tomar ninguna acción porque el nuevo anclaje de confianza va a ser actualizado de forma automática. También, como dije, este proceso va a entrar dentro de los eventos de mantenimiento normales, con las ceremonias trimestrales y también el plan incluye muchas pruebas, ensayos, como para saber que estamos probando todo con suficiente anticipación y también todos son capaces de entender cuál es el impacto que va a generar.

Un área posible de preocupación tiene que ver con el tamaño de la respuesta. Hay una respuesta en particular que es la respuesta que tiene que ver con todas las claves de la DNS en la zona raíz. Y esa repuesta va a crecer a 1.425 bytes durante el proyecto. Es el máximo histórico para esta respuesta porque no hay respuesta que haya sido

tan larga. Parte de la experimentación, sobre todo con el IPv6, plantea que esto puede ser un problema. Este es el caso en el que la norma de los experimentos sugiere una cosa, pero la operación en la práctica real, la evidencia de la gente que esta haciendo DNS en otras zonas dice que no va a ser un problema. Pero para ser conservadores estamos señalando el tema y lo estamos observando cuidadosamente.

El tema de la fragmentación con el IPv6. El tamaño máximo con el software de IPv6, el máximo es de 1.280 bytes. Entonces los que quizás no tenga esta especificación no van a poder recibir la respuesta de 2.435 bytes en la zona raíz. En ese caso. El segmento va a tener que ser dividido en fragmentos. Entonces la posibilidad de que los fragmentos no lleguen al receptor puede existir.

Acá hay una url para ver esto con más detalles y para poder entenderlo. Personalmente no me preocupa mucho este último punto porque hay otras zonas del DNS que están utilizando DNSSEC y que están utilizando estas respuestas generadas, que son cada vez más grandes, y realmente no han experimentado ningún problema operativo. Entonces este es el caso en el que sabemos que va a haber fragmentos, sobre todo en el caso del IPv6 y sus usuarios, pero hay gente que toma los fragmentos, llegan a destino y nosotros sabemos que en teoría esto puede causar problemas, pero por el otro lado también tenemos evidencia operativa que nos muestra que esto no ha sucedido en forma masiva.

Bueno, acá tenemos algunas de las fechas. Ven en qué momento aumentan los tamaños hasta llegar al tamaño máximo. Quiero marcar el 11 de octubre de 2017 como una fecha muy importante porque ahí se da el crecimiento. Para esa fecha, si no tienen entonces el nuevo anclaje

de confianza no van a poder operar. Como operador es importante saber entonces cómo se confía en esta clave y cómo se la configura. Como operador, cómo se actualizan los anclajes de confianza en el software, se hacen a mano, se hace por algún software de configuración, hay que confiar en el anclaje de confianza que trae el software y que fue provisto por el autor o un paquete de la organización, monitoreo en la realización de DNSSEC, y en ese caso lo van a advertir o no. esto es lo importante de saber si hacen validación y si tienen una configuración de anclaje de confianza es importante saber cómo van a actualizar esa configuración. Es posible que utilicen el protocolo de actualizaciones automáticas y lo que tenga que pasar suceda de forma automática. No voy a hablar del último punto.

Una de las cosas que estamos realizando es trabajar con el software del DNS y desarrollo de distribuidores de herramientas porque nos dimos cuenta de que muchas de estas innovaciones y mucho de este software incluye los anclajes de confianza en el software. Por ejemplo, la validación para el software correcto del DNS pone en el anclaje de confianza codificado en el software en sí mismo o en los archivos de configuración de muestra [incomprensible] con eso como pueden ser los distribuidores de sistemas operativos son las organizaciones que cuando tienen un paquete de software quizás incluyen esos anclajes. Entonces estamos trabajando con esas organizaciones para que sepan ellos que van a cambiar los anclajes de confianza, para que lo tenga en cuenta mientras desarrollan el software. Y entonces cuando hacen el [incompresible] del software tengan estos datos en cuenta.

Esta es una de las formas que puede existir para que la gente reciba sus nuevas claves, actualizando el software. Para quienes desarrollan

códigos, también hay pruebas para que ellos puedan saber realmente que los software van a funcionar con los protocolos actualizados, también la ICANN está desarrollando bancos de prueba con los operadores en sí mismos para permitirles entonces utilizar el software que utilizan actualmente y ver entonces si funcionan bien con los anclajes de confianza nuevos.

Con esto termino mi presentación. Acá les doy algunos enlaces para que busquen más información, que está en la página web de ICANN, en la última viñeta, y después otros lugares donde nos pueden seguir. Con esto termino la presentación, pero escucho preguntas y comentarios. Gracias.

TIJANI BEN JEMAA: Gracias por la presentación. Creo que puede haber sido algo complicado porque es importante saber lo que está pasando y también cómo nos vamos a ver afectados.

¿Hay alguna pregunta? Puedo ver una pregunta en el chat que habla del tamaño de la llave de la KSK. Bueno, el tamaño no está cambiando. La clave es de la misma dimensión en cuanto a bits.

¿Alguna otra pregunta?

HEIDI ULLRICH: Tenemos a Olivier pidiendo la palabra. Tijani, por favor, ¿podría hablar más alto? Porque es muy difícil escucharlo.

TIJANI BEN JEMAA: Muchas gracias. Olivier, por favor.

OLIVIER CRÉPIN-LEBLOND: Muchas gracias por toda esta información y esta presentación, que fue muy interesante para ver cuál es parte del trabajo oculto que existe para que el DNSSEC siga funcionando y para que sea más estable de lo que era.

Brevemente, sobre esta implementación de la nueva clave existe la posibilidad de que esto quizás no funcione o que exista alguna interferencia, cuáles son las precauciones que tomaron en caso de que esto suceda.

MATT LARSON: Muchas gracias. Es una buena pregunta.

Estamos tomando diferentes precauciones. Una de las cosas que estamos haciendo es que tenemos disposiciones como para reversar todos los cambios o como para cancelar todo, y en las ceremonias de firmas de las llave creamos las firmas necesarias para el siguiente trimestre. Como resultado entonces siempre vamos a estar trabajando por adelantado. Y lo que estamos haciendo durante el proceso de implementación es realmente leer versiones múltiples como para que de esta manera podemos pasar directamente de la clave actual a la anterior. Esperamos no tener que hacerlo, pero sí hemos previsto esto. Si algo sucede entonces podríamos volver.

La pregunta entonces es qué podría salir mal. Lo que nos preocupa es que si alguien no recibe el mensaje y no actualiza sus validadores con

los anclajes de confianza, la resolución va a fallar. Pero la buena noticia es que esto es algo fácil de solucionar. Lo único que necesitan hacer es actualizar la clase de confianza. Entonces quizás sea doloroso para un ISP por ejemplo porque llaman los clientes y dicen ¿por qué no puedo tener la resolución de este problema? Pero la segunda parte es fácil porque una vez que está diagnosticado lo único que hacen es actualizar en el DNS. Y eso es fácil. Podemos imaginar la situación de esperar de un proveedor un nuevo software. Uno ya está haciendo la validación DNSSEC en el día de hoy. Entonces se va a poder hacer la validación de esos anclajes de confianza. Es fácil de hacerlo si alguien no se enteró y no actualiza lo que tenía que actualizar.

Esto es lo que más nos preocupa. La gente que no está utilizando los protocolos de actualización automática y por algún motivo no se entera de que va a haber una actualización y entonces no hace una actualización de sus anclajes. Pero también lo que hay involucrado en parte de la validación del DNSSEC es que proviene de grandes proveedores de ICCP. Entonces por ejemplo el DNS público de Google, que tiene un gran porcentaje en el tráfico de DNS hace validación del DNSSEC.

Y por el otro lado, nosotros sabemos que ellos saben bien de este cambio, entonces no me interesaría mucho. Pasa lo mismo con [incomprensible], que es una de las más importantes en EE. UU. Hacen validación del DNSSEC. Ellos también saben de esto. Entonces yo creo y espero que las organizaciones más grandes se van a tomar el tiempo para hacer la validación del DNSSEC, que son miembros activos de esto. Van a conocer con mucha anticipación qué es lo que está sucediendo y van a poder tomar las medidas correspondientes. Creo que quizás se

trate de las personas individuales o de los operadores más pequeños los que quizás no reciban la información de la actualización. La idea es que nadie quede afectado, pero creo que quizás obviamente lo mejor sería que esté afectado un individual y no un ISP muy grande.

TIJANI BEN JEMAA: Muchas gracias. ¿Alguna otra pregunta?

Por supuesto, todos saben que podemos no cambiar esas claves. Y aun así vamos a mantener la seguridad. Pero como ustedes saben, toda clave que tengamos, si la utilizamos durante mucho tiempo puede vulnerarse y ya dejar de ser segura. Entonces lo que se está haciendo ahora es crear esta serie de claves durante seis años, y la gente piensa que ahora ya es momento de hacer este cambio para reforzar la seguridad.

¿Hay alguna otra pregunta, Olivier? ¿Quiere hacer alguna otra pregunta?

OLIVIER CRÉPIN-LEBLOND: Sí, Tijani. Tengo otra pregunta sobre este tema.

A ver, efectivamente, sí hay organizaciones importantes que van a abordar esta cuestión y también hay otras organizaciones más pequeñas que pueden enfrentar un desafío. Ahora la pregunta es: ¿hay alguna manera fácil de saber o tener manuales o presentaciones que muestren paso a paso el proceso, lo que se tiene que hacer, o por ejemplo alguna especie… A ver, cómo decirlo… No es un documento de preguntas y respuestas o de preguntas frecuentes, sino más bien un

documento donde haya soluciones a diferentes problemas, como por ejemplo una lista de verificación. Esto quizás podría ser de utilidad para los operadores o desarrolladores cuando estén en el proceso. Sabemos que el DNSSEC en general no es del todo comprendido o plenamente comprendido por los miembros o por la gente que implementa o que administra dominios. No tienen un pleno conocimiento del tema.

Entonces me preguntaba si tienen un plan al respecto porque por supuesto esto es un proceso realmente significativo. Es un cambio muy importante.

MATT LARSON: Sí, es otra muy buena pregunta.

Bueno, lo que vamos a preparar son los recursos que explican cómo se configuran los anclajes de confianza en los diferentes servidores y cómo se lleva a cabo la validación del DNS, por ejemplo en un servidor de nombres recursivos, y en los que ya se están utilizando para que se describan cuáles serían los problemas que se pueden encontrar y que la gente comprenda, mediante la publicación de estos recursos, cómo operar un anclaje de confianza o cómo operarlos o asegurarse de que el proceso sea automático.

OLIVIER CRÉPIN-LEBLOND: Tengo otra pregunta. ¿Puedo?

TIJANI BEN JEMAA: Sí. Adelante, Olivier.

OLIVIER CRÉPIN-LEBLOND: Gracias, Tijani. Mi siguiente pregunta es esta. ¿Cómo va a afectar todo esto a los dominios de alto nivel en zonas que no están firmadas?

MATT LARSON: Bueno, los afecta porque la zona está firmada y toda respuesta de la zona raíz incluye las firmas del DNS. Así que en realidad afecta a todo el mundo.

TIJANI BEN JEMAA: Muchas gracias, Matt. Yesim levantó la mano. Adelante, por favor.

YEŞIM NAZLAR: Gracias, Tijani. Tenemos una pregunta de uno de los participantes que colocaron en el recuadro de preguntas y respuestas. Dice: "Hola. Soy de Bangladés. Soy [Afifa] de Bangladés. No estaba al tanto de todos estos cambios. ¿Cuáles son los planes para propagar esta información en áreas remotas?"

MATT LARSON: Bien. Una de las cosas que estamos haciendo es enviar versiones de esta presentación a diferentes partes del mundo para que lleguen a los operadores de diferentes regiones en todas las partes del mundo. Por ejemplo mi colega y yo vamos a hacer una presentación en Mauritania, en APNIC, en 2 semanas. También hemos hecho una presentación en APNIC, en Asia, hace poco tiempo. La idea es llegar a todos los operadores del mundo.

Quiero anticipar que mis colegas y yo estamos en una etapa preparatoria. Mis colegas de la ICANN saben que esto es necesario. También se están preparando para este cambio de la firma del KSK.

TIJANI BEN JEMAA: Gracias, Matt. ¿Hay alguna otra pregunta o comentario? si no hay comentarios, entonces le voy a dar la palabra a Yesim para que haga el pop quiz.

YEŞIM NAZLAR: Muchas gracias, Tijani. Tenemos solo una pregunta para esta sesión, así que la voy a leer en voz alta. ¿Cuándo es la fecha concreta del evento de la implementación del KSK de raíz? ¿11 de octubre de 2017, 1 de enero de 2017, 11 de julio de 2017 o 11 de octubre de 2018? Por favor emitan su voto ahora.

La pregunta correcta es… ¿Matt?

MATT LARSON: Es el 11 de octubre de 2017.

YEŞIM NAZLAR: Bueno, esta es la finalización de esta parte. Así que, Tijani, le doy la palabra.

TIJANI BEN JEMAA: Muchas gracias, Yesim. ¿Hay alguna otra pregunta para Matt?

HEIDI ULLRICH: Tijani, creo que tenemos una pregunta en el chat por parte de Glenn.

TIJANI BEN JEMAA: ¿La puede leer, Heidi?

HEIDI ULLRICH: Sí, la voy a leer. La pregunta dice: "Nosotros tenemos algunos operadores que se están uniendo o una adopción despareja de los operadores del IPv6. ¿Los operadores van a actuar en forma más diligente con respecto a esta cuestión?"

MATT LARSON: Bueno, yo diría que hay una diferencia entre la implementación IPv6. Y esta diferencia es que, en cuanto a la acción con la implementación del IPv6, esto no siempre trae cuestiones a los usuarios. Entonces cuando se implementa la KSK, va a tener un impacto inmediato en la implementación, pero hasta cierto punto los que no tienen validación del DNS y firmen la clave van a tener una implementación automática. Rápidamente se van a dar cuenta de que hay algún problema, y entonces van a tener que tomar acción al respecto. Pero la acción correctiva sería bastante sencilla.

TIJANI BEN JEMAA: Muchas gracias, Matt, por la respuesta. ¿Alguna otra pregunta por parte de la audiencia? Adelante, Olivier.

OLIVIER CRÉPIN-LEBLOND: Muchas gracias, Tijani. Tengo otra pregunta más.

Me causa curiosidad lo siguiente. ¿Por qué es necesario que se incremente el tamaño de la llave? No veo por qué es necesario esto. Sé que el crecimiento podría también incorporar algunas otras cuestiones.

MATT LARSON: Bueno, en realidad no está cambiando el tamaño de la firma de la llave. Hay un tamaño específico y va a ser el mismo cuando crezca. Lo que puede confundir es que hay otro cambio que se hizo en VeriSign y es en la firma de la clave para la zona raíz, que tenía 4 bits, y en septiembre VeriSign hizo un incremento de esa cantidad. Por cierto, esto lo que hizo fue que hubiese más respuestas a la zona raíz. Esto lo hizo VeriSign y la ICANN lo monitorea muy de cerca. Así que el KSK y el ZFK tienen 48.000 bytes y va a continuar así.

OLIVIER CRÉPIN-LEBLOND: Pero usted mencionó que la llave del DNS iba a incrementarse durante 20 días. Antes de eso era de 1.914. Y que luego se iba a incrementar a 1.455 durante 20 días.

MATT LARSON: Sí. Yo dije eso, pero lamentablemente tengo la diapositiva que no incluye esta presentación, donde se incluye este cambio.

Esto se refiere puntualmente al tamaño de la respuesta, cuando una consulta al servidor raíz se hace. En cualquier momento puede haber 1 o 2 claves de DNS o KSK dependiendo del momento especifico del que se trate. Cuando se implementa una llave, hay 2 claves. Entonces cuando esto se implemente, habrá dos KSK en la zona raíz.

El estado normal es que haya una KSK y una ZFK, pero en este momento debido al proceso, cuando haya dos ZFK y dos KSK, en este caso, en este puntual momento habrá un incremento en el tamaño de la respuesta, que será de 4825 bytes. Pero esto tiene que ver con este proceso puntual y especifico.

OLIVIER CRÉPIN-LEBLOND: Gracias. ¿Esto ya fue verificado, fue evaluado en alguna red interna o es la primera vez que está sucediendo?

MATT LARSON: No, no es la primera vez que sucede. Ya ha sido probado. En las operaciones normales es algo que sucede y que cualquier operador de red o al momento de configurarlo se puede manejar. Hay fragmentos que viajan en las redes, y esto puede afectar a la red que lo recibe. Pero la inquietud es que hay sistemas que descartan estos segmentos o a veces los servidores de nombres envían un paquete grande y que se queda en el camino, pero también resulta imposible de verificar porque depende de las distintas configuraciones que existan. La buena noticia es que como consecuencia del cambio reciente que hizo VeriSign al cambiar la clave criptográfica, y por tanto el tamaño de la clave para la firma de la zona, hay un incremento del tamaño en la llave del DNS. Esto produce algunas consecuencias.

Hay otros TLD que están firmando el DNSSEC, de tal manera que lo que obtienen es mayor a 1.425. Generalmente es un .org. Por lo general no hay problemas con esto, pero el tamaño de la respuesta de la clave del DNS generalmente es mayor y nunca hay ninguna denuncia o queja de

nadie que se queje al respecto porque se solucionan las cuestiones que van surgiendo. Así que yo, en particular, confío mucho en que cualquier cuestión que vaya a surgir va a ser resuelta y que no va a tener ningún alcance demasiado extenso.

TIJANI BEN JEMAA: Muchas gracias, Matt. Olivier, ¿tiene otra pregunta?

OLIVIER CRÉPIN-LEBLOND: No, ya terminé de hacer preguntas.

TIJANI BEN JEMAA: Muchas gracias, Olivier. Y muchas gracias a todos. Tenemos que agradecer a nuestro orador, Matt Larson, que es vicepresidente de investigación para la oficina de CTO de la ICANN, por su gran presentación. Sé que es un poco complicada, un tanto técnica, pero es necesario que comprendamos estas cuestiones y que comprendamos que cuando suceda el cambio todos van a estar utilizando DNSSEC, y aquellos que lo utilicen van a ser afectados. Entonces tenemos que tener en cuenta esto. Así que esta presentación era necesaria para At-Large para los usuarios finales.

Así que nuevamente muchas gracias. Espero que tengamos otras presentaciones con posterioridad, cuando la implementación del KSK se haya llevado a cabo, donde se detallen los pasos. A mi realmente me gustaría también agradecerle otra vez a Matt por la presentación. Y por supuesto también agradecer a nuestro personal técnico, a nuestro personal, el personal de la ICANN, y a todos ustedes por su participación

en este seminario web. Damos por finalizada esta teleconferencia. Muchas gracias a todos por su participación.

[FIN DE LA TRANSCRIPCIÓN]