BARCELONA – Taller sobre las DNSSEC (2 de 3)
Miércoles, 24 de octubre de 2018 – 10:30 a 12:00 CEST
ICANN63 | Barcelona, España

JACQUES LATOUR: Vamos a comenzar rápidamente. Buenos días. Soy Jacques Latour, de CIRA. Steve Crocker está al teléfono. Vamos a moderar este panel. El objetivo de este panel es continuar la discusión que tuvimos en Johannesburgo, en la reunión ICANN59. Hubo una reunión de política y en el taller del DNSSEC analizamos el impacto de política del CDS, CDNSKEY y el CSYNC. ¿Por qué? Porque en ese momento que fue el año pasado fue cuando comenzamos a evaluar esta idea de escanear toda la zona, tomar los CDS, importarlos al registro y todos dijeron, o muchos dijeron: "Eso no se puede hacer porque viola las políticas de la ICANN". Esa fue la razón principal cuando preguntamos por qué. Cuando preguntamos cuáles son las políticas que se estaban violando, nadie sabía.

Después de esta reunión comenzamos a investigar cuáles eran estas políticas que podrían ser impactadas, si había alguna política de DNSSEC. En el acuerdo con el registro, el acuerdo básico con los registros se dice que los operadores pueden operar materiales de DNSSEC de acuerdo con las prácticas de la industria. Es decir, es el método a cumplir. En cuanto a la violación de políticas, el acuerdo con el registro no contiene ninguna disposición que impida que se obtenga el DS directamente del hijo. En el RAA, el acuerdo de acreditación de registrador de 2013 dice que el registrador procesará la información de

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 hallarseincompleta 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.

DNSSEC, transmitiendo órdenes de añadir, remover o cambiar información. Es decir, retransmitir información. Ni almacenar, ni procesar ni capturar. En tal sentido llegamos al acuerdo que no existiría violación del acuerdo porque hay una prescripción exacta de lo que hay que hacer.

Ahora, como no hay violaciones, estamos evaluando múltiples opciones. Steve nos va a contar dónde nos encontramos, cuáles son las opciones a futuro. Steve.

RUSS MUNDY: Steve, ¿nos puede oír?

STEVE CROCKER: Gracias. Gracias, Jacques y a todos los otros panelistas. Mi preocupación es que de alguna manera las cosas funcionen. Veo muchas iniciativas respecto del abordaje con el CDS y el CDNSKEY. Cualquiera estaría bien para mí en tanto funcione pero todavía no he visto un acuerdo y una aceptación generalizada respecto de los registros de gTLD y los registradores entre ellos. Considerando los distintos enfoques me parece que todos pueden categorizarse en tres opciones bastante binarias. ¿Podríamos ver la siguiente diapositiva, por favor?

ORADOR DESCONOCIDO: Parece ser que tenemos algún problema. Estamos teniendo un inconveniente con Adobe, Steve. Adelante. Trataremos de resolver la situación.

STEVE CROCKER: Voy a ver con la presentación frente a mí. Es básico. Con CDS y CDNSKEY y su publicación se espera que los registros y los registradores hagan una extracción de los registros. Ese es el modelo pull. Los registros nuevos, la otra opción, es empujarlos al subirlos a algún tipo de interfaz X. Esa es una opción binaria. La segunda opción binaria es bastante obvia. Comunicar los registros DS y el registro se computa sobre la base de esa clave y la tercera opción binaria es si el rol del padre es asumido por el registro o quizá por el registrador. Aquí podríamos imaginarnos a los registradores escaneando la zona y no el registro. El registrador utilizaría una interfaz para empujar la clave al registro. Ahí veo las diapositivas. Avancemos rápidamente a la siguiente. Todavía no llegamos ahí.

Estas son las tres opciones. Todas las opciones van a funcionar. Se puede hacer incluso más de una. Vi que SWITHC funciona bien tanto en pull como en push. Probablemente optaría por el tipo push. Optaríamos todos, si es que han seguido lo que dije. La siguiente diapositiva. ¿Quién es el que elige? Ese es un tema de discusión. La siguiente.

Esto es lo que yo dije a los presentadores del panel. No queda claro qué partes tenemos que hacer nosotros y qué partes corresponden a otros. Hubo una pregunta que estaba pendiente, si existía algún

impedimento en lo político o en lo contractual y, si existe tal impedimento, qué es lo que impacta, cómo resolverlo. Si debemos ser explícitos acerca de los operadores y de la información del WHOIS, sé que es una idea terrible de la que la gente no quiere ni hablar pero tenemos que abordar los problemas que existan. Con esto le devuelvo la palabra a Jacques.

JACQUES LATOUR: Hemos recuperado las diapositivas recién ahora Steve. Cathy, ¿podemos volver a la diapositiva número tres, cuando muestra las tres opciones? Creo que es importante que la gente las vea. ¿Le parece que las repasemos con el texto ahora en pantalla para que la gente las comprenda bien? Steve, ¿podría cubrir nuevamente las tres opciones brevemente? Porque esto es lo esencial que tenemos que conversar. El dilema es si vamos por push o pull. KSK versus DS. Que el padre sea el registro o el registrador. La situación ideal es que no tuviéramos que elegir, que la industria nos marcara el camino a seguir.

MICHAEL HAUSDING: Hasta ahora hemos tenido el modelo push pero ha planteado dificultades. Pensamos que el modelo pull es más sencillo pero tenemos push disponible y daríamos prioridad a pull. Habría que cambiar algo en la zona del padre. Tengo las diapositivas. Si quieren muestro mis diapositivas. Soy el que sigue en la agenda. Estoy más adelante. Voy a hablar sobre esto.

JACQUES LATOUR: La próxima es Vicky Shrestha, de Cloudflare.

VICKY SHRESTHA: Buenos días. Podemos ir a la siguiente. Yo trabajo en Cloudflare en DNS y manejamos una red global. Hacemos mucho DNS iterativo y manejamos el resolutor de DNS de validación. La siguiente. En esta presentación hablaré del trabajo con DNSSEC que hemos hecho hasta ahora. Lo habilitamos para todos los clientes en 2015. Utilizamos DNSSEC y CDNSKEY desde el principio. Vimos que muchos clientes intentaron habilitar DNSSEC pero el problema es que no hicieron un seguimiento. Habilitan DNSSEC en el portal corporativo y lo dejan ahí. Es decir, no van al registrador, no leen la información del registro ni actualizan el DNSSEC. Ese ha sido el problema. La siguiente.

No hemos tenido un índice de éxito muy bueno que digamos. Esta gráfica muestra distintos TLD según el número de zonas operadas para los clientes y el porcentaje que ha completado la cadena de confianza es bastante bajo. La siguiente.

Hay múltiples problemas que lo causan. Gran parte de los UI pueden no ser sencillos de usar, las interfaces de usuario. Los clientes quizá no entienden cómo subir el DS bien. También puede haber problemas de conocimientos técnicos que la gente no puede seguir. Hubo problemas con falta de soporte del algoritmo por parte del registrador o el registro, el algoritmo 13. También está el problema de que el cliente tenga miedo de que su zona se rompa, se fracture. La siguiente.

Lo que ahora estamos haciendo es hacer CDS y CDNSKEY para todas las zonas con DNSSEC. Pensamos que esto va a permitir que la automatización sea más fácil para los clientes. Lo único que tiene que hacer el cliente es habilitar DNSSEC en el portal y CDS y CDNSKEY se habilita a través del registro padre que desea la zona hija con todos los detalles. La parte técnica está toda automatizada. La siguiente.

Como decía, el cliente habilita DNSSEC, CDS y CDNSKEY se publican en el borde y el padre tiene que hacer un escaneo regular de la zona hija y también podemos añadir verificación y notificación en el lado del cliente. Quizá un periodo de 24 horas de retención, dependiendo de lo que decida el TLD y hacer cambios de DNS. Asegurarnos de que el escaneo sea regular para que el CDS0 sea capturado rápidamente, la CDNSKEY0. Esto es lo mismo que acabo de decir. La próxima.

En este momento tenemos un par de TLD: .CZ, .LI, .CH, .CR que soportan la CDNSKEY y que automáticamente instalan el DS. También trabajamos con el registrador Gandi. Han sido muy colaborativos. Estamos hablando con otros registradores también. La próxima. Lo que nosotros estamos procurando es que todos los operadores del DNS hagan esto por omisión, comiencen a hacerlo. También que DNSSEC sea por default. Esperamos que a través del software que usamos esto se logre. La siguiente. Eso es todo de mi parte. Gracias.

JACQUES LATOUR: Gracias. Ahora tenemos a Ondrej Filip, de CZNIC, quien nos va a contar un poquito sobre la administración automatizada de las claves.

ONDREJ FILIP: Yo soy del dominio .CZ. Quiero hablar de cómo manejar estos temas. La próxima diapositiva. Tenemos un muy buen porcentaje de dominios firmados pero queremos entender un poquito más y no tener que ir a todos los usuarios individuales habilitando esta característica. Sabemos que hay unos 29.000 dominios firmados pero la clave no se publicó o no está en la base de datos. Asumimos que hubo algún problema e identificamos varios problemas. Aun cuando intentamos educar a los registradores, a veces el soporte no es el óptimo. Algunos son perfectos. Andan muy bien. Pero hay otros que no están en una situación de poder ayudar a los clientes a firmar los dominios. Aquellos que se supone que soportan DNSSEC sus titulares no los pueden manejar, no pueden transferir los materiales de la clave del proveedor al registrador y tampoco hay una relación directa con el registro.

Por último, algunos quizá recordarán esa época de la configuración de la zona donde el servicio del nombre se presenta en la zona y uno se olvida. Hay que volver a esto pero con las zonas firmadas con DNSSEC, por supuesto. Para eso hay que cambiar dos cosas. La siguiente diapositiva.

Primero, la implementación de Knot DNS. Implementamos esta característica de Knot DNS y ahora, si se hace de manera automatizada, se empieza a firmar periódicamente la zona raíz también puede publicar los registros CDS o CDNSKEY. Ahí espera al padre. Periódicamente va chequeando los servidores de nombre a ver si existen registros DS. Si aparecen esos registros, ahí termina la

implementación de la clave. Incluso así el algoritmo se puede implementar muy rápidamente a través del servidor de nombres autorizados o resolutores de validación DNSSEC. Es opcional pero hay que asegurar que la cadena se complete. La siguiente diapositiva.

También respaldamos la firma de la llave simple para algunos dominios. También soportamos shared key para más dominios, firma compartida. También se puede hacer así la implementación del algoritmo. Si queremos remover la llave tenemos que hacer una delegación de CDNSKEY de una forma manual. Esta es la versión 2.6 y creo que ya estamos llegando a la 2.73.

La otra parte es el registro. Antes de empezar con la implementación iniciamos la discusión con los registradores y les mostramos tres opciones posibles. O bien no lo implementan o lo implementa a nivel del registrador o lo implementa a nivel de registro. Es sorprendente que esas personas decidieron que si nosotros los implementamos no tenemos que hacer nada. Por lo tanto, nosotros aceptamos el rol y dijimos que vamos a verificar. Decidimos chequear el CDNSKEY en todos los dominios que están en la zona .CZ y así fue como creamos los registros. Utilizamos el modelo pull y esta característica fue implementada en el 2.32. Siguiente. Perdón, veo que no estaba sincronizad con las diapositivas. Siguiente.

Esto fue la implementación en el registro. Vamos a la siguiente. ¿Qué es lo que hacemos? Nosotros todos los días escaneamos todos los dominios en la zona, que nos toma unas tres horas para el .CZ. Tratamos de encontrar records CDNS. Hay tres categorías de dominios.

Dominios sin keys. Luego tenemos que tener algunas reglas. Escaneamos el dominio durante los próximos siete días y si no hay ningún cambio ahí creemos que el registro CDNSKEY está bien y creamos el DS.

Luego tenemos otro tipo de dominios y si hay algún cambio inmediatamente cambiamos a DS en la zona y así continuamos. También hay algunos dominios que tienen records DS ya hechos por registradores manualmente y cuando la información está completa y toda la cadena vuelve a aparecer, volvemos a tener problemas en la base de datos.

Aquí hay algunas estadísticas de nuevo. Comparado con el número de dominios firmados en .CZ es muy pequeño, es un porcentaje del 0,2%. Estamos en alrededor de los 1.700 comparados con los 700.000 dominios firmados en .CZ. Es bueno poder ayudar a esta gente. Siguiente diapositiva.

FRED no solamente es utilizado por nosotros sino también por muchos otros países en el mundo. La buen anoticia es que hay otros países que decidieron seguir nuestros pasos y Costa Rica fue el tercer registro que lo implementó, esta gestión de key set automatizado.

¿Cuáles son nuestros próximos planes? Nosotros estamos modificando un poco el sistema para que haya más locaciones para el escaneado. Estamos haciendo que sea más seguro. Todavía estamos viendo cómo informar a los propietarios de los dominios porque lo que les enviamos a veces es confuso. Debemos hacer algo con eso. También estamos considerando la implementación del modelo push pero estamos por

ahora esperando a que esté listo. No sé muy bien cuándo va a suceder eso.

También hablamos con proveedores de DNS. Creo que el impulso vino de Cloudflare. Pusimos una nueva herramienta. Otro tema que no se cubrió es que hubo una presentación interesante en la última reunión. Fue una presentación hecha por Ondrej Caletka. No es alguien que ustedes conozcan pero es de la República Checa. Él hablaba sobre el DNS inverso. Es un sistema para revertir el DNS también, porque el DNS puede usarse no solamente para traducir nombres a números sino que también se puede usar en orden inverso y tener ese sistema en una base de datos o en la zona inversa sería muy adecuado. Esto es algo que quizá podamos tener en cuenta para la próxima vez. Vamos a la siguiente diapositiva. Eso es todo lo que tengo que decirles. Gracias.

JACQUES LATOUR: Gracias, Ondrej. El siguiente es Michael, de SWITCH. Nos va a hablar sobre la automatización del DNSSEC con CDS.

MICHAEL HAUSDING: Muy bien. Muchas gracias, Jacques. Muchas gracias, Ondrej. Lo acabamos de encender hace dos semanas. Tenemos los primeros nombres de dominio que están puestos en la zona .CH. Mañana vamos a hablar con CZNIC y vamos a ver cuál va a ser el impacto. Seguramente voy a hablar sobre cuál fue la motivación y cuál es nuestra experiencia hasta ahora.

Primero, la adopción de DNSSEC está creciendo en Suiza. De todos modos, debemos hacer cosas para promoverlo. Hablamos con algunos de los registradores respecto de por qué no implementan DNSSEC y hay dos respuestas. Una es que tienen un sistema de registro que a veces no es capaz de automatizar DNSSEC, lo cual requeriría mucha implementación. Lo segundo es que tienen temor de qué es lo que va a suceder con la implementación de la llave. Si miran lo que sucedió antes, hay un registrador que generó una llave en su servidor de nombre. La clave luego se coloca en el registro. El registratario recibe la llave del servidor de nombre y la tiene que cargar al registrador a través de una interfaz web o a veces incluso por email. El registrador luego lo coloca en el registro a través del EPP. Algunos registradores, por ejemplo, solamente lo pueden hacer a través de email en días hábiles. Por lo tanto, si hubo un error hay que esperar hasta que el registrador esté de nuevo en la oficina el lunes.

Después de que activemos el CDS, es mucho más fácil. Solo hay que habilitar la firma en el servidor de nombre, que no es la parte difícil. Por lo menos eso es lo que nosotros pensamos. El registro puede recibirlo a partir de allí. Al menos en teoría podemos tener la llave y luego publicarla. Hay algunas decisiones que hay que tomar si lo hacemos. Si consideramos la motivación de por qué lo hicimos, esto hace que la automatización sea mucho más fácil porque en el momento en que uno publica la llave, el registro la puede recibir y no hay ningún otro sistema involucrado.

La implementación, si ustedes eligen hacer esa implementación, no tienen que preocuparse porque esta implementación es automática y

con CDS también tenemos un mecanismo para actualizar la zona y el padre para esa implementación. También queremos mostrarles que DNSSEC no es tan complicado de usar.

Este es un servidor autoritativo Knot. Es solamente una línea que hay que agregar a la configuración de la zona y queda firmada. Algo bueno con Knot es que tiene muchas características por defecto que permiten que el CDS se publique automáticamente. Para Knot solamente hay que agregar una línea y ahí se habilita la firma del DNSSEC, si es que el registro soporta CDS y listo. Ya está.

Lo mismo ocurre con la parte donde hay que poner solamente dos líneas de configuración. Nosotros seguimos estándares. Le preguntamos al CZNIC qué hacer. Hasta ahora no hemos tenido ningún problema. La pregunta siempre es cómo lo implementamos exactamente, si hay algo que no está en el RFC. Tenemos dos casos de uso donde uno es que la zona ya está validada. Es bastante fácil. Allí validamos o recibimos el record CDS de la zona hija. Lo validamos a través del DNSSEC y si el CDS no cambia durante tres días actualizamos el record set de DS.

Lo que es mucho más complicado y lo que nos ocasionó más problemas es cómo hacer el bootstrap si la zona no está firmada. Digámoslo así, si la zona no tiene DS en la zona padre, no hay una confianza inicial. Ahí dijimos: “Tenemos que generar esa confianza inicial y tenemos que tener al menos algo de confianza en el servidor de nombre autoritativo”. Ahí dijimos: “Vamos a chequear todas las instancias del servidor de nombre autoritativo en IPv4 e IPv6”. Si

tenemos la misma respuesta en esas direcciones para el record CDS, eso es algo en lo que ya podemos confiar.

Lo segundo es evitar el spoofing. No hay ninguna otra forma de spoofear las respuestas a través del UDP. Lo hacemos también durante tres días. Pensamos que es posible hacer un hijack de BGP en todos los servidores de nombres durante tres días. Esto es algo que también se puede hacer. Hacemos las consultas desde distintos puntos de vista. No hay un punto en el que las consultas se puedan hacer desde puntos diferentes. Sería más difícil no hacer una apropiación o un secuestro. Como ven, las respuestas al record CDS durante tres días para TCP vienen de distintos puntos y luego las colocamos en la zona padre.

Hubo una pregunta esta mañana. ¿Qué pasa si la validación DNSSEC no funciona? Si utilizamos el modelo pull, chequeamos que la zona quede validada con DS del registro CDS y si eso no ocurre, no ponemos el DS en la zona padre. Básicamente, no podemos fragmentar el DNSSEC al publicar un record CDS. Sí puede ocurrir con el modelo push si es la clave equivocada. Allí nosotros soportamos solamente algunos algoritmos, incluido un digest zero para el borrado.

Nosotros no comunicamos por email. En general, si nosotros enviamos un email al registrante, no va a entender cuál es el mensaje. Si le enviamos un mensaje al contacto técnico, en la mayoría de los casos, no es técnico y por eso elegimos un enfoque diferente. Decimos: “Vamos a darle a todo titular de dominio la posibilidad de ver cuál es el estado del proceso de publicación de CDS”. Allí ponemos algo que se llama el chequeo de estado del CDS. Se puede ver el nombre de

dominio. Pueden ir a nic.ch/cds y básicamente les vamos a dar allí toda la información que encontramos en el record de CDS. Lo consultamos una vez, luego dos veces y finalmente les damos la fecha donde vamos a poner el record de CDS en la zona padre. Ahora funciona para bootstrap.

Para la implementación, uno de los registradores lo habilitó hace dos días en el periodo en el que la característica está disponible pero los registradores tienen que decir cómo les fue en sus nombres de dominio. Algunos ya los hicieron. Este es el nombre de dominio de Cloudflare que lo validó hoy tres veces y mañana lo vamos a colocar en la zona .CH. Este va a ser entonces uno de los primeros dominios en el que lo hacemos a través del sistema de CDS.

Estos son los números. Tenemos alrededor de un 2% de dominios firmados con DNSSEC. Tenemos unos 57.000 nombres de dominio .CH firmados con DNSSEC. Si miran a los operadores del lado derecho tenemos a Cloudflare, Google Domains y otras empresas de alojamiento que publican los records de CDS. Más adelante en enero vamos a colocar el record de CDS en la zona .CH. Gracias.

JACQUES LATOUR: Gracias, Michael. El siguiente es Richard, quien nos va a contar todo sobre GoDaddy.

RICHARD MERDINGER: Primero quiero agradecer a Steve Crocker por haberme invitado como registrador. GoDaddy obviamente es un registrador muy grande y

también un proveedor de servicio de DNS muy importante. Espero que las diapositivas puedan cargarse. Cuando ustedes piensan en GoDaddy piensan en el registrador primero y no en el proveedor de DNS. Nosotros tenemos el DNSSEC habilitado desde hace ya muchos años. Steve nos ayudó para que eso funcionara en el PIR. Estamos en un punto en el que, como somos un registrador con conexión directa con el registro, y para las zonas de DNS que gestionamos tenemos una implementación de DNSSEC de un solo clic, lo colocamos en nuestro sistema.

También relativamente nos hemos focalizado en nuestro ecosistema y ya es el momento en que empecemos a apoyar al sistema de Puerto Rico porque, como dije, GoDaddy da muchos servicios pero hacemos un servicio que es de registrador y también un servicio de DNS. Cloudflare también es registrador con DNS.

Una de las cuestiones que en general nosotros hacemos es apoyar la idea del CDNSKEY y de la actualización de los records de CDS a través del proveedor de DNS al registro. Sin embargo, nosotros cubrimos la relación entre nosotros y el registro en lo que se refiere a cambiar el paradigma de los servicios que estamos brindando para el registratario o para el titular del dominio. Cuando hay que cambiar o habilitar o deshabilitar DNSSEC en el record de DNS nosotros creemos realmente que tenemos que hacerlo a través del registrador donde las actualizaciones van a ir ocurriendo en forma constante.

Como todos sabemos, con CDNS esto puede ocurrir con mucha fluidez pero puede requerir implementación. Dependiendo del tamaño de

zona podría haber cuestiones pragmáticas como costos de infraestructura, escaneo, etc. Nosotros no pensamos que haya una sola solución sino que tiene que haber un conjunto de soluciones, algunas de ellas pueden ser para aquellos que eligen la implementación. Pueden ver que esa solución está muy bien y nuestra arquitectura, como dijimos ayer, ha sido desarrollada internamente y luego hubo un protocolo público que se llama Domain Connect. Domain Connect es un paradigma a través del cual se puede habilitar proveedores de alojamiento o cualquier tipo de alojamiento de un servicio que pueda configurar el DNS a través de una plantilla a los proveedores DS.

Por ejemplo, si alguien utilizase Wix o Weebly o algún otro sitio web, el sistema Domain Connect va a determinar la configuración específica del DNS donde el aprovisionamiento para ese proveedor está en ese apoyo del DNS. Hay un sistema que va a permitir que Cloudflare, como proveedor de servicio, automáticamente aplique una plantilla a la zona que no conoce a través del proveedor de DNS. Es una manera en que se quita el servicio del proveedor de DNS y se trata de que la implementación sea lo más adecuada posible.

Hablamos del servicio Domain Connect y que los records DS también pueden ser actualizados de manera que el registrador pueda ser considerado en un DNS separado de GoDaddy. El servicio de registrador estarías suscrito a Domain Connect y el proveedor de DNS también estaría suscrito. El proveedor de DNS podría iniciar la actualización del record de DS a través de un EPP al registro. La idea es que el registro en cuestión no implementa este otro mecanismo.

En general, estamos a favor de hacer lo que se presentó. Queremos tener mucho cuidado de no permitir que se hagan cambios de paradigma en la experiencia del DNS para el cliente. Una vez que se opera bajo DNSSEC no queremos ponernos en medio e impedir la actualización continua que debería darse. Eso es todo lo que tenía. No tengo más diapositivas.

JACQUES LATOUR: Gracias, Richard. Solo tengo 100 preguntas. No sé por dónde empezar. Voy a empezar con una pregunta mía para Vicky. Usted dijo que Cloudflare publica un nuevo tipo de registro CDS0 y CDNSKEY0.

VICKY SHRESTHA: No. Cloudflare está publicando CDS y CDNSKEY para todas las zonas con DNSSEC. Habilitamos recientemente CDS0 y CDNSKEY0 si el cliente decide deshabilitar DNSSEC en el portal.

JACQUES LATOUR: No es un nuevo tipo de registro, ¿no?

VICKY SHRESTHA: No. Solo si quieren deshabilitar DNSSEC.

JACQUES LATOUR: ¿Alguna pregunta? Peter.

PETER KOCH: Hola. Soy Peter Koch, el jefe de escepticismo de DENIC. Cuando consideramos las motivaciones para soportar CDS y CDNSKEY Michael creo que dijo que una de las razones era que la implementación del rollover era tan complicado que para qué hacerlo. Si recuerdo bien, una de las motivaciones era capacitar al personal para que en caso de tener que hacer una implementación de emergencia de la clave, la gente pudiera hacerla. Lo que hicimos fue ver que hicimos la gimnasia, fue engorrosa, les enseñamos a los estudiantes a hacer la automatización de la gimnasia por nosotros y ampliamos esta automatización. A mí me parece muy raro. La implementación de emergencia cómo va a interactuar. Antes había mucho trabajo en la transferencia del operador del DNS. Eso va a seguir necesitándose con el registro y el registrador. ¿Cómo se va a manejar esto con el modelo de CDS y CDNSKEY?

MICHAEL HAUSDING: Más de una pregunta en realidad. La primera pregunta sobre el traspaso de la clave. El segundo nivel es bastante distinto. Creo que la implementación de la clave para el nombre de segundo nivel es distinta. La mayoría de los usuarios podrán activarlo pero nunca van a entender cómo funciona. Capacitar en eso es algo que tendremos que dejar en manos del servidor de DNS. No hacerlo creo que no hay capacitación que haya que hacer del lado del registratario.

La segunda pregunta es la implementación de emergencia y el cambio de operador del DNSSEC. En caso de emergencia hay dos posibilidades. Una, hacer el traspaso de emergencia con CDS. Hay que

hacerlo en el servidor CDNS. En ese caso, CDS toma el control y sí puede haber algún tipo de demora. Otra posibilidad es ir al sitio en caso de emergencia, aunque no lo recomendamos. Por eso implementamos el algoritmo cero, para indicar a la zona padre que queremos ir al sitio. Eso también es una posibilidad. Hacerlo a través de CDS. Solo escaneamos la zona una vez por día. Eso genera un retardo de hasta un día hasta que nos podemos dar cuenta de que lo único que se puede hacer en caso de emergencia es ir al sitio pero siempre es posible que .CH empuje una nueva clave o la remueva de la zona. Eso da solo cierto tiempo hasta que se pueden hacer las cosas bien.

JACQUES LATOUR: Steve, ¿tiene una pregunta?

STEVE CROCKER: Sí. Gracias, Jacques. Varias cosas. Quiero responder directamente a la pregunta provocadora de Peter. Gracias, Peter, por ella. Yo entiendo que el rollover es una buena práctica y tiene que hacerse de manera regular, no solo para emergencias, que los algoritmos y las claves no tienen vidas naturales o duraciones naturales. Aun cuando puede decirse que se necesita traspasar la clave, no es manera de manejar un sistema con sostenibilidad a largo plazo. No es solo para emergencias. Tiene que hacerse en forma regular y normal.

En segundo lugar, con respecto al cambio de los operadores del DNS, es importante tener en cuenta lo siguiente. Hace poco mostré una

presentación de [inaudible] que cubría no solo el cambio de un operador a otro sino tener múltiples operadores independientes que releven a los mismos clientes. Ese tipo de versión sería como más fácil para cambiar de un operador al otro. Creo que esta sería una solución excelente y completa del problema de los cambios de operadores.

Volviendo a la pregunta con la que abrí, ¿qué más se necesita? Hay muchas presentaciones hoy que se centran en las soluciones con CDS y CDNSKEY y que los registros hagan el pull de los registros. Las presentaciones casi todas han sido de los ccTLD. No he oído de los gTLD. ¿Cuáles son sus estimaciones? ¿Qué se necesitaría para poner esta solución en el espacio de las partes contratadas de la ICANN? Luego tenemos el abordaje complementario que nos han presentado de tener un modelo push con las interfaces apropiadas.

Voy a repetir lo que dije al comienzo. Yo no tengo ningún interés aquí más allá de lograr que las cosas funcionen. No me importa de qué forma. Lo que a mí me preocupa es que esto se estanque porque la mitad de las partes dicen: “Lo vamos a hacer de esta manera” y la otra mitad va a decir: “Bueno, lo vamos a hacer de la otra”. No me gustaría que nos quedemos atascados en el medio. Gracias.

JACQUES LATOUR: Gracias, Steve. Aquí hay muchos temas que abordar. Uno de los más importantes es el proceso de bootstrap, cómo hacemos que el DS llegue a la zona al inicio. Cuando comenzamos esta discusión, la gente se sentía reacia a tomar un CDS y crear un DS. Ahora lo hemos comenzado a hacer con los ccTLD. En el área de gTLD, la definición de

política en este tema es muy débil, es muy general. Tenemos que crear un texto mejor que defina la forma en que el gTLD acepta el DS del bootstrap, cuál es el proceso para que el DS entre al registro, cuál es la opción que vamos a aceptar o no. A partir de ahí, elaborar un caso.

En este momento no sabemos dónde están con exactitud. Es difícil generar un proceso. En GoDaddy hay un ejemplo. Si ustedes crean un dominio .CA y el hijo, dominio se firma de inmediato. Hay un registro CDS. Sé que es un dominio nuevo porque lo creé en mi registro. Si hago el pull y tomo el CDS y lo añado de inmediata, eso va en contra… A ver, cuál es su reacción. ¿Qué piensa? Hay un segundo panel de política sobre esto. Podemos volver a hablar.

RICHARD MERDINGER: Entiendo que el registro es parte de quien hace la iniciación y del DNSSEC. El registrador crea el registro y el registro es parte de esa transacción multifacética que substancia DNSSEC. Es distinto de la otra política. Eso no es un problema.

JACQUES LATOUR: Ustedes crearon el dominio, ¿verdad?

RICHARD MERDINGER: Sí.

JACQUES LATOUR: Pero ustedes siempre crean el dominio, ¿sí?

RICHARD MERDINGER: Si creamos el dominio y la política del registro es no hacer DNSSEC, una instancia subsiguiente tiene que ser iniciada por el registrador. Esto lo hicimos a través de la transacción multifacética que es iniciada por el registrador. El otro escenario es que hay dos transacciones. Una es crear y la otra es la instanciación del DNSSEC. Si soy vago les pido disculpas. Es el día 35 de la ICANN.

JACQUES LATOUR: Tengo que pensar un poquito. Si crean un dominio…

PAUL WOUTERS: No, termine. Adelante.

JACQUES LATOUR: Termino. Si usted crea un dominio y .COM no escanea, GoDaddy toma el DS y lo añade automáticamente.

RICHARD MERDINGER: Sí.

JACQUES LATOUR: Eso sería fantástico.

RICHARD MERDINGER: Sí. Lo hacemos para nuestras propias zonas con DNSSEC. Por eso se está tornando en parte del ecosistema. Hay que definirlo todavía.

PAUL WOUTERS: Soy uno de los dos autores del RFC correspondiente. Se hizo así porque había una demanda de los operadores de DNS de poder hacerlo sin involucrar a los registros que a menudo un cliente cambia el registro y no el registrador. El titular del dominio muchas veces no conoce estos detalles técnicos. Si cambia de proveedor de DNS y no entiende siquiera qué es DNSSEC. Si pasamos a un hoster de DNS que tiene capacidad de hacer DNSSEC, estos detalles técnicos al titular del dominio realmente no le importan pero el hoster que va a desplegar DNSSEC por default tiene que saberlo, por eso hicimos esta separación en el uso, porque queríamos que se automatizara esta parte lo más posible.

RICHARD MERDINGER: Si me permite responder, hay algunos elementos… A ver, perdón. Las líneas son muy difusas aquí. Hay algunos elementos donde el SRS y la base de datos de la registración en el registro contienen atributos del nombre de dominio. Algunos de estos atributos también residen, en mi opinión, dentro del archivo de la zona raíz, los servidores de nombre, etc. La selección de proveedor de los servidores de nombres y los registros DS necesitan más componentes de configuración, aun cuando viven como parte del ecosistema que están en el DNS general. El retorno me está desconcentrando.

JACQUES LATOUR: Steve tenía una pregunta, un comentario final.

STEVE CROCKER: Gracias. Mi pregunta intenta entender si hay alguna atención aquí. Es una pregunta para Rich en particular. Si el registro hace el escaneo y sube información nueva que a mitad de camino no llega al registrador, uno de los comentarios que oigo mucho desde la perspectiva de política es que el registrador tiene que tener la información completa sobre la zona y es una de las razones por las cuales no tiene que existir un camino que pase por encima del registrador. Rich está en muy buena posición de darnos más detalles al respecto. Le pregunto qué piensa si entra nueva información del DS del hijo hacia el registro y no pasa desde el cliente hacia usted, si no va hacia usted.

RICHARD MERDINGER: Gracias, Steve. Volviendo al paradigma original, es tan simple como que el registro escanea, actualizan el record DS, se crea un mensaje en la nota y el registratario es notificado del cambio y podemos actualizar nuestros sistemas para estar en sincronización. Tenemos que asegurarnos de que los cambios de configuración del DNS, que todos los sistemas estén sincronizados. La verdad, no sé qué pasa con el sonido.

RICK WILHELM: Rick Wilhelm, de VeriSign. En relación con lo que hablamos antes, la falla de registración, típicamente durante el proceso en mi experiencia como registrador antes y registro ahora el DNSSEC está configurado sobre la creación inicial del registro, el create inicial. Muchas veces el

registratario potencial no quiere ponerse en el medio de la registración, del proceso de registración. Cuando yo era registrador, eso yo no lo quería en mi flujo para demorar una conversión. No sé cómo es el flujo de Rich en este momento, si se puede ofrecer durante el flujo inicial de la registración pero la mayoría de las veces el create y el adding de los registros se hace en general en el flujo posterior a la creación.

RICHARD MERDINGER: Rápidamente, voy a decir que sí. Usted tiene razón. Hay muchos nombres de dominio que no se instancian. Se ponen por default en el DNSSEC, lo que tiene sentido a gran escala.

JACQUES LATOUR: ¿Uno o dos?

ORADOR DESCONOCIDO: Hay una extensión de EPP que el registro puede actualizar al registrador con más información. Puede decirle: “Mire, aquí tengo nueva información del DNS para que usted pueda actualizar sus registros”.

JACQUES LATOUR: Gracias por la aclaración. Patrik.

PATRIK FÄLTSTRÖM: Debemos separar la activación y desactivación del DNSSEC inicial, dependiendo si hay o no registros y la actualización de los registros DS. Es la gran pregunta de quién tiene la responsabilidad para que funcione la zona. Hay un acuerdo contractual entre el registrador y el titular del nombre y la activación y la desactivación del DNSSEC. Esa operación, como dije muchas veces en el IETF y como todos saben, es algo que yo creo en personal que es algo que corresponde al registrador. Es su responsabilidad. Las actualizaciones de los registros DS cuando el DNSSEC está funcionando, está activo, esa es una historia totalmente distinta. Apoyo lo que veo en las diapositivas, si es que no lo entendí mal.

RICHARD MERDINGER: No sé si es uno o dos. Me perdí esa parte. Con respecto a lo que usted decía, Patrik, la habilitación de DNSSEC… Les pido disculpas. Debo tomar un segundo para responder.

JACQUES LATOUR: De acuerdo. ¿Alguna otra pregunta? Creo que podríamos hablar días. Agradeceré a los panelistas por esta sesión. Muchas gracias.

RUSS MUNDY: Muchas gracias por ese panel. Les agradezco a todos los panelistas. Nuestra siguiente sesión, nuestro siguiente panel es sobre el tema quizá favorito de todos, especialmente ahora que estuvo muy bien, que es el traspaso de la KSK. Tenemos a Wes y a Matt. Wes va a ir primero. Wes, ni bien puedas empezar.

WES HARDAKER: Sé que estamos retrasados. Wes Hardaker, de la Universidad de California. Les voy a hablar un poco sobre cómo creo yo que funcionó el traspaso de la KSK. Creo que fue una de las mejores instancias de la raíz. Cómo mi perspectiva cambió de preocupación al principio hacia otra de calma. Esta es la principal. Voy a empezar con mi paranoia después de los miedos que tuve y finalmente vamos a hablar de la realidad.

Mi paranoia inicial estaba fundamentada en qué es lo que sucedería si el mundo se cae de la red. Esto podría ser muy malo y me puse un poco paranoico. ¿Qué pasa entonces con todos los resolutores? ¿Se vuelven locos y empiezan a mandar millones de solicitudes? Eso ya pasó antes. Este gráfico era uno de mis miedos principales, que hay mucho tráfico en el traspaso, en la implementación. Como operador de red, una de las cosas que más me preocupaba era que esto volviera a ocurrir. Esa era mi paranoia. Esto me llevó a utilizar muchos datos muy interesantes que yo podía analizar.

Antes hablé sobre encontrar software de VPN desconfigurado que los usuarios pudiesen tener un problema en el keyroll y ver si había alguna queja. Hoy voy a hablar sobre mi fracaso para encontrar algo más. Estas fueran muy buenas noticias por las cuales la implementación funcionó tan bien. Para ver quién está en problemas, quién puede ser impactado, esta es una de las cuestiones con las que todos han tratado de trabajo. Geoff Huston hizo mucho trabajo. Hay que saber dos cosas. Cuál es la clave que está validada. Hay un par de fuentes de

información, una de las cuales es la RFC 8145. La otra es la KSK signaling. Ninguna de estas son señales completas y la realidad es que es imposible tener un conjunto de datos perfecto. Este es uno de los fracasos, de hecho. Me parece que si leyésemos las señales hoy buscaríamos claves para ver que teníamos esa información del lado receptor. Lo otro que tenemos que saber es si están validadas. Hay mucho debate respecto de si es posible medir si un resolutor está validando simplemente al mirar el tráfico.

Un poco de contexto ahora. Cómo funciona la resolución con respecto a un resolutor validante. Primero, el resolutor le dice a la raíz: "¿Tienes www.ejemplo.com?" Si ustedes vieron el DNSSEC para Principiantes, van a ver que está esa parte en el conjunto. La raíz responde con el nameserver para .COM y allí incluye el record de DS en la firma de todos estos datos. Es interesante. El resolutor inmediatamente envía la solicitud al record DS hacia la raíz .COM y no tiene que hacerlo necesariamente. De hecho, tiene el record firmado que le enviaron pero no queda claro cuál es el resolutor que lo hace y cuál es el que no.

Mark me confirmó que BIND sí lo hace y no llegaron al punto en el que tienen que chequear los datos en la sección adicional para ver si lo pueden mantener allí. Esto me llevó a la hipótesis de que un resolutor validante que está consultando datos legítimos en la raíz en el 50% de los casos son para records de DS y el otro 50% son para las originales. El DS no debería estar consultando ninguna otra cosa porque no hay ninguna otra cosa que buscar en la raíz.

El primer paso es que hay que remover todo esto que está ocurriendo ya en registros de basura. Lo violeta que vemos en este gráfico lo hizo uno de mis becarios. Indica todos los multiniveles. Si ustedes buscan www.ejemplo.com o [inaudible] van a ver que no existe. La línea naranja son los datos de basura que se generan para determinar si es correcto. Es fascinante que una de las señales principales a la raíz son datos junk porque cada vez que deja de funcionar, manda conjuntos de caracteres basura. Las otras tres líneas son las otras consultas simples como .COM o university, etc.

Estos son los resultados. Si mi hipótesis es correcta, y uno esperaría que todos los datos se envíen a los servidores de raíz, el 50% de las consultas van a ser consultas DS. El eje horizontal es básicamente el porcentaje y el vertical es el de la cantidad de hosts que envían ese porcentaje. Vemos dos puntas muy grandes. De eso se trata mi hipótesis. Cuando los hosts envían más datos, están más cercanos al 50% porque recuerden que esto es desde la perspectiva de unos datos de raíz del 25 de septiembre antes de la implementación. Lo de la izquierda no estoy muy seguro, no sé muy bien por qué la gente envía el 10%.

Suponiendo que mi hipótesis es correcta, yo decidí que vamos a empezar a ver esa punta. Vamos a reducir qué es lo que vamos a mirar a cosas que están dentro del 25% del record, suponiendo que estos son resolutores validantes y estos son los que yo quiero verificar. De nuevo, esto es el 25 de septiembre antes de la implementación. Mi paranoia todavía seguía muy alta para esa fecha.

La siguiente pregunta es cuáles de estos validadores en esa subida gigantesca envían solamente señales de validación KSK 2010. Estos iban a ser los que iban a tener problemas. Esto es lo que yo hice para el software VPN anterior. Hubo 45.806 resolutores matching en ese bump. El apoyo para la clave fue 420. Hubo todo un conjunto que no entró en la nueva llave. ¿Quieren adivinar cuántos son los que utilizaron la llave vieja? 12. Es una reducción de los 18 anteriores. Solamente 12 resolutores validantes, solo 12 estaban enviando la llave antigua. Había 420 nuevos. Claramente, se estaba perdiendo la señal. Esa discrepancia entre 12 y 420 hizo que todo fuese mucho mejor y la implementación una semana después funcionó bien. Mi idea era equivocada. Eso es lo que sucede. Me equivoco todo el tiempo.

Mi siguiente pregunta es cuáles son los records de DS que se están enviando, cuáles eran las consultas. Los resolutores solamente envían un query de DS a .COM y nunca a algo como example.com. ¿Los resolutores son razonables? No. No lo son. Cuando entramos en estos dos resolutores vemos que hay muchos que son consultas basura.

¿Cómo es la vida real? Les voy a mostrar un gráfico de nuestra red de operación. Ustedes no tienen que entender qué son estas líneas pero son gráficos que muestran tráfico a nuestro servidor raíz. Esto fue antes de la implementación. Si ustedes miran, van a ver que las líneas van hacia arriba. Estos fueron los momentos de susto en los que todos decían: “Esto podría no funcionar”. Esta es la subida, un par de horas después donde todo volvió a la normalidad. Después nos quedamos todos tranquilos. En este caso una línea recta quiere decir que la persona vivió y no murió como en el mundo médico.

En conclusión pareciera que hubo dos cuestiones importantes. La actualización del software y la actualización de la configuración. Las dos requerían que el evento funcionara muy bien. Yo realmente creo que el año extra en el que tomamos una excelente decisión con Matt y con su equipo, porque no estoy muy seguro de si hubiese funcionado bien hace un año, nos dio suficiente tiempo para que muchas cosas cambien.

Lo último son los resolutores. Nosotros creemos que los entendemos pero cada vez que vamos a ver qué es lo que están haciendo vemos que el grupo de RSSAC está realizando un estudio para ver cómo los resolutores se comportan. Esperamos ver esos datos porque a veces ocurren cosas raras. Si alguien vio Bill and Ted's Excellent Adventure, ahí hay una cita sobre esto. Realmente nosotros vamos a tener que entenderlos mejor para estar seguros de que todo lo que hagamos en el DNS funcione bien. Gracias.

RUSS MUNDY: Muchas gracias, Wes. Vamos a pasar a Matt y vamos a aceptar las preguntas al final.

MATT LARSON: Hola. Soy Matt Larson, vicepresidente de investigación. Estuve involucrado con la implementación de la KSK de la zona raíz. En caso de que estén en suspense, les digo que nosotros sí hicimos el traspaso de la KSK. Sí la implementamos. Ocurrió a tiempo, tal como se programó. Tengo algunos datos para mostrarles. Se está cargando.

RUSS MUNDY: ¿No son maravillosas las computadoras?

WES HARDAKER: Mientras esperamos, les cuento que hace dos días yo fui a ver algunos datos para ver cuántos resolutores entraban en ese 50% y son 10. Hay 2 menos pero no son los mismos 10.

RUSS MUNDY: Está en la sala pero todavía no llegó al Adobe Connect. Le vamos a pedir a Matt que continúe de todos modos.

MATT LARSON: Como dije, el traspaso ocurrió con la publicación de la zona raíz el 11 de octubre a las 16:00 UTC. Esta es la línea de tiempo de los eventos. Tuvimos una ventana de tres horas donde le dedicamos más tiempo de lo normal a mirar a la zona raíz. La función de IANA no inspecciona la zona antes de publicarla pero en este caso VeriSign tuvo mucho cuidado porque queríamos estar seguros de que se podía confirmar que todos estaban listos y luego ocurrió a tiempo. Lo hicimos desde Ámsterdam. Este es VeriSign en Ámsterdam. Todos queríamos estar en un avión volando a Ámsterdam para la KSK y con mucha movilidad nos dieron el espacio. Se lo agradecemos. El joven es el que tiene una copia del año 2010 donde hubo una instancia de una reactualización a la derecha.

Algo que sí vimos es que si ustedes miran la cantidad de consultas DNS en la raíz vemos que sí aumentó. Hay una animación y lamentablemente no se la puedo mostrar pero tengo capturas de pantalla. Pido disculpas si las diapositivas no se pueden leer. La que hay que mirar es la de arriba a la izquierda. Estas son consultas de DNS de cada uno de los servidores de raíz individuales que dan datos estadísticos a la ICANN y a la izquierda tenemos el conjunto de datos.

Lo que se puede ver es que la escala cambia lamentablemente. Parece que es lo mismo pero no lo es. Ni siquiera puedo ver desde aquí. Son 1.400 consultas por segundo y a la derecha, bien a la derecha del gráfico, está el traspaso de la KSK. Aquí entonces estamos llegando a las 48 horas después de la implementación de la KSK. Lo que vemos es también el gráfico de la escala que está en 2.500 consultas por segundo. Si vemos cómo está ahora, llega a 4.000 consultas por segundo.

Lo otro para ver de este gráfico es que la línea amarilla que ustedes casi no pueden ver es de hace una semana. Si se preguntan si es que esta consulta va a seguir por siempre la respuesta es que no porque es ahora, una semana después de la implementación, cuando la roja y la amarilla están iguales. Hemos llegado a una cierta meseta. Por lo tanto, tratamos de ver qué es exactamente lo que está sucediendo y para poder empezar esta investigación el equipo hizo un muy buen trabajo.

Ciertamente, nosotros esperábamos más consultas de DNSKEY porque cuando el resolutor tiene un ancla de confianza, tiene que haber

alguien que le diga al DNSKEY si es que nunca va a encontrar a estas consultas y consultas y consultas que dependen de los resolutores. Lo que decidimos hacer fue mirar el comportamiento de la consulta DNSKEY. Eso ocurrió el 10 y el 14 de octubre. Hubo más de un millón de resolutores únicos que pedían una DNSKEY durante los cuatro días completos. 155.000 de ellos ocurrieron tanto el 10 como el 14 de octubre. 85.000 resolutores enviaron un pedido, una solicitud al menos una vez al día. Esto fue solamente en el transcurso de esas fechas, por eso tenemos los datos paquete por paquete.

Vamos a ver los 155.000 resolutores que nos hablaron el 10 y el 14. Este gráfico nos da un poco más de explicación. Primero les voy a dar la explicación. El eje X más abajo implica cuántos queries envió el resolutor el 10 de octubre y el eje Y representa cuánto envió el 14 de octubre. Cada uno de estos puntos representa un resolutor específico. En la zona verde vamos a indicar que envió el mismo orden de magnitud de consultas el 10 que lo que ocurrió el día 14. El eje X y el eje Y son lo mismo. Esta es una escala de log, por lo tanto es a la potencia de 10. Lo que ven a la izquierda más abajo son los resolutores que enviaron unas consultas de DNS key relativamente bajas. Pasaron de 10 a 100 y a medida que vamos llegando a la derecha vamos a tener cada vez un volumen más alto.

¿Qué es lo que vemos allí en ese color un poco violeta? Ese círculo son aquellos que enviaron mucho más el 14 que el 10. Como pueden ver, potencialmente es en realidad un orden de magnitud que está basado en cómo fue costeado. Son tres órdenes de magnitud a la décima el 10 y el 14. Ese es el conjunto de 145.000 que estábamos mirando antes.

Aquí vemos cuántos resolutores entran en cada una de las categorías en el orden de magnitud pero vamos a ir directamente a eso. Los últimos tres puntos son el resumen de lo que yo les quiero explicar aquí. Casi el 96% de los resolutores siguieron en el mismo orden de magnitud en términos de la cantidad de consultas que hubo pero hay un grupo de 2.000 que enviaron más que el orden de magnitud. Algunos de ellos continúan enviando muchas consultas al DNS. Es un aumento muy importante.

También es importante decir que hay un número mucho mayor de más de 4.000 que están enviando menos queries DNS key. Esto es en las primeras fases de esta investigación. Todavía no les puedo decir a ustedes más que eso. Hay que continuar mirando para poder entender. Seguramente este va a ser uno de los misterios del tráfico que todas las direcciones de servidores raíz están enviando esta radiación de background al DNS.

Esto no salió bien. Este es el gráfico. Casi, casi lo podemos ver. No importa. No me gustan los datos de todos modos. Este es el informe 8145. Este es el conjunto de datos que nos llevó a la decisión de posponer un año más la implementación. Lo que se ve aquí es que cuantos más datos teníamos, menos nos preguntábamos qué era lo que nos decían. Por eso vemos ese pico en la implementación de la KSK y ahora tenemos un porcentaje más alto de resolutores pero luego esa subida se retiró. Volvió a bajar. Lo que quería era mostrarles que todavía se puede ir a un sitio web para ver si en el futuro vamos a poder publicar esos datos pero realmente creo que en este punto tenemos que ver qué hacer con nuestra investigación.

Como todos probablemente sepan, hubo muy poco impacto para contar como resultado del traspaso. Hubo un único informe de problemas muy menor y varias cuestiones que se escucharon por Twitter y las listas de mail. Una persona dijo: “Una de las cosas que estoy monitoreando se rompió. Se debe al traspaso”. Una cosa muy menor. Hubo dos interrupciones que son de origen sospechoso. En especial, el de Irlanda. Fue muy sospechoso que el de Irlanda estuviera relacionado con el traspaso pero nadie habla. Estamos investigando a ver qué pasa. No es necesario conocer los detalles. Hay que definir si fue un problema del traspaso o no. luego el de Vermont, también un tema sospechoso. Los contacté y me dijeron que me iban a volver a contactar. Veremos.

Mi aquí me recuerda que el traspaso no terminó. Quedan cosas por hacer. La ceremonia de la KSK Q4 va a generar firmas que revocarán en el 2010 y eso pasará el 11 de enero. Ese es el día que publicaremos la zona raíz con el conjunto de bit revoke. Una firma adicional será en 2011. Si se revoca la clave hay que demostrar prueba de posesión. Esto significa que vamos a tener una respuesta de DNS aquí un poquito más grande. Habrá un máximo histórico de respuestas. No tenemos indicación de que esta mayor respuesta sea parte de este proceso.

Hace un año y medio, fue en julio de 2017 cuando publicamos cuatro DNS key en la zona raíz por primera vez. Esto ha venido pasando sin reportes de problemas. Creo que probablemente haya un aumento. Nos preocupa un poco pero va a pasar. El 22 de marzo es cuando la KSK 2010 se quitará de la zona raíz. Dos ZSK en los bordes. Todavía no llegamos. Lo más importante de la clave KSK 2010 sigue existiendo.

Hay dos módulos HSM en la instalación de gestión de la costa este y vamos a seguir manejándolo. Esa es mi última diapositiva. No tengo mucho más para decir respecto del futuro más allá de que estamos casi a punto de terminar el traspaso.

Solo decir una vez más lo que he venido diciendo. En la ICANN intentamos trabajar con la comunidad en las direcciones para los futuros traspasos de la KSK. No nos corresponde a nosotros decidir sino trabajar con la comunidad. Creo que funcionaría muy bien si presentáramos un proceso preliminar a discutir. Si no, tendremos interminables sugerencias de cómo hacer las cosas. Tenemos que ser más concretos. Hay muchas cosas de las que tenemos que hablar. La frecuencia de los traspasos, si vamos a tener una clave standby y también el algoritmo. Son todos temas relacionados pero separados. Tenemos que ver cómo darles un marco y presentar a la comunidad para que la discusión sea productiva. Espero que en Kobe podamos hablar un poquito más de esto e iniciar la discusión. Eso sería todo.

RUSS MUNDY: Gracias, Matt. Muchísimas gracias a todos los panelistas. Estamos a punto de cerrar. No tenemos tiempo para preguntas porque tenemos que dejar la sala porque este almuerzo no es para nosotros. El nuestro es afuera, subiendo dos niveles la escalera. Es el Banquet Hall. No olviden el ticket.

[FIN DE LA TRANSCRIPCIÓN]