SAN JUAN – Actualización sobre el traspaso de la KSK
Miércoles, 14 de marzo de 2018 – 16:15 a 16:45 AST
ICANN61 | San Juan, Puerto Rico

ORADOR DESCONOCIDO: Hola a todos. Vamos a comenzar con la sesión de traspaso de la KSK en breve. ¿Podríamos poner las presentaciones en pantalla, por favor?

Vamos a comenzar en 30 segundos.

Buenas tardes a todos. Esta es una sesión de actualización sobre el traspaso de la KSK. Espero que haya algunas personas que no me hayan visto dar esta presentación durante esta conferencia de la ICANN. Espero, por lo menos. Voy a empezar con un resumen de cómo llegamos a la situación actual. Creo que todo el mundo sabe, si les interesa el tema como para estar en esta sala, que el traspaso de la KSK iba a tener lugar el 11 de octubre de 2017 pero decidimos posponerlo.

Verisign analizó los datos de RFC 8145 y encontraron que el 7-8% de los resolutores que están informando, sabemos que es un número pequeño en este momento, solo tenían lo que llamamos la KSK de 2010. No tenían la nueva KSK. Había algo que no estaba bien con ese 7-8%. La oficina del director de tecnología de la ICANN repitió ese análisis con información diferente de los

***Nota: El contenido de este documento es producto resultante de la transcripción de un archivo de audio a un archivo de texto. Si bien la transcripción es fiel al audio en su mayor proporción, en algunos casos puede hallarse incompleta o inexacta por falta de fidelidad del audio, como también puede haber sido corregida gramaticalmente para mejorar la calidad y comprensión del texto. Esta transcripción es proporcionada como material adicional al archive, pero no debe ser considerada como registro autoritativo.***

servidores raíz y encontraron más o menos lo mismo. Según el momento en que miramos el porcentaje es más alto o más bajo.

Hay un porcentaje más alto del que esperábamos. No sabíamos por qué, no entendíamos por qué esos resolutores todavía informaban con la clave anterior. Decidimos pausar el traspaso y tratar de definir por qué esos resolutores no tenían la nueva KSK. Tomamos una lista de 500 resolutores que en el mes de septiembre de 2017 habían informado de que estaban con la clave anterior. Es decir, la KSK 2010. Tratamos de encontrarlos y nos dimos cuenta de que tratar de encontrar a los operadores basándonos solo en la dirección de IP es muy difícil. Ya lo sabíamos pero esto es una prueba claro de eso.

Solo pudimos ponernos en contacto con el 20%, 100 direcciones. De ellas, la mayoría estaban en rangos que tenían elementos efímeros como máquinas virtuales. También el RFC 8145 dice que la señal se manda como una consulta de DNS. Iba siendo enviada de un resolutor al próximo. Sabíamos que se iban derivando las consultas. Quizá una máquina tuviera solamente la KSK 2010.

Aquí la ventaja es que no había una sola causa, que hubiera sido lo ideal. Si hubiera habido una o dos causas raíz, podríamos haber hablado con los proveedores para que resuelvan los problemas que encontraron y hubiéramos mejorado nuestro

mensaje de comunicación pero eso no es lo que pasó. Sin un claro camino para avanzar, la investigación no dijo nada. El equipo de investigación pidió comentarios a la comunidad. Llegamos a fines de diciembre de 2017 y dijimos que íbamos a aceptar comentarios e íbamos a hablar en una página especial de la ICANN que está abierta para debatir este tema. Si no están en esta lista todavía, anótense. Tiene muy poco volumen en este momento pero vamos a ir actualizándolo con este proyecto.

Los resultados de este intercambio de ideas. Hay acuerdos generales de que no hubo una buena medición en este caso. El equipo de diseño que reunió la ICANN y que ahora ya hace dos años que presentaron el informe sobre el traspaso de la KSK hizo recomendaciones. Pensaron que una buena medida sería conocer la cantidad de usuarios afectados. La mitad de un 1% de usuarios afectados después del traspaso sería una indicación de que había una importante de problemas. La cantidad de usuarios es una medición razonable pero algo difícil de medir.

La RFC 8145 no nos daba estos datos. La idea es que se iban a hacer mediciones mejores en el futuro y se buscaba algo que ahora llamamos Sentinel, que es un documento que preparó Warren Kumari de Google y que la gente de APNIC está utilizando para hacer mediciones. Todavía no lo tenemos hoy. El consenso en ese grupo fue que la ICANN debería hacer el traspaso de la

clave en forma oportuna y que debía seguir comunicando esto como lo hemos hecho externamente.

Eso nos llevó al 1 de febrero, donde publicamos un plan preliminar. Quiero decir que es un plan preliminar para el traspaso de la KSK. Los componentes de ese plan fueron los siguientes. Primero íbamos a posponer el traspaso un año. Vamos a hacer el traspaso el 11 de octubre de 2018. Esperamos que de esta lista surgieran criterios para medir pero hasta ahora nadie sugirió ningún criterio en especial. También íbamos a seguir con las actividades de difusión externa, difusión como esta, reunión que íbamos a publicar y publicitar el traspaso de la KSK. También íbamos a publicar instantáneas mensuales de los datos del informe del anclaje de confianza según RFC 8145. La idea era ver los comentarios públicos para que nos fueran diciendo si esto era un proyecto importante o no.

Lo importante es que tenemos un periodo de comentarios públicos abierto. Ahora tenemos solamente un documento preliminar que está abierto porque queremos recibir los comentarios de la comunidad respecto de esta propuesta. Este periodo de comentario público termina el 2 de abril. Aquí está la URL de la página donde se explica todo. Está abajo de todo, en la diapositiva que tenemos en pantalla.

Si seguimos adelante con el plan, el cronograma es el que vemos aquí en el plan preliminar y sería más o menos como esto. El 2 de abril se cierra el periodo de comentarios públicos. A mediados de abril el personal debe publicar su informe. También revisaremos el plan según fuera necesario y lo publicaremos. Si ustedes no conocen la cadencia de las reuniones de la junta directiva de la ICANN, la junta se reúne seis veces por año. En cada reunión pública de la ICANN, tres veces. Además, entre reuniones públicas de la ICANN tiene talleres intermedios. La próxima reunión de la junta directiva de la ICANN será en mayo. Es un taller y en ese momento le pediremos a la junta que presente una resolución pidiéndole a SSAC y también a RSSAC… No actualicé estas diapositivas. SSAC y RSSAC que revisen el plan, que presenten sus comentarios antes del 1 de octubre.

Seguramente tendremos otra sesión en Panamá para hablar sobre el traspaso de la KSK. El 1 de agosto esperamos haber recibido los comentarios de RSSAC y SSAC. Si no hace falta cambiar la fecha según las revisiones, a mediados de agosto habremos publicado el plan final y en el workshop de septiembre le pediremos a la junta directiva que presente un documento pidiéndole al personal que haga el traspaso el 11 de octubre. Es lo que tenemos por ahora. Quiero subrayar una y otra vez que realmente esperamos recibir los comentarios y

aportes de la comunidad a través del periodo de comentarios públicos.

El resto de mi presentación voy a hablar sobre las señales que estamos recibiendo a través de estos informes de anclaje de confianza RFC 8145. En este momento, la oficina del director de tecnología tiene acceso a los datos del RFC 8145. En realidad, esta diapositiva ahora está un poco desactualizada porque ya tenemos información de 12 servidores raíz más. Ya agregamos el H a la lista de servidores que nos están dando datos.

El análisis inicial a fines de 2017 utilizó datos pickup de B, D y F pero desde entonces hemos estado utilizando un excelente plugin para DNS cap. Los operadores raíz utilizan DNS cap y esto analiza el tráfico en tiempo real, cada 60 segundos. Este plugin prepara un informe de estadísticas y también los informes de anclaje de confianza que ha visto, los envía como consulta al DNS, lo que es muy inteligente, a una zona que opera la ICANN.

Pueden ver ejemplos de cómo son esos informes. Tienen fecha, tienen el IP fuente. Se utilizan guiones en lugar de puntos. Hay anclajes de confianza que se utilizan. Aquí los pueden ver en la pantalla. Fíjense. Incluye el ID de nodo y el ID del servidor raíz. Con todo esto, podemos compilar este tipo de gráficos. A media que pasa el tiempo, cada vez recibimos más informes de

servidores adicionales. Se lo voy a explicar porque no se entiende claramente a primera vista.

Las tres líneas representan dos cosas diferentes. Las líneas rojas y verdes representan la cantidad de IP que están informando datos según 8145. Los pueden ver en el eje de la izquierda, la cantidad de fuentes. Pueden ver el transcurso del tiempo. Pueden ver la línea verde, por ejemplo. Ese es el número total de fuentes que informan datos de anclaje de confianza. Estas son fuentes únicas por día. Es decir, en este momento 50.000 direcciones de IP únicas están informando datos de anclaje de confianza diariamente. La línea roja son los que están informando que solo tienen la clave antigua. Si dividimos la línea roja por la verde, obtenemos el porcentaje. El porcentaje es la línea negra. Esta escala hay que leerla utilizando el eje de la derecha. Ahora vemos que estamos en un 20% de resolutores que tienen datos que solamente utilizan la clave anterior.

Fíjense que hay un crecimiento importante a mediados de enero, donde muchos empezaron a informar. El porcentaje empeoró. Creemos que esto se debe a un upgrade que se hizo en Unbound. Unbound 168 se hizo a mediados de enero y creemos que ese Unbound se introdujo por una vulnerabilidad. Como se trataba de un patch de vulnerabilidad, todos los usuarios hicieron un upgrade. Pusieron ese parche pero no cayó la KSK después de que pasó el periodo de implementación.

Voy a explicarlo de otra manera. Si alguien hace un upgrade de Unbound y utiliza la herramienta Unbound inmediatamente va a actualizar el depósito de anclaje de confianza con lo que debe hacer. Inmediatamente, la KSK de 2010 y de 2020. Muchos, si no hacen bien la implementación, tienen el Unbound y siguen utilizando la KSK anterior, pero si hacen las cosas correctamente, habrán incluido la KSK 2017. Pero no pasó en algunos casos. Una hipótesis sería que estas son máquinas virtuales o contenedores efímeros así que si uno empieza a operar, informa la clave anterior según 8145. Deberíamos decir KSK 2010. Informa KSK 2010, opera un par de días, un par de horas, después se desconecta. Nunca tiene tiempo de completar todo lo exigido y la próxima vez que vuelva a operar, sigue informando solamente la KSK 2010. Tenemos que analizar un poco más esto pero yo no pude seguir preparando las diapositivas. Tuvimos que venir a Puerto Rico a compartirlas.

Ahora estamos analizando las IP, con qué frecuencia se presentan, con qué frecuencia informan información. Sabemos que Unbound y Bind presentan estos informes sobre 8145 de manera frecuente. Tenemos IP que no lo están haciendo. Un supuesto razonable sería que son efímeros, que operan y dejan de operar. Esa no es la única razón posiblemente pero es una razón posible. Lo estamos investigando.

Aquí tenemos gráficos de servidores raíz individuales. Este gráfico era para todos los servidores raíz. Este que vemos aquí es para los servidores de los cuales tenemos datos. Pueden ver que los datos vienen de diferentes servidores y de diferentes momentos. Si ven los gráficos, son bastante parecidos, con la excepción de la raíz J. La raíz J se ve mejor que las demás. Por lo menos en términos porcentuales pero no recibimos informes de todas las instancias de la raíz J. Quizá eso explique lo que vemos.

En general, los diferentes servidores raíz informan datos similares. Lo que creo que sí es interesante es el cambio en conducta que se vio a mediados de enero cuando vimos ese crecimiento. Ese gráfico muestra direcciones de IP únicas que se van agregando día tras día. Aquí vemos que en ese día, en enero, la cantidad de fuentes que nos están informando, datos que nunca vimos antes. Si lo ven de izquierda a derecha, nunca teníamos más de unos cientos de direcciones IP nuevas cada día. Después del evento de upgrade que creemos que tuvo lugar en enero, hay muchas más fuentes únicas que están presentando informes diariamente. Alrededor de 15.000 o 16.000.

Si representamos un gráfico con la cantidad de IP únicas que se acumulan diariamente, veríamos esto. La línea verde muestra en momentos determinados cuántas direcciones de IP únicas vemos. Obviamente, el número empieza pequeño a la izquierda de manera que pasa el tiempo y más direcciones de IP únicas

estamos viendo. Hoy en día estamos 730.000 aproximadamente. A la fecha, tenemos 730.000 IP diferentes. Esto es una combinación de IPv4 e IPv6. 730.000 han informado datos. De estos, aproximadamente 250.000 en un momento u otro informaron que solo tenían la KSK 2010.

El cálculo aquí, si vemos los números totales, la situación actual es aun peor. Un 35% del total de direcciones que estamos viendo informan solo la KSK 2010. Yo decidí ver esto por /24. Aquí pueden ver cómo es este gráfico que es un poco diferente. Hay un pico después del aumento de enero y después decayó un poco. Si vemos el total, vemos que todavía hay muchas /24. Miren la línea verde, que va cayendo más adelante. Esto sería un promedio de dos IP por /24. Yo pensé que este número iba a ser más pequeño. Esto indicaría que hay bloques que tienen un montón de direcciones y podemos investigar esos bloques y quizá sean cajas de direcciones que son máquinas dinámicas efímeras. Esas son muchísimas direcciones.

Lo interesante es que el número total de direcciones que informan la KSK 2010 o la 2010 y la 2017 es números mayor que el número total de IP únicas. Esto significa que hay fuentes que han informado la KSK 2010 y después informaron que tienen la 2017, no necesariamente en ese orden pero presentaron ambos informes. Esto quizá se explique por lo siguiente. Imaginen que una fuente informa que tiene la KSK 2010 y después, más

adelante, informa la 2010 y la 2017. Una razón, pero no la única posible, es que quizá ese equipo recibió un upgrade y ahora tiene la nueva KSK pero de estas 750.000 IP solamente 1.550 informan ambas claves. Es decir, que no hay muchos equipos que puedan apoyar esta hipótesis.

El tema es que hay un problema con la señal 8145. Sabemos que el hecho de que veamos un informe de una IP fuente, no tenemos garantía de que esta configuración no se venga de ese IP. Puede ser que otro equipo esté mandando su 8145 a esa dirección de IP que después la envía a un servidor raíz y ahí la vemos. Otra explicación que nos muestra por qué quizá haya una sola fuente informando que tiene KSK 2010 y 2017. Además, hay una implementación que informó la 8145 aunque no estaba validando. Si tuviera KSK 2010, no era importante porque no hacía validación DNS. Estaba configurada pero no importaba.

Si quieren estos gráficos para ustedes, los actualizamos semanalmente. Esta es la URL que tienen: roottrustanchorreports.icann.org. Empecé a analizar los datos de esta manera. Esta tabla no está basada en los 250.000 IP que han informado sobre la KSK 2010. Son menos los que tenemos en esta pantalla. No recuerdo cuál es el número total pero aquí consideramos la cantidad de fuentes por sistema de números autónomos. Después hacer una clasificación reversa. No, me corrijo. Esto no habla de KSK 2010. Estos son todos los números

de sistema autónomo informando. Tengo que correrlo otra vez viendo la KSK 2010. Así podremos intentar averiguar qué está pasando con las fuentes que tienen la mayor cantidad de resolutores apuntando a KSK 2010.

Distribuimos una lista de direcciones IP que reportan solamente la KSK 2010 al ISPCP y a los RIR. El objetivo es doble. Por un lado, actualizar esos sistemas y, además, estamos muy interesados en saber qué es lo que está ocurriendo y por qué los sistemas no se están actualizando. Uno de los mejores resultados sería encontrar que de hecho tenemos un espacio de direcciones donde hay muchas máquinas con la configuración de KSK 2010. Eso sería un hallazgo positivo. Esta diapositiva está desactualizada. Ahora tengo la autorización de la ICANN para poner la lista a disposición del público. La vamos a ajustar un poco, a afinar un poco. Se va a parecer a esta. Ustedes van a poder hacer clic sobre el ASN y van a tener todas estas direcciones que informan un KSK 2010. Va a ser mucho más fácil para un operador saber qué es lo que está pasando en su red. Obviamente, después vamos a conectarnos con los operadores empezando con los que tienen la mayor parte de informes de KSK 2010 para entender qué es lo que está ocurriendo.

Los próximos pasos. Tratar de seguir investigando en lo que está ocurriendo con los datos de 8145. No estoy satisfecho con la señal que nos da pero por el momento son los únicos datos que

tenemos. Lo más responsable que podemos hacer es seguir investigando para entender qué es lo que nos dice. Si llegamos al punto en que estamos convencidos de que realmente no nos dice nada valioso, eso en sí mismo también será un hallazgo positivo.

Como dije, vamos a tratar de contactarnos con las redes que informan grandes cantidades de resolutores con KSK 2010. Vamos a ayudar a otros a que hagan esto, a otros que están investigando estas fuentes. Vamos a seguir publicitando esto, tanto mis colegas como yo. Queremos seguir escuchando a la comunidad porque, como dije, ustedes pueden ayudarnos haciendo comentarios sobre el plan. Por favor, suscríbanse a la lista de KSK rollover para seguir actualizados. Hagan comentarios también sobre el plan. Esto es todo por el momento.

HOWARD BENN: Soy Howard Benn, de Samsung Electronics. Con respecto a esa diapositiva que usted mostró con todos los operadores, entiendo que aquí seguramente es la red LTE que se ejecuta totalmente con máquinas virtuales. Seguramente nunca llegará al límite de los 30 días. Sería interesante ver una versión de los operadores móviles para ver si todos enfrentan los mismos

problemas. Si quiere, puedo darle información de contacto porque ese equipo es nuestro.

ORADOR DESCONOCIDO: Gracias.

MARK MCFADDEN: Hola. Mark McFadden, de ISP, pero hablo a título personal. ¿Podría ir a la diapositiva número cuatro, por favor? Esta. Estoy viendo la parte inferior de la diapositiva donde dice: "Resultados de los debates" y los puntos uno y tres. Los voy a poner con mis propias palabras. Dígame si estoy equivocado. El primer punto dice que no sabemos cuál será el efecto de esto sobre Internet. El tercer punto dice: "Háganlo de todas formas". ¿Estoy equivocado?

ORADOR DESCONOCIDO: Esa sería la interpretación de ver el vaso medio vacío.

MARK MCFADDEN: ¿Podría decirme cuál es la interpretación del vaso medio lleno?

ORADOR DESCONOCIDO: Creo que el resto de la presentación es el vaso medio lleno. Le voy a dar una respuesta en serio. La respuesta en serio es que es

difícil saber qué hacer. Cuando llegamos al punto en el que estamos en el otoño, decidimos que teníamos que involucrar a la comunidad y recibir el aporte de la comunidad. El resumen que usted dio es lo que dijo a la comunidad. Debo señalar que en general las personas que están en el traspaso de la KSK son personas que apoyan DNSSEC y tienen capital personal y no sé qué más. Invirtieron en DNSSEC y quieren que ocurra la rollover. Mirando hacia atrás, no es sorprendente que hayamos llegado a esto pero por eso los comentarios públicos son tan importantes, para poder mostrarle esto a un público más amplio y para que aquellos que tienen la interpretación del vaso medio vacío puedan entender.

MARK MCFADDEN: Sigo teniendo la perspectiva del vaso medio vacío. Yo apoyo DNSSEC y voy a hacer comentarios individuales sobre esto. No puedo superar los puntos uno y tres. Me parece que hay una disonancia cognitiva. Alguien propone introducir un cambio en la raíz y no sabemos cuál será el efecto. Estoy de acuerdo con usted y confío totalmente en su análisis de la mala señal de las señales que ustedes reciben pero a medida que pasan los días, las señales que recibimos, que es la única información de diagnóstico que ustedes tienen, la señal va empeorando solamente. Una vez más, esa es mi descripción de la situación.

A mí me parece que esta diapositiva, todas las diapositivas posteriores son muy atractivas pero esta, con los puntos uno y tres y el resultado de los debates son cosas que no entiendo. No conozco a nadie en la comunidad técnica que diga: "Sí, adelante. Continúen con el cambio en la raíz cuando en realidad no sabemos cuál va a ser el resultado". Gracias. Voy a hacer esos comentarios también a modo individual.

ORADOR DESCONOCIDO: Quisiera explicarle cuál podría ser otra interpretación. No es mi interpretación. Solamente estoy repitiendo lo que escuché. También está el potencial de no hacer el traspaso de la llave. Esto podría reducir la confianza y podría generar una amenaza a la seguridad física, a la seguridad operativa. De todas formas, no hacer el traspaso podría afectar la confianza en la llave. Si combinamos esto con la idea de que no va a ser tan malo, de que se puede reparar rápidamente y aceptamos que va a haber algunos problemas, entonces eso es lo que lleva a pensar que sí hay que hacer el traspaso de la llave.

MARK MCFADDEN: El argumento en torno a la reputación es: "Vamos a hacer el traspaso porque queremos que la gente confíe en DNSSEC". Entiendo la parte que tiene que ver con la reputación. Por otra parte, si la gente hace deducciones equivocadas, y me sorprende

que hagan deducciones, entonces es peor que lo que yo pensé que iba a ser y tenemos que hacer quizá un traspaso hacia atrás. Me parece que tenemos un problema que afecta a la reputación de ambas formas. Eso pone a la ICANN en una situación difícil si se consiente eso. No estoy tan convencido de que el tema de reputación que afecta a DNSSEC sea el mismo que el de una implementación desconocida o con interrogantes que se hará en octubre.

ORADOR DESCONOCIDO: Gracias. ¿Alguna otra pregunta o comentario? Cathy, ¿hay algo que venga de la conexión remota?

ORADOR DESCONOCIDO: No.

ORADOR DESCONOCIDO: Gracias por la presentación. Mi pregunta es la siguiente. En Nigeria tenemos cuatro operadores de redes móviles y una gran cantidad de ISP. Vimos que solo una de los cuatro operadores tiene DNSSEC. Los otros tres operadores de telefonía celular tienen otro sistema de validación que no es DNSSEC. Mi primera pregunta es qué ventaja tiene DNSSEC con respecto a los otros sistemas de validación de seguridad. ¿Es necesario que los otros tres operadores migren a DNSSEC? La última pregunta es la

siguiente. ¿Los otros proveedores de servicios de red que utilizan otros sistemas de validación deberían actualizar el traspaso?

ORADOR DESCONOCIDO: ¿Podría repetir la última parte de la pregunta, por favor?

ORADOR DESCONOCIDO: La última parte de la pregunta es que tres de los operadores de servicios de red no utilizan el sistema de validación de DNSSEC. ¿Qué pasará con el traspaso de la KSK?

ORADOR DESCONOCIDO: Perdón, ¿cuál es el...?

ORADOR DESCONOCIDO: El efecto. ¿Habrá algún impacto?

ORADOR DESCONOCIDO: Esa pregunta es fácil. Si no están haciendo validación con DNSSEC, entonces con el traspaso de la KSK no tendrá ningún impacto. La posición de ICANN org es que la validación con DNSSEC es algo bueno. Sería bueno que usted aliente a las empresas a hacer validación con DNSSEC. Perdón, ahora no recuerdo la primera parte de su pregunta.

ORADOR DESCONOCIDO: ¿Hay alguna ventaja para aquellos que no están haciendo DNSSEC para que migren a DNSSEC?

ORADOR DESCONOCIDO: Es lo que acabo de decir. La posición de ICANN org es que sí debe hacerse la validación con DNSSEC porque sin esta validación no tenemos garantías de que la respuesta que usted reciba realmente esté respondiendo a la pregunta que usted hizo y que provenga de quien usted piensa que proviene. No tenemos una garantía criptográfica de que las respuestas que usted recibe realmente vengan de donde usted cree que vienen. Tenemos que hacer DNSSEC para asegurarnos de que la respuesta viene de quien dice que viene. Los resolutores modernos hoy en día son muy inteligentes y saben cómo evitar que los rastreen pero hoy en día, para tener un alto nivel de seguridad hay que tener DNSSEC. Sin DNSSEC somos más vulnerables a respuestas fraudulentas que no son correctas.

ORADOR DESCONOCIDO: Muchas gracias.

ORADOR DESCONOCIDO: ¿Hay alguna otra pregunta? Bueno, muchas gracias por haber venido entonces.

**[FIN DE LA TRANSCRIPCIÓN]**