ANDREA GLANDON: Buenos días, buenas tardes y buenas noches a todos. Bienvenidos al seminario web de creación de capacidades de At-Large sobre el traspaso de la KSK, el miércoles 13 de junio de 2018 a las 21:00 UTC. Nuestros presentadores de hoy son David Conrad y Andrei Kolesnikov. No vamos a pasar asistencia porque es un seminario web. Contamos con interpretación en español y francés. Por favor, quiero pedirles que mencionen sus nombres para que los intérpretes puedan identificarlos en los canales lingüísticos correspondientes y también para la transcripción. Por favor, hablen a una velocidad razonable para permitir a los intérpretes traducir adecuadamente.

Por favor, si están conectados en el puente telefónico o a través de Adobe Connect, les pedimos que silencien sus teléfonos y sus líneas. Muchas gracias por participar. Ahora le voy a dar la palabra al señor Tijani Ben Jemaa, quien es el presidente del grupo de trabajo de creación de capacidades.

TIJANI BEN JEMAA: Muchas gracias, Andrea. Buenas tardes, buenos días y buenas noches a todos. Como ustedes han escuchado, este es un seminario web sobre el traspaso de la KSK. En realidad, habrá dos seminarios web sobre el traspaso. Uno antes del traspaso y otro será hecho luego del traspaso de la KSK. Hoy hemos invitado como presentador a David Conrad, director de Tecnologías de la ICANN, para que nos cuente sobre el traspaso. Tiene mucho conocimiento sobre este tema. También habrá una segunda parte que estará a cargo de Andrei Kolesnikov, coordinador de enlace de At-Large. Ahora es miembro también del RSSAC.

ANDREA GLANDON: Tijani, ¿se encuentra conectado al audio?

TIJANI BEN JEMAA: ¿Me escuchan?

ANDREA GLANDON: Sí, lo escuchamos. Adelante, Tijani, por favor.

TIJANI BEN JEMAA: Bien, perfecto. Continúo entonces. Vamos a comenzar con la presentación. Andrea, si antes tiene que hacer algún anuncio, por favor, tiene la palabra ahora para hacerlo.

ANDREA GLANDON: Sí. Muchas gracias, Tijani. Quiero comentarles algunas cuestiones antes de comenzar. Para la sesión de preguntas y respuestas durante este seminario web pueden ver en la parte izquierda de la pantalla un recuadro donde pueden colocar sus preguntas. También lo pueden hacer en el cuadro de chat. Estas van a ser enviadas directamente a los presentadores. Tengan en cuenta también que vamos a tener una sesión de preguntas y respuestas luego de la presentación, y también un cuestionario. En cuanto al cuestionario, vamos a hacerlo luego de la presentación para que todas las personas que participan en el AC puedan responder a las preguntas de este cuestionario. Se va a mostrar en la parte derecha de la pantalla. Finalmente, al final del seminario web y de la sesión de preguntas y respuestas habrá una encuesta sobre

experiencia del usuario con siete preguntas. Por favor, les pedimos que se queden y dediquen esos tres minutos a completar esa encuesta que ayudará a mejorar el programa de creación de capacidades. Muchas gracias. Tijani, tiene la palabra nuevamente.

TIJANI BEN JEMAA: Muchas gracias. Ahora le voy a dar la palabra a los presentadores. Adelante, por favor. Andrei, adelante, por favor.

DAVID CONRAD: Vamos a poner en la pantalla esta presentación. Luego voy a darle la palabra a Andrei Kolesnikov. Finalmente vamos a tener una sesión de preguntas y respuestas, si les parece bien.

TIJANI BEN JEMAA: Sí, adelante.

DAVID CONRAD: Bien. Entonces voy a comenzar. Supongo que tengo el control de la presentación. Como dije, soy David Conrad. Soy el CTO, el director de Tecnología de la ICANN y voy a hablar ahora del traspaso de la clave para la firma de la DNSSEC de la zona raíz. Para comenzar, hay algunas cuestiones básicas a tener en cuenta. Esta charla está relacionada con el sistema de nombres de dominio, en particular con las extensiones de seguridad que se le agregan. El DNSSEC fue definido como una estructura que tiene la capacidad de evitar que los actores malos creen una consulta y que obtengan una respuesta y que se envenene la

memoria caché y que esto se inserte en el caché de los resolutores, y que esto dé como resultado un ataque. Hay formas similares de ataques.

Estas formas de ataque generalmente no se ven en la vida diaria porque hay diferentes maneras de atacar la infraestructura. No obstante, son ataques teóricos que se han demostrado en la práctica. Mi opinión personal es que los ataques que resultan más sencillos son los más difíciles de resolver. Muchas veces se hacen cuando se puede colocar un parche o una aplicación o cuando las contraseñas no son lo suficientemente sólidas. Por esto se agrega las DNSSEC, para evitar este tipo de ataques, para evitar ciertas cuestiones como ataques que se hubieran podido prevenir con el uso del DNSSEC.

DNSSEC son extensiones de seguridad que se definieron en las especificaciones del protocolo del DNS y funcionan de la siguiente manera. Se aplican firmas digitales a los datos del DNS utilizando una jerarquía dentro del DNS que llega a un nivel masivo, a una escala masiva. Se encuentran en la raíz. También en otras zonas pero básicamente aquí estamos hablando de la raíz. Cuando las reglas se rompen, existe la firma de la clave, que sirve para poder firmar los datos. La razón por la cual se hace esta diferencia es que muchas veces no es necesario que se efectúe la KSK o la firma de la clave en la zona raíz.

El DNSSEC tiene dos partes, si se quiere. La firma de la zona, que se realiza a través de los administradores de la zona. Los administradores de los TLD en el espacio de los nuevos gTLD están obligados por contrato a hacerlo. Muchos ccTLD también firman sus zonas. La raíz fue firmada por primera vez en el 2010 y este proceso implica una firma criptográfica y provee una forma de protección si esto se modifica o los datos se

modifican después de la firma, entonces es posible detectar esa modificación realizada. La detección de la modificación se conoce como validación. Esto se efectúa a través de los resolutores recursivos. Estos resolutores también pueden verificar las firmas y los resolutores stub son resolutores que se utilizan a través de aplicaciones de software. Si la validación es exitosa, entonces se da una respuesta a la aplicación. Si la validación no es exitosa, entonces se retorna como respuesta un error. El DNSSEC no evita la modificación de los datos de la zona para quienes son malos actores pero sí se pueden detectar estas modificaciones.

La KSK del DNSSEC en la zona raíz es la clave criptográfica mayor en la jerarquía de validación de las DNSSEC que permite la validación de la información. La forma en la que funciona la validación es que los datos de DNSSEC llegan junto con la firma. El validador verifica todo esto. Se obtiene la firma que se asocia con el principal. Luego se verifica y también se verifica a nivel de la raíz. En la raíz, si no hay una zona principal que pueda verificar la información principal, entonces se verifican todos los resolutores que han hecho la verificación del DNSSEC y se crea lo que se llama un anclaje de confianza. Este anclaje de confianza es una porción pública de la KSK en sí.

Las DNSSEC usan una criptografía métrica. Hay una clave pública y una privada. La privada es la parte de la raíz y la pública se configura en los resolutores. Lo que esto significa es lo siguiente. Si nosotros queremos cambiar la KSK de la zona raíz, significa que vamos a generar un par de llaves públicas y privadas nuevas y vamos a necesitar cambiar la configuración de todos los resolutores en todo el mundo para reflejar esta porción de la clave pública.

Históricamente tuvimos una clave que se generó inicialmente en julio de 2010. Esto se conoce como la KSK 2010. Creamos una nueva KSK allá por el 2017. Esto es lo que va a poner en el ambiente de producción en algún punto durante este año y esto se denomina KSK 2017. El impacto de esto será en los operadores de los servidores recursivos que son generalmente empresas o ISP u operadores de red. Casi todo el mundo puede operar un resolutor. Esos van a tener que, por supuesto, observar sus configuraciones para determinar si las DNSSEC están habilitadas. Si esto es así, tendrán que ver si la información de configuración de la KSK 2017 es correcta y también habrá información de la KSK 2010 o si solamente tienen información sobre la KSK 2010. Si tienen la información de la KSK 2010, solamente esa información, esto indica que hay un problema.

La KSK 2010 es la que actualmente se está utilizando. No había nada antes de esta KSK. La parte pública se configura en los resolutores y da como resultado la clave pública que se utiliza para validar los datos. Si está habilitada la DNSSEC y los resolutores de validación lo hacen, hay un sistema automatizado para actualizar esta clave. La nueva clave, la KSK 2017, va a ser automáticamente insertada en estos datos de configuración. Ustedes ven que dice 2017. Esto no es un error. Fue generado en el 2017 y así se va a llamar. La idea era traspasar la clave en el 2017 pero se tuvo que retrasar el proceso. Se suspendió para poder llevar a cabo ciertas investigaciones. Afortunadamente, vamos a avanzar en esto y se hará en el 2018. Quería aclarar esta posible confusión que pueda surgir con esto del 2017.

¿Cuál es el enfoque del traspaso de la KSK? Esto fue el resultado de una planificación que comenzó allá por el 2013. Cuando firmamos la raíz en

el 2010, dentro de la declaración de prácticas de las DNSSEC, que este es un documento de políticas que se toma en cuenta con la firma del DNSSEC, nosotros nos comprometimos a cambiar la KSK después de cinco años. En realidad, comenzamos con el proceso. Comenzamos a pensar en el cambio, allá por el 2013. Hubo ciertas circunstancias que nos distrajeron en el medio, como por ejemplo fue la transición de las funciones de la IANA. Esta planificación fue suspendida porque todos estábamos trabajando en la transición de la custodia de la IANA. Había muchos de nuestros colegas que por supuesto estaban trabajando en ese tema y cuando la transición de la custodia de la IANA finalizó, también tuvimos que continuar en contacto con el equipo técnico y reanudamos la planificación técnica allá por el 2015.

Debido al estándar que existe para hacer la automatización de estas cuestiones, nosotros tomamos un enfoque de trabajar en forma lenta y segura, teniendo en cuenta el ciclo de actualización normal de la KSK. Utilizamos la KSK para firmar las KSK de la raíz. Toda acción que teníamos que tomar para el traspaso de la KSK se llevó a cabo en forma trimestral. Estas son las normas definidas por el RFC 5011. Nosotros suponemos que no todos los resolutores van a actualizar la clave para tener una actualización automática de la KSK. Si se cambian los resolutores en forma remota, esto poner nerviosas a ciertas personas.

El protocolo se definió. Se decidió utilizar estas reglas. Los puntos importantes a tener en cuenta en el plan original fueron los siguientes. Nosotros creamos la KSK en octubre de 2016. Básicamente, esto fue copiado de las instalaciones que están en la costa oeste. Fueron instaladas en los módulos de seguridad que tienen el mayor nivel de seguridad posible. En febrero del 2017, la nueva clave, la KSK 2017, ya

estaba lista para ser puesta en funcionamiento. Después del 2 de febrero, nosotros comenzamos a hacer una publicación del tema y se hizo de diferentes formas. Esto incluía el estampado de remeras, por ejemplo, la publicación en el sitio web de la IANA y en muchos otros sitios web. En julio de 2017, el proceso se inició y comenzaron las actualizaciones automáticas, lo que implicaba que la KSK iba a ser insertada en los resolutores que estaban configurados para poder aceptar esta actualización automática.

El plan era que en octubre de 2017, nosotros íbamos a comenzar a utilizar la nueva KSK al firmar las llaves de la zona raíz pero, como se debatió oportunamente, nosotros decidimos retrasar el uso de esta zona porque nos dimos cuenta de lo que realmente estaba sucediendo. El plan siguiente fue revocar la clave vieja para que no sea utilizada en el futuro y, en algún punto, todavía no hemos determinado la fecha exacta porque la clave todavía no está siendo implementada, pero finalmente remover esa clave va a ser un proceso automatizado.

Como todos saben, nosotros suspendimos el traspaso de la KSK. Desde ese entonces comenzamos un proceso de restaurar el traspaso. En este punto nuestro plan es que un año después de la planificación del traspaso de la KSK, se use la nueva KSK para firmar la zona raíz en octubre de 2018. Es ahí cuando se va a efectuar la firma para la llave de la zona raíz.

La revocación de la clave de 2010 se realizará un trimestre después. Lo mismo va a ocurrir con la eliminación de la clave porque no hay apuro. Tenemos suficiente tiempo para realizarlo. ¿Por qué actualizamos todos estos puntos? cuando comenzó el proceso de traspaso no había forma

de medir las configuraciones del resolutor. Tampoco sabíamos cuántas personas habían activado todo lo referido a RFC 5011. Confiábamos en el plan de comunicación para garantizar que todos hicieran la actualización de manera adecuada.

Durante el proyecto de traspaso de la KSK surgió un RFC que definía los mecanismos que permitirían medir de qué manera los resolutores se configuraban para poder publicarse. Esto fue realmente sorprendente. La especificación para esta tecnología, el RFC 8145, surgió en 2017. En agosto del 2017 uno de los autores decidió trabajar con Verisign. Verisign opera dos servidores raíz y se decidió ver si había alguna señal de esta publicación de mecanismos de medida. Los datos que obtuvimos resultaron muy confusos. No eran solamente confusos sino que también nos preocupaban. Por eso decidimos pausar el traspaso de la KSK para poder determinar exactamente lo que estaba sucediendo.

Como mencioné, este RFC, que es el 8145, cuyo título es “Conocimiento sobre los anclajes de confianza y su firma”. Perdón, ahí tenemos un gráfico que no quería mostrarles. Se muestra en el gráfico el porcentaje de los resolutores o en realidad se anuncia el KSK del 2010. También voy a publicar en el chat la URL para que ustedes puedan verificar estas estadísticas que se den aquí, que es la publicación de la KSK 2010 y 2017. Veo que Adobe Connect no permite mostrar el gráfico en la pantalla.

Decía entonces que nosotros recibimos allá por septiembre de 2017, un mes antes de utilizar la nueva clave y entrarla en producción, nos dimos cuenta de que había una gran cantidad de resolutores que decían que solamente tenían la KSK 2010, no ambas claves, la KSK 2010 y 2017. En este entonces nosotros asumimos que el porcentaje iba a ser muy bajo.

En ese entonces era del 7%, según lo que decía Verisign. Nosotros, la ICANN, comenzamos a analizar los datos de los servidores a los cuales teníamos acceso. No solo a los que podíamos acceder sino que también pudimos obtener datos de otros servidores raíz que se operaban en California, del consorcio de Internet, entre otros.

Comenzamos a recabar información, a recabar datos y nuestras cifras mostraban algo un poco peor de lo que nos decía Verisign. Lo que era más preocupante era que el porcentaje de resolutores que mostraban solamente la KSK 2010 cada vez era mayor dado que había gente que, con respecto al código 8145, tenían una mala configuración. Este número parecía incrementarse cada vez más. Cuando comenzamos a ver esto nos hicimos algunas preguntas. ¿Qué nos decían los datos? Recuerden que había un código que se había implementado, que no había existido hasta abril de 2017. Era algo muy nuevo. Solo iba a funcionar con resolutores que lo habían implementado y había gente que los había adoptado y también había adoptado las últimas actualizaciones de los resolutores.

Los datos comenzaban a tener sentido. Tuvimos en cuenta las especificaciones. También identificamos algunos errores en algunos resolutores muy conocidos. Esto nos dio la posibilidad de explicar o de darnos cuenta de lo que estaba sucediendo. Comenzamos a tomar en cuenta la información que ya teníamos a nivel de los servidores raíz y tratamos de rastrear qué era lo que creaba estos anuncios con respecto a la configuración de la KSK. En los servidores raíz veíamos las direcciones de IP del resolutor que consultaban al servidor raíz. Desafortunadamente, resultó que el modelo simplista que muchos tenían con respecto al funcionamiento del DNS tenía una aplicación que

comunicaba al resolutor y parecía un tanto raro. Había otros dispositivos que forzaban al avance de la consulta y la dirección IP que obteníamos del resolutor en definitiva no tenía ninguna relación con el que realizaba la consulta o el dispositivo. No podíamos ver el último eslabón de la cadena y teníamos muy poca información para poder identificar la fuente. Es decir, el comienzo de la cadena en el resolutor.

Hablamos con algunos colegas, investigamos cuáles eran las causas de todo esto. Parecía ser que había una máquina virtual que configuraba ciertas cuestiones que atacaba solamente a aquellos que tenían el KSK 2010. Hacía que los resolutores respondieran a esta máquina virtual. Enviaba este anuncio sobre la KSK 2010 pero en realidad no había ningún panorama claro de lo que estaba sucediendo. Continuamos investigando el tema. Como mencioné en el 2017, tuvimos incertidumbre y por eso detuvimos el traspaso. El plan en sí anticipaba algunas cuestiones que tenían que ver con ciertos puntos de verificación o con ciertas respuestas automáticas.

El plan funcionó pero como estábamos luchando o tratando de entender lo que sucedía en ese entonces hicimos lo que la organización tenía que hacer para poder entender lo que estaba sucediendo. Consultamos con la comunidad. Nos pusimos en contacto con expertos del DNS. Tratamos de identificar una forma de avanzar y también preparamos un plan actualizado. Lo presentamos para comentario público. Obtuvimos algunos comentarios, incluso el ALAC hizo comentarios. Esto finalmente dio como resultado un plan revisado. Esta sería la respuesta breve, por así decirlo, en cuanto a este plan. Los datos del código 8145 no pueden ser tenidos en cuenta porque muestran que los resolutores están mal configurados pero no indica cuántos usuarios están detrás de estos

resolutores. Nosotros tenemos que cuidar o tener en cuenta a los usuarios. Eso es lo que nos importa.

En ese punto, veíamos un 25% de consultas al DNS que estaban siendo validadas y dado que esto es un porcentaje bastante bajo teniendo en cuenta la cantidad de resolutores que existen, como por ejemplo los resolutores de Comcast, de Google. Comcast es el proveedor más importante de los Estados Unidos. La consecuencia de esto era que el código 8145 señalaba que había un resolutor mal configurado pero había un sistema o una aplicación que se ejecutaba y probablemente ningún usuario iba a ser afectado por eso. No teníamos manera de comprobar esto.

Uno de los puntos principales en este debate fue que no sabíamos qué mostraban estos datos en relación al impacto que iba a tener con respecto a los usuarios finales. Aquí vemos un gráfico que muestra el informe de los anclajes de confianza de todos los servidores raíz. Vemos que hay un pico. Allí vemos unos 180.000 aproximadamente direcciones de IP únicas. Voy a volver al gráfico anterior.

Como decía entonces, tenemos 180.000. Esto era lo que veíamos y en rojo vemos la cantidad de fuentes que informaban solamente la KSK 2010. En la siguiente diapositiva que, una vez más, no la podemos observar claramente porque no muestra gráfico, muestra el porcentaje. En realidad, estas diapositivas fueron preparadas para una presentación de CERT, que es el equipo de respuestas de emergencias informáticas. Por eso aquí menciona la palabra CERT.

Lo importante es que si la KSK está mal configurada, si solo es la 2010, y avanzamos y firmamos la zona raíz con la KSK 2017, esto va a implicar

que toda resolución que se lleve a cabo a través de los resolutores, no va a funcionar. Va a fallar. Simplemente porque la clave es incorrecta. Nosotros tratamos de abordar este tema consultándolo con la comunidad. Nos comunicamos con los expertos pero la realidad es que sabemos que no vamos a poder llegar a todo el mundo dentro de la comunidad con este plan de traspaso de la KSK. No todo el mundo lo va a entender. El criterio es que si menos del 0,1% de los usuarios finales son impactados o afectados, entonces vamos a considerar que el proceso es exitoso y no vamos a retrasar el traspaso.

La información que tenemos es que se están configurando una serie de resolutores pero esto no nos dice cuántos usuarios finales han sido afectados. El aporte que tuvimos de la comunidad fue algo general porque no tenemos información sobre los usuarios finales, aunque sabemos que los resolutores a gran escala están configurados de manera correcta. Ahora tendríamos que ver qué sucede y saber si el porcentaje está por debajo del 0,1%.

Si uno sabe la respuesta de un resolutor, yo sé que algunos sí, la forma de reconocer la KSK 2017 es la siguiente. Hay una etiqueta que es 20326. Esto debería aparecer en la configuración. El registro de recursos de la clave del DNS se muestra de esta manera. Esto es la criptografía.

El estado actual del sistema. La KSK se cambió en buenas condiciones. El enfoque que nosotros tomamos fue un enfoque lento y cauteloso. Las actualizaciones automáticas funcionan cada 30 días pero también estamos listos desde agosto de 2017. Los sistemas están efectuando las actualizaciones automáticas. Se están configurando para poder implementar la KSK 2017. Podríamos avanzar pero, como dijimos

anteriormente, no lo hicimos. El proceso de traspaso desde el punto de vista de un validador se asume que las DNSSEC están operando o ya configuradas para funcionar. Todos los validadores deberían ya tener la nueva KSK implementada. Si no, lo van a tener que hacer en forma manual.

¿Cómo se puede saber esto? Si un resolutor está validado, se sabe de la siguiente manera. Hay un dominio que es DNSSEC-failed.org. Si ustedes mandan una consulta y les devuelve una dirección IP, esto significa que el DNSSEC no está habilitado. Si obtienen otro mensaje, entonces significa que sí están implementadas. Si obtienen como resultado una dirección de IP significa que la validación no está habilitada.

En un sistema de UNIX o en otros sistemas hay una etiqueta dig que les permite enviar la consulta y allí van a poder ingresar el nombre de dominio o la dirección IP que desean verificar y podrán saber la respuesta. Verán un encabezado y allí podrán ver si está habilitada o no la validación del DNSSEC.

En la siguiente diapositiva pueden ver un ejemplo de una validación de las DNSSEC que no está habilitada. Generalmente nos preguntan cómo sabemos o cómo se sabe si la KSK 2017 está configurada públicamente en el resolutor. Históricamente la respuesta desafortunada es que no se puede saber. No hay forma de saberlo a menos que se tenga acceso a la gestión de los resolutores para poder verificar qué tipo de KSK ha sido configurada. Esto está cambiando con una nueva especificación que es KSK Sentinel, donde hay consultas que se envían y permiten obtener información para saber si la KSK está configurada en los resolutores pero

esto todavía no ha sido plenamente implementado. Probablemente lleve algo de tiempo.

Si tienen acceso al nivel de administración de los resolutores, hay una serie de comandos, dependiendo del resolutor que les pueden indicar si la KSK está implementada o no. Allí pueden ver en pantalla la información de los diferentes enfoques que se pueden tomar. En realidad, no hay manera. Un usuario final no tiene manera de verificar si su resolutor tiene configurada la KSK. Este es un problema desde el momento en que se implementó el DNSSEC.

Esta URL les da información sobre cómo verificar los anclajes de confianza. ¿Qué se debería ver? Si han configurado correctamente la KSK, tendrían que ver dos anclajes de confianza. La KSK 2017, que tiene una identificación de clave que es 20326 y la KSK 2010 cuya identificación es 19036. Luego se va a eliminar la KSK 2010. Todavía no hemos definido exactamente cuándo lo vamos a hacer. Seguramente será en algún punto en el futuro.

¿Cómo se ve esta información? Aquí en las siguientes diapositivas lo pueden ver. Voy a avanzar rápidamente. Aquí mostramos las diferentes formas de visualizar la KSK. Por ejemplo, con Bind lo pueden ver de esta manera. Unbound es un poco más complicado ya que tienen que buscar en la respuesta del DNS para saber cuál es la configuración de la KSK pero aun así pueden obtener esa información. Si ven que ambas KSK están instaladas, no se tienen que preocupar porque es así como debe funcionar. Si no es así, tienen que arreglarlo. ¿De qué manera lo van a hacer? Aquí vemos una URL donde pueden obtener información sobre cómo solucionar el tema.

¿Dónde se consigue la KSK? La oficial está disponible en formato XML en la página web de la IANA. También lo pueden hacer vía DNS. También hay otras vías que quizá sean un poco más comunes porque tienen que ver con la distribución de, por ejemplo, los sistemas operativos como Microsoft Windows. Las actualizaciones de software también van a dar las configuraciones actualizadas y la información actualizada que incluyan la nueva clave.

¿Cuáles son los indicios de que un anclaje de confianza es erróneo o incorrecto? Si no tienen la clave correcta y no utilizan la nueva clave firmada en la zona raíz lo que van a ver es un mensaje de error que va a presentarse como serve fail. Allí tendrán que ver qué es lo que sucede pero, si no ven ninguna señal, probablemente ese sea un buen indicio de que la KSK no ha sido actualizada correctamente. En cuanto al futuro, en algún punto vamos a revocar la KSK 2010 después de que se implemente la KSK 2017 en el 2018, a menos que la comunidad nos indique lo contrario. También habrá otros traspasos de la KSK.

Yo mencioné la declaración de las DNSSEC. Hicimos el traspaso luego de cinco años. La suposición actual es que vamos a hacer el traspaso cada cinco años aproximadamente. Esto es así a menos que la comunidad nos indique lo contrario. Hemos hablado con la comunidad técnica y nos ha dicho que hay que incrementar la frecuencia del traspaso de la KSK para garantizar que la KSK y su infraestructura nos permita cambiar la clave en caso de ser necesario en lugar de tener que hacer continuamente este ejercicio porque, si uno no ejercita algo, cuando realmente lo necesite no va a estar disponible luego.

Hay otros que dicen que el traspaso de la KSK fue una mala idea y que no tendríamos que volver a hacerlo. En este punto creo que la frecuencia correcta para hacerlo es cada cinco años. El 11 de octubre de 2018 vamos a poner el reloj en cero para contar y determinar lo que va a suceder en los próximos cinco años.

Algunas herramientas y recursos que brinda la ICANN son los siguientes. Allí ven una serie de herramientas que pueden utilizar para validar los anclajes de confianza y para conocer sobre el traspaso. Tenemos páginas de información sobre el traspaso. También vemos que están los anclajes de confianza. Hay un software que puede también verificar las validaciones y las actualizaciones en forma periódica. Tenemos un banco de pruebas de actualización para permitir que la gente verifique que los sistemas estén funcionando correctamente. Si visitan este sitio web pueden ver de qué manera funcionan estos bancos de prueba y también tenemos el apoyo del RFC 5011.

Aquí también pueden ver otros recursos de información o educativos de la ICANN. Ahí ven un enlace con información. Una vez más, en relación a las URL, ustedes pueden encontrar aquí información que sea relevante. Con esto voy a darle la palabra ahora a Andrei para que nos cuente un poco sobre la gestión de la KSK en los ccTLD. Andrei, adelante, por favor.

ANDREI KOLESNIKOV: Muchas gracias, David. En primer lugar, quiero decir que para mí es algo muy bueno tener toda esta información en línea a disposición. Creo que es muy bueno también que la ICANN haga tareas de difusión y alcance de manera tal que se haga llegar este mensaje a los operadores de los resolutores.

Yo voy a ser un poco más práctico. Voy a reiterar algunas de las cosas dichas por mi colega. En primer lugar, el DNS es un sistema distribuido y todo comienza con el punto de los nombres de dominio. Al hacerlo, uno entra en la zona raíz. Tenemos TLD que son prácticamente iguales en todas partes. Básicamente, lo que hacen las DNSSEC es lo siguiente. Se las agrega criptográficamente. Se les da una clave por separado. Tenemos dos claves. Una clave para la firma de la clave y otra para la firma de la zona.

Esto es la magia de la criptografía. Yo no soy muy bueno con la criptografía pero sí soy práctico. Por ejemplo, tenemos una ceremonia que se realiza en las sedes de la ICANN y esta ceremonia es como un show en cierto modo. Cuando uno firma la zona se hace una presentación. Están representantes confiables de la comunidad. Son personas elegidas entre personas que no están conectadas a la gestión de la zona raíz justamente.

Para la zona raíz o para los TLD, se eligen a estas personas. Básicamente participan en esta actividad. Hay distintos componentes de la KSK que están involucrados. Si vamos al próximo nivel de la raíz, pasamos al TLD, en 2012 se firmó también la raíz con respecto a los TLD. Esto se realiza en una sala cerrada, bajo llave, sin conexión de Internet, en una computadora que está conectada a un módulo de seguridad de hardware. Básicamente, esto se realiza generando una clave. Luego se la retira en un flash y se sube al resolutor principal para la zona. Luego se implementa, se despliega la clave en el anclaje de confianza.

En todo este sistema se trabaja con los TLD, con la raíz y quienes están a cargo de los nombres de dominio confían en cada TLD. Tenemos un

esquema que es muy bonito pero lo principal es que esto funcione bien y también que funcionen bien los registros de las DNSSEC. A veces se firman muchas zonas y necesitamos este anclaje de confianza que es muy importante. Es muy importante mantener este anclaje de confianza. Básicamente, la firma de la KSK implica toda la infraestructura pero principalmente los resolutores y los anclajes de confianza.

Tenemos a uno de los mejores expertos en DNSSEC con nosotros en esta ocasión, en este seminario web. Russ Mundy está con nosotros. Él es una de las personas que realmente entienden cada detalle de las DNSSEC desde el principio. Yo no he preparado una presentación. Yo soy una persona del entorno técnico pero también soy muy práctico. La idea era darles la mayor cantidad de información posible sobre las DNSSEC a ustedes, a las personas de ALAC y de At-Large, a esta comunidad respecto de este tema y este proceso de la KSK. Es importante entender no solo cómo se hace el traspaso de la KSK y no solo el tema del 2010 sino también que es importante entender cómo todas las DNSSEC funcionan, cómo funciona todo este sistema. Por eso surgió la idea de este seminario.

Dicho esto entonces finaliza mi breve intervención en esta presentación. Si alguien desea ahondar en cuanto a los TLD o a algún tema de mi especialidad me puede contactar con todo gusto. Tijani, dicho esto le doy la palabra. Creo que pasamos a la sesión de preguntas y respuestas. ¿Hola? Tijani, tiene la palabra. Tijani, le doy la palabra.

DAVID CONRAD: Parece que tiene silenciado el micrófono.

ANDREI KOLESNIKOV: Como tenemos a Russ aquí con nosotros, en la sesión, quizá él también pueda responder preguntas de los participantes en este seminario web.

ANDREA GLANDON: ¿Quieren que hagamos la pequeña evaluación?

DAVID CONRAD: Sí. Tenemos un cuestionario breve. Quizá lo podemos hacer ahora. A ver. Creo que Alan está primero en la lista de personas que solicitan la palabra.

ALAN GREENBERG: Gracias. Tengo dos preguntas. Usted mencionó criterios que podrían utilizar para retrotraer este traspaso. ¿Qué significa retrotraer el traspaso? ¿Cuál sería el plazo correspondiente? ¿Es algo que se puede retrotraer? ¿Cuáles son los detalles?

DAVID CONRAD: El plan original definido por la comunidad para el traspaso contenía criterios según los cuales íbamos a retroceder y volver a la KSK 2010 si más de un porcentaje de usuarios se veían negativamente afectados por el traspaso. Esos eran los criterios definidos por la comunidad pero, en retrospectiva, realmente no quedaba muy claro qué significaba esto porque en aquel momento, e incluso hoy, no tenemos una manera sencilla de determinar cuántos usuarios finales se verán impactados por el traspaso de la KSK.

Como dije, esperamos solucionar esto en cierta medida con el proyecto KSK Sentinel. Creo que está en la última ronda de consultas en el IETF y luego será implementado en algunos resolutores. Hubo un tercer resolutor que desafortunadamente implementó otra medida anterior. Esto implicará un tiempo para desplegar e implementar este software y una vez realizado esto podremos tener una mejor idea, un mejor muestreo de los usuarios finales y de sus resolutores de configuración para poder estimar con mayor exactitud cuántos usuarios se verán afectados por la falla del traspaso de la KSK.

¿Qué implica este retroceso? Implica dejar de usar la KSK 2017 para firmar la raíz y volver a usar la KSK 2010 para firmar la raíz. En teoría, esto significaría que habría una o dos zonas mientras podemos identificar si hay un problema y podamos determinar si hace falta hacer esto retroceso porque, como se supone que deben existir ambas claves, pero la mala configuración estaría solo con la clave vieja, entonces, tener solo la clave vieja sería algo relativamente sencillo y sin inconvenientes. Desafortunadamente, debido a cómo funciona el DNS con la memoria caché, etc. sin duda esto sería bastante disruptivo.

Hacer este retroceso es algo que nosotros preferimos evitar, por supuesto. Ese es uno de los motivos por los cuales decidimos suspender el traspaso hasta comprender mejor los datos. También quería decir, porque me olvidé de decirlo en mi presentación, que hay un análisis que realizamos con APNIC y en ese análisis se trata de hacer una correlación entre el RFC 8145 y los datos obtenidos por APNIC con Google Ads y con consultas con habilitación de DNSSEC en sus buscadores.

Nosotros pudimos obtener mediante ese enfoque una información que nos deja mucho más tranquilos dado que las cifras que obtuvimos son menores a 0,05% de resolutores con mala configuración. Perdón. Los usuarios finales tendrían un impacto menor de 0,05%. Eso quise decir, que es menor que el 0,1% que activaría este retroceso.

ALAN GREENBERG: Entonces, en resumen, este retroceso en concepto significa volver hacia atrás mediante un switch que llevaría unas horas. Se recurriría a una memoria caché en poco tiempo, en lugar de un caché a largo plazo.

DAVID CONRAD: Claro. Esto surgiría después de la publicación de la zona con la KSK 2017 y se volvería a la 2010.

ALAN GREENBERG: Tres meses después, hacer un retroceso, significa que quizá no se puede volver atrás. ¿Eso es lo que significa?

DAVID CONRAD: Claro, exactamente. Como Russ está en el seminario web, por favor, corríjame, Russ, si me equivoco.

RUSS MUNDY: *Los intérpretes pedimos disculpas pero el audio de Russ Mundy no tiene el volumen suficiente como para ser interpretado con exactitud.*

Cada usuario final tiene a disposición dos o tres resolutores de DNS. Si ninguno funciona correctamente, quizá la respuesta no venga tan rápidamente pero aun así obtendrían una respuesta.

Los intérpretes pedimos disculpas pero el audio de Russ Mundy no tiene el volumen suficiente como para poder ser interpretado con exactitud en el canal en español.

Los intérpretes pedimos disculpas pero su audio no tiene el volumen suficiente para ser interpretado con exactitud al canal en español.

DAVID CONRAD: Una de las ventajas del DNS es que se pueden predecir cómo va a reaccionar, independientemente de la configuración de los usuarios finales. Como dijo Russ, es difícil ver qué es lo que va a suceder. Olivier, tiene la palabra.

OLIVIER CRÉPIN-LEBLOND: Muchas gracias, David. ¿Me pueden oír?

DAVID CONRAD: Sí.

OLIVIER CRÉPIN-LEBLOND: Tengo tres preguntas breves. Primero, ¿por qué se tiene que hacer el traspaso el 11 de octubre exactamente?

DAVID CONRAD: Cuando la comunidad se sentó a identificar las mejores fechas, teniendo en cuenta la necesidad de hacer el traspaso junto con las ceremonias trimestrales de firma de la zona, básicamente se trató de evitar todo tipo de día feriado, no laboral, fin de semana. Surgió la fecha de 11 de octubre de 2017. Dado que suspendimos el traspaso en esa fecha se decidió posponerlo un año exactamente para simplificar las comunicaciones. Hubo sugerencias de hacer de cuenta que la fecha en realidad siempre fue 2018 y que hubo un error de tipeo en 2017, pero no. esa no fue la razón.

OLIVIER CRÉPIN-LEBLOND: El tema con esta fecha es que es bien entrada la semana. Estamos casi cerca del fin de semana, si uno piensa en el 11 de octubre de 2018. Por eso preguntaba.

Mi segunda pregunta es la siguiente. Usted presentó algunos gráficos. Yo vi la presentación original donde sí se podían ver los gráficos y hay un pico creo que en el 1 de abril o el día antes, el día previo en marzo. Hay un pico de actividad. ¿Qué pasa allí?

DAVID CONRAD: Nosotros lo analizamos. Lo que sucede es lo siguiente. Pido disculpas porque no lo mencioné antes. Lo que sucede es que hay un software de VPN que tenía la KSK original en su software de VPN a la vez. Vimos una serie de direcciones IP con fuente única y eso se debe a que este software de VPN que estaba en máquinas de clientes iba a estar conectado al DNS. Estos resolutores indicaban que tenían solo la KSK 2010. Había muy pocas máquinas en Internet que se conectaban en

distintos lugares y que se mostraban como direcciones de IP únicas. Creemos que ese pico de actividad se debe a que el desarrollador de software de VPN publicó un nuevo código que impactó sobre una gran cantidad de clientes de la VPN que a la vez les hizo ver que había algo que estaba sucediendo.

Las estadísticas en esa época, en esa fecha o en fechas cercanas mostraban el rumbo correcto, indicando que iba descendiendo este pico de actividad y que el número de direcciones IP que tenían esta mala configuración inicialmente estaba entre el 20% y el 22%, lo cual nos inquietaba y creo que entonces la universidad del sur de California investigó y descubrió esta cuestión de la VPN. Se empezó a solucionar el problema y la actividad mejoró.

OLIVIER CRÉPIN-LEBLOND: Mi tercera pregunta es un tanto controversial. Quiero decir lo siguiente. Acabo de volver de una reunión en la cual se realizó una presentación, una reunión de RIPE y se hablaba del DNS y de las DNSSEC. En la presentación se decía que se podía hacer todo con DNS sobre TLS y deshacerse de todo esto de las DNSSEC básicamente. ¿Qué piensa?

DAVID CONRAD: Eso se sugirió en múltiples oportunidades. Personalmente considero que las DNSSEC protegen a los datos en sí, ese viaje, ese tráfico de los datos. El DNS sobre TLS protege el transporte de datos. Esto también se habló en otras oportunidades, con otras medidas de seguridad. Es una tecnología muy interesante pero protege el transporte, no los datos en sí. Personalmente, considero que es mejor proteger los datos pero creo

que deberíamos utilizar ambos. La ventaja es muy significativa en cuanto a lograr una protección más profunda. El DNS en TLS resuelve una serie de problemas pero no todos y no protege la memoria caché como lo hacen las DNSSEC. Quizá le puedo preguntar a Russ si quiere agregar algo al respecto.

RUSS MUNDY: *Los intérpretes pedimos disculpas pero el audio de Russ Mundy no tiene el volumen suficiente para ser interpretado con exactitud al canal en español.*

Los intérpretes pedimos disculpas pero su audio no tiene el volumen suficiente como para ser interpretado con exactitud al canal en español.

Los intérpretes pedimos disculpas pero su audio no tiene el volumen suficiente como para ser interpretado con exactitud al canal en español.

ANDREA GLANDON: Disculpen la interrupción. Por favor, si están utilizando un manos libres, les pedimos que utilicen el auricular del teléfono o que hablen con un poquito más de volumen porque no los podemos oír bien.

RUSS MUNDY: Le pido disculpas. Al final…

Los intérpretes pedimos disculpas pero su audio no tiene el volumen suficiente como para ser interpretado con exactitud al canal en español.

DAVID CONRAD: Quiero agregar que algo que nos facilitan las DNSSEC en contraposición a DNS sobre TLS es un mecanismo que nos protege contra los ataques de denegación de servicio. Las DNSSEC nos dan una respuesta ante una consulta de un nombre que no existe que nos permite reducir las posibilidades o la oportunidad de un tipo de ataque de denegación de servicio que inunda los servidores de nombres con consultas de nombres que no existen. Esto fue implementado recientemente en las DNSSEC, en los resolutores habilitados con DNSSEC, y permite detener o evitar estos ataques o esta manera en particular de ataque de denegación de servicio, sobre todo en los dispositivos de la Internet de las cosas. Con las DNSSEC y esta nueva medida de seguridad es posible filtrar este tipo de ataque a nivel del resolutor o de los resolutores.

DAVID CONRAD: Hadia, tiene la palabra.

HADIA ELMINIAWI: Ahora estamos pasando al traspaso de la KSK. Ya es momento de hacerlo. Han pasado más de cinco años. Esto es una necesidad. Sé que los datos disponibles no son muy tranquilizadores pero de todas maneras me pregunto por qué seguimos dudando acerca de esto.

DAVID CONRAD: Yo creo que seguimos dudando porque estuvimos, por así decirlo, jugando con los motores del avión mientras el avión todavía estaba en vuelo. Hay que ser cauteloso porque si uno tiene dos motores y se le rompe uno, no lo va a pasar muy bien. Cuando la comunidad produjo un plan muy cuidadoso y cauteloso para el traspaso de la KSK, nosotros lo

tomamos en consideración y lo queremos implementar con el mayor cuidado posible. Hay quienes sugieren que tenemos que hacer este traspaso de la KSK con mayor frecuencia por una cuestión de infraestructura. Personalmente, me interesaría algo un tanto diferente, que es un traspaso de algoritmo. Es decir, cambiar los algoritmos, porque tengo mucha confianza en que la infraestructura que generamos resiste a que se vea afectada la clave.

Aun así, puede haber un nuevo ataque que requiera el cambio de un algoritmo y pasar a otro que no sea susceptible de sufrir un tipo de ataque en particular. Además, hay mejores algoritmos de seguridad que se fueron creando desde que se crearon los que estamos utilizando en la actualidad. Yo espero poder cambiar los que estamos usando a uno de estos nuevos algoritmos con mayor seguridad. Alan tiene la palabra.

ALAN GREENBERG: Uno de los comentarios que hizo ALAC fue pedirle a la ICANN que suministrara alguna herramienta o una URL para que alguien pudiera hacer la consulta que usted menciona y verificar si el resolutor que están utilizando tiene habilitadas las DNSSEC. Seguramente, en el mundo en desarrollo esto no es así. Saber que su resolutor no está habilitado para las DNSSEC, en cierto modo nos quita presión en nuestra región. Sin embargo, lo importante es qué hacemos si dice que el resolutor está habilitado para las DNSSEC y uno no sabe si tiene instalada la nueva clave o no. Esperamos que la ICANN nos dé algún tipo de herramienta que no requiera que una persona tenga bagaje técnico para interpretar la respuesta y que nos dé orientación para saber qué hacer en ese punto.

Si uno, como usuario regular, llama a la mesa de ayuda de su ISP y le empieza a preguntar por la KSK, primero la persona que atiende el teléfono no sabrá de lo que estamos hablando. Necesitamos algún tipo de guion o alguna herramienta para que una gran cantidad de usuarios en el mundo, y definitivamente la comunidad de At-Large que tiene acceso a muchas personas, para que los usuarios puedan ver si potencialmente hay un problema. Necesitamos contar con una URL que tenga un mensaje técnico de manera tal que las personas correspondientes sepan qué hacer ante algún tipo de problema o falencia. Me gustaría reabrir este tema y ver si la ICANN puede hacer algo al respecto porque aliviaría ciertas tensiones y nos brindaría cierta orientación también.

DAVID CONRAD: Muchas gracias por la pregunta. Esa pregunta, qué hacer si uno es un usuario final, surgió internamente dentro de la organización en varias ocasiones pero también dentro de la comunidad técnica a la cual hemos consultado. Parte del desafío fue el siguiente. Nosotros en la organización habíamos planificado cómo comunicar esto a los usuarios finales. La comunidad de operadores de red pensó que no sería una buena idea porque se verían bombardeados con preguntas y la persona, por ejemplo, que hacía la pregunta, no podría entender qué es lo que estaba preguntando y aun si lo entendieran, si entendieran la respuesta, no sería suficiente con una de estas preguntas que habíamos planificado en este plan de comunicación.

Preparar una herramienta fue algo que analizamos a nivel interno. En ese momento, el desafío fue el siguiente. Uno puede ver si está

habilitado el validador de DNSSEC pero no se puede ver qué tipo de clave están utilizando. Podemos decirles que están habilitadas las DNSSEC pero, como usted señala, podemos reducir un poco el universo de personas que necesitan hacer una investigación más exhaustiva sobre este tema pero, aun así, seguimos teniendo el problema de algunos ISP y de sus configuraciones y qué tipo de configuración están utilizando o cualquier otro tipo de configuraciones con habilitación de las DNSSEC. Con lo cual, los usuarios finales tendrían que llamar a sus ISP y formular estas preguntas que en muchas ocasiones son incómodas para los ISP y se cansan de recibir estas preguntas rápidamente. Tenemos que ver qué hacemos si vemos que el ISP está haciendo lo correcto en cuanto a la validación pero uno no quiere incomodarlo con estas preguntas. Estamos tratando de ver cómo resolverlo.

ALAN GREENBERG: En Panamá vamos a tener una sesión para hablar sobre este tema.

DAVID CONRAD: Me parece una muy buena idea. Tiene la palabra Andrei.

ANDREI KOLESNIKOV: Tengo una pregunta. Esto es como un problema doble. Tenemos material que pasa por el resolutor. Después también tenemos una cuestión de criptografía y una cuestión de algoritmos.

DAVID CONRAD: Creo que es lo último que usted mencionó. Hay que entender, por lo menos, o eso es lo que yo entiendo según el algoritmo que se está

utilizando en este momento. Es muy, muy poco probable que se vea comprometido con la tecnología que conocemos actualmente. Sin embargo, este RSA es vulnerable a quantum crypto, a ese tipo de problemas. Uno de los desafíos con el algoritmo existente es que las firmas son realmente muy, muy grandes. Con lo cual, es más difícil y uno tiene paquetes más grandes en consecuencia, lo cual genera problemas, sobre todo con IPv6.

La idea es pasar a un nuevo algoritmo que tenga mejores características en cuanto a la resistencia a problemas criptografías pero que también tenga firmas más pequeñas, mucho más pequeñas. Que sean por lo menos de la mitad del tamaño de las firmas actuales. Eso facilitaría las cosas desde una perspectiva operativa.

TIJANI BEN JEMAA: En este momento no hay más preguntas. Le voy a pedir a Andrea, por favor, que pase a las preguntas sobre esta sesión de capacitación.

ANDREA GLANDON: La primera pregunta es la siguiente. La vemos en pantalla. ¿Por qué es importante rotar la llave o hacer el traspaso? Pueden escribir sus respuestas en ese espacio en blanco. Luego pueden presionar “Enviar”. David, si usted quiere, podemos ir repasando las respuestas. Si usted nos puede indicar cuál es la correcta. David, ¿puede ver las respuestas?

DAVID CONRAD: Sí, las veo. Tenemos más respuestas que están surgiendo pero sí, la seguridad del DNS, cuestiones de seguridad. La motivación es cumplir

con la directiva de la comunidad de cambiar cada cinco años. Hay una respuesta en francés también. Para evitar cualquier cosa. Yo indicaría ejercitar o practicar con la infraestructura en caso de que necesitemos hacer este traspaso de la clave, aunque también es bueno poder cambiar el algoritmo. De igual modo, cambiar una clave, por ejemplo, una clave de acceso con frecuencia se considera una buena práctica de seguridad.

ANDREA GLANDON: Muy bien. Vamos a pasar a la próxima pregunta que dice: ¿Qué previenen las DNSSEC? Pueden escribir sus respuestas en ese casillero en blanco que está debajo de la pregunta y luego enviar la respuesta. Usted, David, puede ir viendo las respuestas que se van publicando. Después nos puede indicar cuál es la respuesta correcta. Parece que tenemos tres respuestas por ahora, David.

DAVID CONRAD: Ahí surgió una más. Parece que tenemos cinco respuestas.

ANDREA GLANDON: Vamos a repasar las respuestas.

DAVID CONRAD: Tenemos envenenamiento de la memoria caché, como un riesgo. Algo en francés, supongo. Luego las DNSSEC protegen los datos, evitan la alteración de los datos. Yo estaría de acuerdo con esta última respuesta que acabo de leer, que protege a los datos en sí y evita su manipulación. También se evita el envenenamiento de la memoria caché. La respuesta

que dice que es algo malo, que nos protege de algo malo, por supuesto es válida.

ANDREA GLANDON: Muchas gracias. Con esto creo que terminamos las preguntas sobre la presentación. Tijani, ¿quiere dar por finalizada esta teleconferencia?

TIJANI BEN JEMAA: Sí, muchas gracias, Andrea. Muchas gracias. Ahora vamos a pasar a la encuesta sobre este seminario web.

ANDREA GLANDON: Muy bien. Tenemos la encuesta en pantalla. Primera pregunta: ¿Qué le pareció el horario de este seminario web a las 21:00 UTC? ¿Le pareció demasiado temprano, bien o demasiado tarde?

Pasamos a la próxima pregunta de la encuesta. ¿Qué le pareció la tecnología utilizada en el seminario web? ¿Muy bien, bien, suficiente, mal o muy mal?

Tercera pregunta. ¿Los presentadores demostraron dominio del tema? ¿Muy fuerte, fuerte, suficiente, débil o extremadamente débil? Es lo que dice en pantalla.

Próxima pregunta. ¿Está satisfecho con el seminario web? Extremadamente satisfecho, satisfecho, moderadamente satisfecho, ligeramente satisfecho o no estoy satisfecho.

Próxima pregunta. ¿En qué región vive actualmente? África, Asia, Australia y las islas del Pacífico, Europa, América Latina y el Caribe o Norteamérica.

Próxima pregunta. ¿Cuántos años de experiencia tiene la comunidad de la ICANN? Menos de 1 año, de 1 a 3 años, de 3 a 5 años, de 5 a 10 años, más de 10 años.

La última pregunta es: ¿Qué temas le gustaría que tratáramos en futuros seminarios web? Tienen un casillero en blanco para escribir sus respuestas. Luego la pueden enviar.

Gracias, Tijani. Estas son todas las preguntas de evaluación y de la encuesta sobre el seminario web.

TIJANI BEN JEMAA: Muchas gracias, Andrea. Esta pregunta es importante. Todas las preguntas son importantes. Si no las respondieron ahora en el Adobe Connect, por favor, envíennos sugerencias de temas para futuros seminarios web que sirven para que nosotros organicemos más sesiones dentro de este programa de creación de capacidades. Gracias a todos. Gracias a David por esta presentación. Gracias a los demás presentadores, a nuestro maravilloso personal, a nuestros intérpretes y a todos ustedes por participar. Gracias a todos. Damos por finalizado este seminario web. Muchas gracias a todos.

ANDREA GLANDON: Esta sesión ha concluido. Recuerden desconectar todas sus líneas. Muchas gracias. Buen resto de la jornada para todos. Gracias.

[FIN DE LA TRANSCRIPCIÓN]