ICANN77 | Foro sobre políticas – Sesión conjunta: ALAC y SSAC
Jueves, 15 de junio de 2023 – 13:45 a 15:00 DCA

YEŞİM SAĞLAM: Buenas tardes a todos. Voy a tomar la palabra y quiero darles la bienvenida a esta reunión de ALAC con SSAC. Tenemos que iniciar la grabación. ¿Quieren comenzar, por favor? Vamos a comenzar esta sesión. Damos inicio a la grabación.

Hola. Bienvenidos a esta reunión conjunta de ALAC y el SSAC. Mi nombre es Yeşim Sağlam y soy la coordinadora de participación remota para esta sesión. Tengan en cuenta que esta sesión está siendo grabada y que se rige por los estándares de conducta esperados de la ICANN.

Durante esta sesión las preguntas y los comentarios presentados en el chat solamente se leerán en voz alta si se establecen en la forma adecuada, como se indica en el chat. Voy a leer las preguntas y los comentarios en voz alta durante el tiempo establecido por el presidente o el moderador de la sesión.

La interpretación para esta sesión será en inglés, español y francés. Hagan clic en el icono de interpretación en Zoom y seleccionen el idioma en el que desean escuchar la sesión. Si desean tomar la palabra, levanten la mano en la sala de Zoom y una vez que el facilitador de la sesión mencione su nombre, pueden activar su micrófono y hablar. Antes de hablar asegúrense de haber seleccionado

el idioma en el cual hablarán en el menú de interpretación. Digan su nombre para los registros y el idioma en el que desean hablar si no hablarán en inglés. Al hablar recuerden silenciar todos los otros dispositivos y notificaciones. Hablen claramente y a una velocidad razonable para permitir una interpretación adecuada.

Esta sesión incluye transcripción en tiempo real automatizada. Tengan en cuenta que esta transcripción no es oficial ni autorizada. Para ver la transcripción en tiempo real hagan clic en el botón de Closed Caption en la barra de herramientas de Zoom. Para garantizar la transparencia de la participación en el modelo de múltiples partes interesadas de la ICANN solicitamos que se conecten a las sesiones de Zoom utilizando el nombre completo que incluya el nombre y el apellido. Serán eliminados de la sesión si no se conectan utilizando el nombre completo. Ahora sí, le doy la palabra a Joanna Kulesza, vicepresidenta de ALAC. Gracias.

JOANNA KULESZA: Muchas gracias, Yeşim. Gracias a todos por participar en esta sesión conjunta tradicional entre ALAC y el SSAC. Si están mirando la agenda y se ven un poco confundidos, yo no soy Jonathan Zuck. Sé que se sorprenden un poquito. Muy brevemente, estoy aquí para presentar a nuestros invitados. Estoy muy contenta de estar acompañada de los enlaces del SSAC. Entiendo que Andrei Kolesnikov está en línea. De ser así, quiero compartir esta sesión con él para que nos dé una introducción de lo que se espera y cuáles son los otros temas de interés que esperamos debatir hoy. Andrei, ¿puede tomar la palabra?

ANDREI KOLESNIKOV: Hola. Soy Andrei Kolesnikov. Espero que me puedan escuchar. Quizá incluso me pueden ver porque apagué la cámara por un momento porque tengo poco ancho de banda. Vamos a comenzar con nuestra reunión de ALAC y SSAC. No sé cuánto tiempo ha pasado desde que comenzó la primera reunión pero es una buena tradición. Mantengámosla. Vamos a pasar a la agenda directamente. Esta sesión estará estructurada de la misma manera. Habrá comentarios de apertura de parte de Jonathan y Rod, y luego varios temas establecidos con respecto a los grupos de trabajo. Luego habrá un momento para comentarios de cierre. No le voy a dedicar mucho tiempo a esto. Le voy a dar ahora sí la palabra a Jonathan y a Rod. Muchas gracias.

ROD RASMUSSEN: Muchas gracias, Andrei. Muchas gracias a ALAC por establecer este espacio para nosotros. Siempre es una reunión muy interesante y muy útil. Dentro de las reuniones de la ICANN es agradable reunirse y actualizarse sobre las iniciativas porque tenemos mucha superposición. Sé que hay nuevos en esta sala. Quiero asegurarles que el Comité Asesor de Seguridad y Estabilidad asesora a la junta directiva de la ICANN sobre una enorme cantidad de temas. Hablamos de la seguridad y la estabilidad de Internet. En general, esto se superpone con las cuestiones de los usuarios finales, la experiencia que tiene la gente cuando utiliza Internet. Muchas de las iniciativas en las que está trabajando ALAC las estamos trabajando nosotros también y nos encontramos a menudo alineados en puntos de vista y otras veces no.

por lo tanto, es muy bueno tener estas conversaciones. Podemos entrar en los detalles más técnicos de las preguntas que ustedes pueden tener, quizá no tienen la experiencia o no tienen la cantidad de expertos. Aquí hay muchos expertos en ALAC, claro. A Jonathan lo excluimos.

Quería darles entonces un poco de contexto. Vamos a hablar de una cantidad de temas sobre los cuales les daré la palabra a los miembros del SSAC, las personas que están en nuestro comité. Quiero recordarles a los miembros de nuestro comité, también lo hago yo, que hablen lenta y claramente para que todo esto se pueda interpretar adecuadamente. Tenemos personal técnico aquí que tiene la tendencia a hablar muy rápido. Vamos a la siguiente diapositiva.

Les voy a solicitar que sean un poco indulgentes y que salteemos un par de diapositivas y que pasemos a la sección de coalición de nombres. Adelante. Una más. Ahí estamos. Ahora le voy a dar la palabra a Matt Thomas, porque él se tiene que ir rápidamente y luego volveré yo a hablar de otros temas. Le doy entonces la palabra a Matt.

MATT THOMAS: Hola a todos. Disculpas por no poder estar en persona. Tengo algunos conflictos personales esta semana. Me llamo Matt Thomas y soy uno de los copresidentes del proyecto de análisis de colisión de nombres junto con Suzanne Wolf. Seguramente ustedes están familiarizados con el trabajo de colisión de nombres, que está presente desde hace años. Hemos dado varias lecturas al ALAC en las últimas reuniones de

la ICANN pero quería solamente dar una actualización breve el día de hoy.

En líneas generales, el proyecto del NCAP está buscando insertar una serie de cuestiones y dar asesoramiento a la junta de la ICANN respecto de aquellos temas que tienen que ver con la colisión de nombres. Hay un aspecto específico de asesoramiento sobre las cadenas de caracteres no delegadas, que son HOME, CORP y MAIL.

Hay nueve preguntas que han sido presentadas por la junta. El grupo ha estado trabajando con la comunidad en los últimos años de una manera inclusiva. Son unos 25 miembros de los grupos de discusión y 14 miembros de los grupos del SSAC. Son todos ellos parte del esfuerzo. En este momento estamos considerando casi finalizando el estudio NCAP que consiste en cinco entregables, uno de los cuales fue las preguntas de la junta que mencioné anteriormente.

También tiene que ver con tres informes por separado. El primero de los cuales es un estudio de caso sobre las cadenas de caracteres en colisión que considera CORP, HOME y MAIL además de internal, LAN y local. El estudio se realizó utilizando datos de consultas de DNS y de los servidores A a J durante varios años. Esto nos permite destacar los cambios que han ocurrido en el DNS con relación a estas cadenas de caracteres y las propiedades de sus colisiones de nombres. Esto ya se completó. Está puesto para comentario público. El grupo de discusión ha tenido consenso en este informe.

El segundo informe es un estudio de perspectiva sobre las consultas de DNS para TLD no existentes y este informe fue importante porque nos

permitió considerar los distintos puntos en la jerarquía del DNS para así comprender cuáles son las limitaciones y dónde se encuentran esas limitaciones cuando consideramos los datos de DNS que se utilizan para analizar los riesgos de colisión de nombres. Este informe también está listo para comentario público y ha generado consenso dentro del grupo de debate.

Lo que no tenemos aquí, en esta página, es el tercer informe, que está siendo realizado por los investigadores técnicos contratados por la ICANN para dar apoyo al estudio NCAP2. Ese estudio analizó los informes de colisión de nombres recibidos por la ICANN desde el año 2012 hasta el presente, y permite hacer un análisis de curso. Esto también se grupo de ha finalizado. No está para comentario público pero será parte del quinto entregable que debo mencionar. Eso es el informe del estudio dos, que básicamente se trata de un informe que reúne esos tres informes independientes, las preguntas de la junta y presenta, esperamos nosotros, un conjunto de informaciones relevantes a la junta de la ICANN en cuanto a cuál es la percepción que hay sobre la colisión de nombres y qué se debe hacer de cara al futuro.

Para destacar entonces algunos de los hallazgos principales, el grupo de debate ha identificado que las colisiones de nombres continúan siendo un problema fundamental que existe en el DNS y que una gran cantidad de los problemas de colisiones de nombres surgen de cuestiones como los protocolos de descubrimiento de servicio de DNS. El grupo de discusión también ha hablado sobre unas mediciones denominadas diagnósticos críticos para describir cuantitativamente

los riesgos potenciales vinculados con una cadena de caracteres. Hablaremos sobre estos CDM en breve.

Lo importante que ustedes deben entender aquí es que esos CDM aumentan en volumen y en diversidad. La diversidad significa varias dimensiones de cuestiones como la cantidad de redes o dominios de segundo nivel o algo parecido. La mitigación y la remediación es más problemática. El impacto para un daño potencial es alto también. Quiero destacar también que hemos identificado en los grupos de debate que hay oportunidades para que las plataformas de mediciones sean extendidas para ayudar a los solicitantes a presentar sus solicitudes y que puedan estar más informados sobre los riesgos potenciales de colisiones de nombres para ciertas cadenas de caracteres que quieren solicitar.

Algunas de las mediciones críticas que el grupo ha decidido conversar también surgen de algunas de las mediciones que se utilizaron en el año 2012 por el grupo Jazz y otros. Estas mediciones colectivamente analizan el volumen y la diversidad de las consultas que tienen que ver con las IP y la distribución de ASN y otros problemas de las consultas de DNS como la diversidad de qtype, la cantidad de etiquetas y requiere también incluir un componente cuantitativo que analiza algunos descubrimientos anticuados sobre la colisión de nombres que pueden estar incluidos en el DNS de dominio público y cuál es el daño potencial que podrían generar debido a la naturaleza de estas consultas. Siguiente diapositiva, por favor.

El objetivo del estudio dos es garantizar que las colisiones de nombres se puedan evaluar y para que esto pueda ocurrir debemos hacer que

las colisiones de nombres sean visibles. Una de las cuestiones que ha notado el grupo de discusión es que hay una brecha técnica desde el 2012 hasta el presente. El ecosistema del DNS ha cambiado sustancialmente y hemos visto la introducción de algunos resolutores públicos recursivos y algunas cuestiones como de protocolo como la minimización de queue name, el NX domain cut, todos los cuales impedían la observación o las capacidades en la raíz para realizar esa observación. Para poder hacerlo, el flujo de trabajo propuesto ha establecido desviarse pero, de todos modos, estar en la esfera de la ronda de 2012 que permita que las colisiones de nombres puedan ser tratadas de un modo más sostenible y determinista. Siguiente diapositiva, por favor.

Aquí vemos cómo se vería este flujo de trabajo a un alto nivel. Una de las cuestiones importantes que ven en este gráfico es que hay cuatro subastas presentes. Una de las cuestiones a las que le ha dedicado mucho tiempo el grupo es que debe haber una posibilidad de que las solicitudes y los solicitantes no se estanquen en una situación en el limbo, como CORP, HOME y MAIL. El flujo de trabajo ahora propone cuatro oportunidades diferentes para que esas solicitudes sean retiradas o finalizadas.

En general, el flujo de trabajo comienza con el solicitante que decide qué tipo de cadena de caracteres quiere solicitar. Como dije antes, hemos dicho que hay oportunidades para que haya mediciones de plataformas existentes que se desarrollen como por ejemplo el programa ITHI, que se ha extendido, y hacer que esos datos estén disponibles antes de la presentación de las solicitudes y que al menos

se pueda tener una forma de verificar si esto puede resultar problemático. Luego, el solicitante presenta su solicitud y comienza el proceso. El proceso pasa luego a la sección que está en color violeta y el equipo de revisión técnica realiza su propia evaluación estática. En la próxima diapositiva veremos que este grupo utiliza los datos disponibles públicamente para poder hacer una evaluación inicial para determinar si hay riesgos de colisiones y cuál es el impacto para esa cadena de caracteres en particular.

Si se trata de un alto riesgo, y el solicitante no quiere proceder, se ofrece una oportunidad. De lo contrario, la cadena de caracteres se delega al grupo de sistema de servidores y se planea que el control del servidor autoritativo sea precisamente controlado por un tercero neutral durante una fase denominada evaluación de colisión pasiva. En ese caso el TLD seguirá retornando una respuesta de que no hay datos. Ahora el equipo del TRT puede realizar una recolección de datos de DNS para esa cadena de caracteres. Esa recolección de datos también incluye algunos de los problemas técnicos que mencioné antes, como la minimización de queue name, donde hay ciertos aspectos de los datos del DNS que ahora son más ricos y contienen información para permitir una evaluación más adecuada de la colisión de nombres.

A medida que avanza ese periodo de tiempo durante el [PCA], si hay algo que identifica el TRT se ofrecerá una oportunidad para el solicitante nuevamente, antes de entrar a la fase final de la evaluación, que se denomina la evaluación de colisión activa. Esta evaluación en lugar de retornar una respuesta no existente para la cadena de

caracteres mostrará una dirección IP ruteable donde el TRT podrá efectivamente loguear y monitorear los intentos de conexión y entender un poco mejor cuáles son los tipos de servicios, sistemas y software que potencialmente pueden utilizar esa cadena de caracteres para informar un poco mejor los riesgos de evaluación de colisión de nombres.

De nuevo, aquí se ofrece una opción para las evaluaciones que puedan identificar el riesgo potencial pero el TRT va a establecer de todos modos un paquete de recomendaciones, las va a enviar a la junta directiva y una vez que la junta tome esas decisiones, el TRT dará su garantía al solicitante. Siguiente diapositiva.

Como dije antes, el equipo de revisión técnico con un tercero son las características más importantes de este flujo de trabajo. El TRT es un grupo de gente que deben tener una profunda comprensión del DNS y deben entender también cómo funciona la infraestructura de Internet y de qué manera hay una interfaz entre el DNS y las aplicaciones y los servicios. Deberán poder entender cuáles son esas mediciones de diagnóstico que mencionamos antes y de qué manera incluir esto en una evaluación de riesgo.

Nosotros anticipamos que van a tener cuatro responsabilidades principales. Eso es evaluar la colisión de nombres, documentar los hallazgos y recomendaciones. También evaluar potencialmente cualquier plan de corrección, remediación, y también trabajar en las funciones de respuestas de emergencia. Similarmente van a estar los proveedores de servicios neutrales, que puede ser un ente separado del TRT. Nuevamente, esto es parte del detalle de implementación.

Todas las responsabilidades serían operar en ese entorno de evaluación de colisiones tanto activas como pasivas y haciendo esa evaluación para el TRT. Nuevamente, también con las funciones de repuestas de emergencia.

Debo señalar que el grupo de discusiones está en el momento de hacer sus hallazgos y recomendaciones. Estamos felices de tener nuevas personas uniéndose a este grupo si usted está interesado y quiere información para unirse al grupo, aquí estamos. Siempre pueden acudir a mí. Con gusto podré conversar aparte con cualquiera que lo desee. Estoy listo para sus preguntas.

ROD RASMUSSEN: Gracias. Estamos listos. ¿Alguna pregunta? Jonathan, adelante.

JONATHAN ZUCK: Voy a hacer una pregunta inexperta si me lo permiten. Estoy fascinado con este concepto de evaluación de riesgo. Veo que hay diferentes niveles de responsabilidad para un solicitante en base al riesgo preevaluado. Está como separado. Eso los ayuda a decidir si solicitan esto o no. una vez que lo hacen, entonces el conjunto de responsabilidades es el mismo. ¿Hay como un umbral o es un trabajo cuantitativo que se hace diciendo que usted tiene que hacer esto si está en este nivel de riesgo?

MATT THOMAS: Es una muy buena pregunta pero lamentablemente con las medidas cuantitativas no existe un número mágico para las discusiones para decir que por encima de esta cantidad de consultas o de CDM estás en este o en aquel conjunto. Lamentablemente es más que nada cualitativo que cuantitativo y que requiere las experticias del TRT para emitir ese juicio.

ROD RASMUSSEN: ¿Tenemos alguna otra pregunta? Muy bien. Como dijo Matt, estamos llegando al final. Sería genial tener más personas revisando esto y dando sus aportes pero es tarde. Tendrían que ponerse al día muy rápido. Estas son las mismas diapositivas que teníamos la última vez. El NCAP es muy importante. Quiero asegurarme de que todos estén anuentes de dónde estamos. Tuvimos una excelente reunión aquí, en D.C. Estamos buscando tener un cara a cara. Tuvimos muy buen progreso y queremos replicar la experiencia para poder lanzar. Listos para que otros puedan hacer cualquier lanzamiento que tengan que hacer.

Gracias, Matt. Podríamos ahora respaldar esto y volver a la parte de la automatización del DS. Voy a darle la palabra a Peter. Peter, si por favor nos puedes resaltar un poquito esto. Veo que son las mismas diapositivas de la vez pasada. Si puedes decirnos qué es lo que sigue.

PETER THOMASSEN: Peter Thomassen, de SSAC. Esto se está presentando directamente desde Google slides porque no parecen ser los más actualizados pero

podría presentar con estos también. Es solo que es un poco difícil volver a cargar la presentación.

ROD RASMUSSEN: Tendríamos que ir con lo que tenemos frente a nosotros.

PETER THOMASSEN: Muy bien. Como ya hemos discutido múltiples veces en este foro, cuando se tiene un dominio que tiene DNSSEC y se rotan las llaves, especialmente cuando se intercambian las llaves, es importante que se haga el cambio también con el dominio. Hay un intercambio entre el registrante y el registratario cuando el registrante también es el proveedor de DNS para ese dominio, pero si ese no es el caso alguien tiene que darle esa noticia a las distintas partes. El proceso es bastante exitoso.

El 40% de los registratarios tienen éxito. Lo que se necesita es mayor automatización. Voy a hablar más de eso en un momento. En la siguiente diapositiva tenemos un diagrama que muestra exactamente eso. En la parte de arriba tienen al padre, en la parte de abajo el dependiente o el hijo. Cuando hay seguridad del dominio, luego vemos también cuando el operador no es el mismo que el registratario, vemos que se le piden los detalles al operador y se le pasan al registratario. Luego hay una interfaz con el revendedor. Luego eso se le pasa al servidor de TLD. La dificultad aquí está en ese paso intermedio donde se da esa acción intermedia. Siguiente diapositiva.

Hay algo de automatización que ya está ahí. Hay algunos ccTLD que tienen algo de automatización implementada. La forma en como funciona es que el operador de DNS del hijo trabaja haciendo este intercambio y se hace lo que se llama el escaneado de CDS. Ese escaneado tiene dos problemas.

Primero, el tiempo de convergencia toma como más o menos un día. No se sabe inmediatamente a qué hora se va a hacer el cambio. Sabemos que toma un día o algo así, dependiendo de cuál sea el intervalo de escaneo y en qué día se va a hacer efectivo. El segundo problema es un problema de escalado. Cuanto más CDS busque el padre en el hijo, dependiendo de cuántos dominios tengan, tendríamos que escanear todos esos a diario a menos que ese número aumente. No parece ser un problema práctico hasta ahora pero viendo los números de los registros de ccTLD ellos dicen que no tienen muchas preocupaciones en cuanto al escalamiento pero a futuro podría ser un problema si la gente desea que se haga el escaneo más frecuentemente.

Una forma de mitigar esto sería mejorar los escaneos que se dan a diario teniendo como una especie de gatillo que desencadene esos escaneos. Ahora pongo un registro CDS y ya no tienes que esperar a que el temporizador marque que se haga el escaneado hasta mañana a la noche. Algo similar existe para la réplica de servidores DNS. Se tendrían que desarrollar los diferentes software para lograr esto y eso está en una fase de desarrollo.

Luego, adicionalmente, en el modelo RRR hay dos partes. Una es el registratario y otra es el registrador. Ambos podrían buscar los

registros CDS de la cuenta hija y tratar de buscar eso a través del EPP, y buscar los registros de la cuenta madre y buscar la forma en que se sincronicen. Eso es algo un poco un reto pero depende de quién hace el escaneo y al parecer se hace de manera más natural en uno de los modelos cuando el registrador hace el escaneo. Parece ser el enfoque más fácil, más fluido pero también hay varios ccTLD que pueden hacer el escaneo. Vamos a decir que hay un dominio y que quien tiene el nombre de dominio puede hacer el escaneo. Entonces tendrías dos escaneos y esas dos partes tendrían que ponerse de acuerdo en quién sería la que hace el escaneo. Lo que estoy tratando de decir es que, aunque suene bien que el enfoque de escaneo es bueno, siempre hay que ver los detalles.

Muy bien. Aquí vemos un diagrama que muestra cómo se simplifica la situación cuando se tiene ese tipo de escaneo. Como pueden ver, la etapa intermedia entre el padre y el hijo con el registrador, pueden ver cómo se puede hacer también el escaneo de manera directa y se pueden descubrir los registros de CDS desde el registrador y también en el servidor TLD. Eso no es algo que esté soportado por todos los registradores y puede pasar que uno quede sin sincronizarse.

Lo mismo pasa con el escaneo del registrador. El registrador usualmente es la parte que recibe la nueva información del DS. Ese escaneo, que es la flecha número dos aquí, vemos cómo se busca que el registrador obtenga la misma información del operador de DNS y todos los pasos subsiguientes que tienen que ver con que el registrador pase esa información al registro y lo demás seguir igual. Siguiente diapositiva, por favor.

Tenemos algunas posiciones preliminares en el SSAC sobre este tema y, como dije, esto es muy preliminar y podríamos dar algunos detalles la próxima semana con los informes, idealmente antes de la próxima reunión de la ICANN en octubre en Hamburgo. Las posiciones preliminares son que los DNS son difíciles de configurar para las personas. Algunas personas no lo hacen de manera exitosa y por eso es importante que se dé la automatización de DS, especialmente aquellos que tienen una funcionalidad requerida y otras cosas. Aunque los registradores pueden tratar de hacer eso, y podríamos pensar en la automatización de los DS, también tendríamos que ver cómo pueden apoyar la participación en otros procesos que tengan que ver, por ejemplo, con el enfoque de notificación que expliqué antes.

Sería bueno tratar de fomentar eso y también hay dominios que no están bajo TLD o ccTLD, bajo la autoridad de estos sino de otros y sabemos que eso puede ser para otros RRR también. Como dije, si el escaneo lo hace el registrador, tenemos aquí una especie de acuerdo pero hay algunos que ya hacen el escaneo y eso no debe ser considerado un paso atrás. De hecho, sería excelente si los registradores pudiesen incluir el apoyo de los DNS en sus servidores y así los padres, que saben que están haciendo el control pueden ayudar a los registradores, especialmente dado que está aumentando su capacidad.

Eso es lo que puedo decir sobre las actualizaciones de CDS. La parte de notificaciones, de manera interesante, también involucra que los operadores de DNS también los manden. Los envían a un número de entidades que podrían estar afectadas por esta recomendación. Una

vez que se les haya dado el soporte, que manden los mensajes. Si hay un cambio de llave que requiere que se actualicen los registros de DNS, que se anuncie. Habría que hacer esa recomendación pero sabemos que todavía no se puede actuar sobre ello. Creo que esas son todas las diapositivas que tenía. Si alguien tiene alguna pregunta, estoy listo para responderles.

ROD RASMUSSEN: ¿Alguna pregunta? ¿No hay preguntas en Zoom? Jim.

JAMES GALVIN: Solo quería mencionar que no sé si ALAC tiene una posición per se sobre las cosas que están relacionadas con el DNSSEC pero sí quisiera mencionar que ALAC ha considerado esto y este tema con los registros de DS que afectan a los usuarios, a los registradores y su capacidad de despegar la DNS Act. Sé que a veces estas cosas pueden parecer supertécnicas e inmediatamente uno no necesariamente se percata de lo que está sucediendo pero sí quisiera que el ALAC se tomara un tiempo para pensar en esto porque tenemos personas como Peter y otros en el grupo de trabajo que con gusto podrían explicarlo un poco más a fondo para recibir los aportes de ustedes y saber cómo se sienten respecto al trabajo realizado y que se consideren para saber si quieren o no tener un rol en todo esto, pero no querría hablar de parte de SSAC.

ROD RASMUSSEN: Agregando a lo que dijo Jim, tuvimos el taller de DNSSEC. No sé cuántos saben que lo hacemos pero lo hacemos. En cada reunión de la ICANN tenemos un taller. Es formato de políticas, medio día, y este año se dedicó completamente a esto pero también para poner en contexto este tema porque estamos invirtiendo tanto tiempo y esfuerzo en lidiar con este tema tan operacional y tiene que ver con que estamos tratando de completar las bases de DNSSEC y hacer que esto sea un servicio operacional porque hay otras cosas que dependen de ello. Este es ese tipo de cosas que pueden dejar pendiente la adaptación del DNSSEC. Muchos negocios y otras personas que quieren crear servicios nuevos podrían beneficiarse de una criptografía que sea universalmente aceptada y que pueda interoperarse entre diferentes islotes que sean ya de confianza, por decirlo así, en el mundo. Eso sería desde la perspectiva gubernamental y técnica. Si hay algo que cumple con eso es el DNSSEC.

Indistintamente de cuánto tiempo trabajemos en esto, creo que terminar estos temas es importante para poder tener esos servicios que sean confiables y que los gobiernos utilicen para interoperar entre ellos, que utilizan las empresas para que todos podamos hacer dinero vendiendo cosas que están basadas en estos servicios. Les exhorto a que en su tiempo libre lo repasen. Grabamos estas sesiones y hemos puesto todo como en perspectiva este año. Por favor, échenle un vistazo y hablen con las personas de SSAC, especialmente con Jacques, que está aquí. Está haciendo cosas increíbles en Canadá con las identidades digitales y diferentes cosas que se pueden utilizar para interactuar los unos con los otros utilizando la licencia de conducir y es por eso que estamos pasando tanto tiempo en esto porque al final del

día se trata de que los usuarios de Internet puedan utilizar estas cosas que son muy nuevas y novedades. Gracias. Jonathan, tienes la palabra.

JONATHAN ZUCK: Estoy de acuerdo. ¿Por qué dedicamos tanto tiempo a esto? Creo que la comunidad de At-Large puede tener un punto de vista sobre el trabajo de colisión de nombres respecto de la última ronda y creo que han apoyado mucho el trabajo. Hemos dado suficiente respaldo pero creo que esto proviene del comentario público y si hay algo más creativo que deberíamos hacer para evangelizar, personalmente veo que cada vez hay más personas que ven cómo podemos hacer uso y hacer una difusión más grande a una audiencia más grande. La conversación entonces no tiene que ver únicamente con la sustancia sino algunos de los mecanismos y quién tiene que escuchar, porque tenemos que estar en una posición en la que hay personas que tienen que escuchar este mensaje.

ROD RASMUSSEN: Esto se alinea muy bien con lo que nosotros pensamos y tenemos un taller anual en septiembre. Este tema, el DNSSEC y la seguridad en general, están dentro del plan estratégico de la ICANN. También tenemos un trabajo en el que estamos empezando a tener un poco más de tracción junto con el departamento de comunicaciones de la ICANN respecto de la creación de mensajes. Nos gustaría colaborar en este sentido porque ustedes son un muy buen canal para estas cuestiones. Gracias. Perdón. ¿Hay alguien que tiene una pregunta? Parece que hay algo que no funcionó. ¿Podemos probar nuevamente?

HADIA ELMINIAWI: Creo que la parte obvia de At-Large sería promover la adopción de DNSSEC pero claro que no todos los que estamos aquí somos no técnicos pero At-Large básicamente son gente que no son técnicos. Cómo esperan ustedes que nosotros promovamos la adopción de DNSSEC. Gracias.

ROD RASMUSSEN: Muy buena pregunta. Esta es una de las cuestiones en las que tenemos que trabajar. No se trata, me parece, de la tecnología en sí. O sea, sí, pero en realidad es la cuestión de qué podemos hacer con ella. Mi caso de uso es uno que ya usa todo el tiempo. Mi caso de uso favorito. Hay alguien que tiene una licencia de conducir digital canadiense, va a Tokio, quiere tomar algo con alcohol y cómo va a probar que es mayor con una licencia digital, pero la tecnología debería ayudar a eso.

Hay algunos defensores de chicas de 20 años canadienses que quieren ir a un bar en Tokio. Tenemos casos de uso como este, donde los usuarios finales quieren hacer algo y la tecnología lo puede permitir. Esto es lo que debemos defender, por lo que debemos abogar. Para que esto suceda necesitamos la tecnología.

[PETER THOMASSEN]: Quiero agregar algo más. La promesa del DNS no son solamente los casos de uso para beber sino también evitar el spoofing de DNS y cómo entonces difundir esto. Hace unos 10 años inició HTTPS y los certificados empezaron a ser libres y la adopción aumentó. Todos

empezaron a encriptar el tráfico HTTP, incluso si uno no sabe exactamente qué es. Lo mismo se aplica a DNSSEC. Si tenemos un nombre de dominio, deberíamos poder esperar que sea seguro sin importar cuál es el tipo de tecnología, del mismo modo que esperamos que un navegador sea seguro. Lo mismo si hay un airbag en un coche. Lo mismo debería ocurrir entonces para dominios.

ROD RASMUSSEN: Tiene la palabra Barry.

BARRY LEIBA: Lo que Rod y Peter han respondido es por qué tenemos que promover esto pero ustedes están preguntando qué se puede hacer para promoverlo como una persona no técnica. La respuesta, creo yo, es que la comunidad de At-Large se dirige a los operadores en los proveedores de servicio que todos usamos y les dicen: "Ustedes necesitan DNSSEC y esta es la razón". Ahí uno lo promueve de esta manera. Dice: "Yo estoy pagando por este servicio y necesito este servicio".

AMRITA CHOUDHURY: Quiero decir algo a partir de lo que dijo Barry. Nosotros podemos ser los canales amplificadores pero lo que necesitamos es más comunicación, específicamente realizada para los objetivos específicos. Si hablamos con los formuladores de política necesitamos explicar por qué es importante. Si vamos a un ISP o a un proveedor de servicio, necesitamos algo que podamos mostrar como beneficio no

solamente para mí como usuario sino también para que ellos lo puedan implementar. Es decir, que si vamos a tener estos materiales de comunicación, estos canales deberían poder ayudarnos a pasarlos a las RALO, que en sus regiones respectivas o países lo pueden promover porque cuando los técnicos o las empresas hablan, esto está apoyado por los usuarios finales y, si es así, amplifica la información. Esta es la ayuda que se necesita. No cómo lo hacemos sino cuál es el tipo de comunicación.

ROD RASMUSSEN: Gracias. Este es un gran aporte para nosotros en el equipo de comunicaciones de ICANN. Gracias. Vamos a pasar al punto siguiente. ¿Hay alguien que quiera hablar?

HADIA ELMINIAWI: Rápidamente, todos los operadores de registro conocen DNSSEC. Los que no lo están implementando lo hacen por razones que tienen. Para promover todo esto, debemos trabajar en conjunto y tener respuestas a las razones por las cuales no están ellos implementando DNSSEC. Por otro lado, debemos también trabajar en conjunto en la creación de los casos de uso que usted acaba de mencionar.

ROD RASMUSSEN: Esto es un poco más amplio del tema en el que hablamos. Hubo buenos aportes de ustedes y cómo podemos pensar nuestra propia conversación. Excelente. Siguiente diapositiva. ¿Qué tenemos aquí? Una pregunta online, disculpen. Es un comentario. Gracias, John. Es un

muy buen comentario. Es sobre los revendedores. Los ISP y los registradores son los más fáciles de educar en DNSSEC. Lo difícil es que los desarrolladores lo adopten. Esto es un 25% de los gTLD. Excelente observación. Estoy totalmente de acuerdo. Pasemos al siguiente. Es un poco confuso porque hay dos cosas distintas.

Esta es la alineación sobre los nuevos gTLD. Una de las preguntas que tenemos pendientes es el NCAP que viene al final desde la perspectiva del SSAC. Lo otro interesante son algunos acontecimientos recientes en cuanto al uso indebido en los nuevos gTLD. En el SAC114 tenemos ese problema. Hay dos cuestiones ahí. Una son las modificaciones a los contratos, que todos estaban teniendo en cuenta. Ese es un buen paso adelante. En general entonces estamos avanzando, al menos del lado de la respuesta.

Está habiendo también algunos estudios en el Instituto del Uso Indebido del DNS y también del lado de la ICANN en sí. La ICANN no está realizando el estudio sino que lo financia, lo cual es muy importante. Es una gran distinción. Se trata de un estudio independiente. Quizá menos lúdico pero esto nos da muy pocas oportunidades como para poder comentar cómo van las cosas en el proceso. Después de haber hablado con el CTO podría haber alguna oportunidad de dar un asesoramiento externo a los investigadores. Lo haremos esto del lado del SSAC con algunos parámetros y algunas ideas sobre dónde buscar, cuáles son los datos que debemos buscar y tratar de entender las causas y la prevalencia del uso indebido en algunos TLD en registradores, etc. Esto podría ser algo en lo que ALAC

podría trabajar para tener algunas ideas. Vamos a compartir con ustedes lo que venga de este frente pero esto es una oportunidad.

La pregunta es cuándo se va a hacer el estudio en relación con el inicio del proceso y cuando se va a finalizar, etc. Lo que queremos ver es que el estudio se haga y que tenga algún impacto en las evaluaciones y en los programas para ir en contra del uso indebido. Jonathan, ¿quiere agregar algo más sobre este tema antes de continuar?

JONATHAN ZUCK: Estamos muy alineados, me parece. Tuvimos una conversación antes, de que el verdadero hito vendrá después del periodo de solicitudes. Si hay un PDP que tiene que ocurrir o algo por el estilo para tratar algunos de los descubrimientos realizados antes de que todo se delegue.

ROD RASMUSSEN: Gautam ha sido aceptado en el SSAC recientemente. Tiene que ser aprobado por la junta. Tiene que ser aprobado el proceso pero hay trabajo que está haciendo en estos grupos permanentemente como miembro.

GAUTAM AKIWATE: Sí. Quiero dar una actualización. La meta de este grupo de trabajo es trabajar con las prácticas no documentadas que se ocupan de los nombres a un alto nivel. Esto se debe a algunos problemas en el registro y de qué manera un dominio da servicio a otro dominio y de

qué manera los registratarios realizan el trabajo, algunos de los cuales exponen los dominios como solución a los hackeos y esto es parte de mi trabajo de doctorado. Hay un vínculo en la próxima diapositiva. Medio millón de dominios han sido expuestos. Esto excluye muchos dominios sensibles y algunos dominios de gobierno.

Hay un documento en el que he trabajado que incluye los detalles más técnicos en cuanto a cómo esto empieza a ocurrir. Ese es el aspecto técnico de los registros y registradores para discutir qué es lo que podemos hacer y el grupo de trabajo se ocupa de dos cosas. Primero, cómo mitigamos la resolución de los dominios, aquellos dominios que ya han sido secuestrados. No solamente medio millón de los dominios secuestrados sino también un tercio de aquellos dominios que han sido secuestrados por actores que trataron de utilizar estos dominios para distintos objetivos, sobre todo para la optimización de motores de búsqueda.

La segunda pregunta en la que está trabajando el grupo es cuáles son las opciones, las prácticas que pueden adoptar los registradores para que esto no ocurra en el futuro. La idea de alto nivel es analizar cada una de estas opciones utilizando el marco para saber cuáles son los beneficios, las cargas y qué podemos hacer como partes interesadas, y cuál es el riesgo en cada uno de estos casos para los registratarios en sí.

Dicho esto, buena parte de la conversación ha tenido que ver con que los registratarios deben ser responsables de monitorear su propio dominio. Esto es agregado a los propios dominios. Debe haber algunas verificaciones operativas para que esto no suceda en el futuro y

esperamos que los registros y registradores puedan evaluar las distintas opciones y elegir una opción que funcione bien para ellos y que finalmente el grupo de trabajo se ocupe de monitorear la zona para nuevas prácticas que puedan surgir y que pongan en riesgo los dominios. Esto es lo que estamos haciendo.

ROD RASMUSSEN: Gracias. Veo que hemos hecho un muy buen progreso en esto y hemos incluido en este grupo de trabajo operadores que normalmente no son miembros de SSAC pero que han trabajado con algunas de las partes y pueden ver la parte operativa de las cosas y pueden dar una perspectiva interesante y ayudar a compartir el mensaje con la audiencia y decirles cuál es el enfoque, las diferentes soluciones para este problema. ¿Tenemos alguna pregunta respecto a este tema? Al parecer no. Bien. Esperamos avanzar con este trabajo y que se pueda hacer de aquí a Hamburgo. Quisiera dar una excelente presentación sobre las recomendaciones a las que lleguemos, sin presiones.

Muy bien. Me voy a saltar esta parte porque no ha cambiado de la última vez. Solo recuerden que cuando transfieran dominios no se olviden de DNSSEC. Sí, la parte de la transferencia lo consideran fuera de alcance. Dije: "¿En serio?" Creo que esto nos lleva ahora al último punto, el punto que ustedes trajeron a colación. Quiero escuchar más sobre sus inquietudes y algunas ideas de los miembros que han expresado en cuanto a este tema en la última semana.

JONATHAN ZUCK: Sí. Este es un tema que fue delegado hace muchos años. Aunque estos dominios ZIP y MOV fueron delegados hace muchos años, en el 2012, recientemente fueron liberados y creo que tenían una idea para esto. Los liberaron y los pusieron como dominios genéricos. Eso generó investigaciones por parte de otros que vieron el potencial. Son lo que nosotros llamaríamos extensiones de archivos confiables. Es decir, cosas que la gente se sienta cómoda abriendo, por regla general. Pueden ser por ejemplo un vídeo o una URL falsa que hace que parezca que está atada algún tipo de ajunto y tiene algún riesgo asociado con ello.

He visto que hay tres componentes para todo esto. Uno, qué se puede hacer ahora si es que se puede hacer algo. Quizá nada. Quizá educación, porque todos estamos muy involucrados con la educación pero no tengo la respuesta única para esto. Sé que se dio una reunión con Google donde hablaron de lo felices que están monitoreando todo y cuando estaban tratando de determinar cuál es el nivel de uso indebido que se está dando lamentablemente vimos que algunos están registrando ciertos nombres especiales. Hay algunos DNS que son como falsos, por así decirlo. No los reales. Solamente ha pasado un mes desde que se hizo esto para detectar cuando hay uso indebido. Ellos están muy aguerridos con la idea de hacer un monitoreo.

Como dije, hay un blog de Google que habla de cuando hay muchos formatos de archivos que encajan con esto pero cuando vemos que buscamos una categoría de reconocimiento general me llamó la atención ver que esto va en paralelo con el trabajo que se está haciendo en evaluación de riesgo. Sabemos que la URL es la ubicación

del archivo y se ve muy similar en otros puntos. Cuando vemos el marco de evaluación de riesgos para usuarios vemos que se puede aplicar aquí.

La última pregunta podría ser si deberíamos estamos pensando antes de la próxima edición nuevas extensiones de archivos como JPG, GIF y otros que la gente ya acepta como extensiones de los adjuntos que llegan a su correo electrónico. Ustedes piensan mucho en estas cosas y han hecho un proyecto por lo que veo, por eso les pregunto.

ROD RASMUSSEN: Sí. Esas son preguntas muy interesantes e ideas interesantes. Así como tienen ustedes problemas de que alguien ponga en una cadena una marca conocida para hacer phishing, nos preocupa porque estamos viendo la colisión de nombres como algo que puede filtrarse hasta el DNS y desde la perspectiva del DNS no parece ser un problema. Eso es lo que hemos visto en este estudio de colisión de nombres. Esto es algo similar, donde tenemos interacciones interesantes que se pueden dar. Creo que ya conversamos sobre esto. Mi proveedor de cable de Internet me llamó ahorita para ofrecerme algo, por ejemplo.

Hemos tenido conversaciones sobre cuáles son los antecedentes, qué es lo que está pasando aquí, por qué tenemos estos temas, estos problemas. Tenemos algunos sistemas que ya sabemos quiénes lo crearon. Hay cierta interpretación de las cosas. Por ejemplo, que una extensión puede hacer algo pero también está la parte de la interfaz del usuario humano, que es la parte más difícil porque tienes todas las funcionalidades en una, por lo menos en el contexto de un buscador.

Tu buscador tiene que poder hacer algo en la web y además algo más. Si estás viendo lo que va a ser un TLD y estás creando imagen y vas a hacer algo más, todo eso se vuelve muy interesante. Este otro tema ya ha sido delegado hasta donde yo sé, especialmente dado que no veo a nadie gritando que se están colapsando los puentes y demás. Supongo que no hay nada práctico que se pueda hacer viéndolo en retrospectiva.

JONATHAN ZUCK: Hay personas que sí están haciendo mucho ruido. Estuvo en las noticias y demás. Cuando hablamos de que estos son temas que han llegado a la sala de la casa de la gente. Quizá sí tenemos que conversarlo.

ROD RASMUSSEN: Sí. Lo que digo es que no veo a personas que tengan uniforme que estén saltando de emoción con esto. Creo que es parte de los retos para la organización de la ICANN responder ciertas preguntas sobre esto porque mi conocimiento llega hasta aquí. Tenemos expertos que conocen mucho más a fondo este tema y les dije que hay personas aquí que saben algo del SSAC y pueden hablar sobre los efectos potenciales y teniendo personas de ese perfil sería genial si tomasen el micrófono. Sí, adelante. Una pregunta directa sería mucho más fácil.

BILL JOURIS: Al parecer no podemos hacer nada hasta que tengamos un desastre entre manos. Es lo que estoy escuchando.

ROD RASMUSSEN: Pasamos por un proceso. Vimos todas las verificaciones. Está ya el animal vivo y en el agua. Nadie ha muerto todavía. Es una metáfora fatal pero realmente, cuando aprobamos esto, el umbral de referencia era: "Nadie ha muerto todavía" pero entiendo cuando decimos a qué nivel me detengo. Técnicamente sabemos cómo hacerlo. Lo sacas de la zona raíz, excelente. Hay un montón de abogados que van a tener algo que decir con respecto a eso y está esa parte. Luego de ahí en adelante eso sería un tema interesante también porque si no hay nada más quizá se puede convertir en una pieza importante para crear anuencia sobre este tema.

Lo que estamos tratando de decir es que estamos aquí, hemos hablado de esto desde hace como unos 10-15 años, pero ahora que la gente ya lo ve sería interesante saber qué es lo que dice la gente. Sería excelente tener aporte de parte de ustedes porque han tenido mucha más observación que nosotros. Nosotros somos las personas técnicas que en teoría sabemos cómo funciona esto. ¿Algo que decir, Bill?

BILL JOURIS: Quizá tenemos que hablar con el consejo de la ICANN y decir: "¿Realmente tenemos que tener algo en el contrato que diga que tenemos que de alguna manera revocar esto de una determinada delegación?" Si usted ya tiene por lo menos el lenguaje, estará usted listo para cuando sea el momento de utilizar todo esto para estar en posición de salir huyendo cuando llegue el momento del desastre o

tendremos que esperar que venga la policía u otras agencias gubernamentales a decirnos qué hacer. Ya hemos pasado por eso.

JONATHAN ZUCK: ¿Cómo podría aplicar esto técnicamente para la siguiente ronda?

PETER THOMASSEN: Quisiera poner en perspectiva los comentarios del grupo que ha visto la parte del riesgo. Creo que sí podría ser un problema si usted recibe un enlace que diga .ZIP y usted recibe lo que no esperaba pero creo que eso ya es un problema porque está pasando a veces y le puede redireccionar a un archivo que puede ser ejecutable. De hecho, con un dominio .ZIP puede tener después un .JPG o algo así. Lo que estoy diciendo es que esto tiene un rol en la extensión .ZIP y no ha sido siempre así en el pasado.

Lo más importante del uso indebido es cuando se tiene un DNS que de alguna manera confunde y la gente tiene la idea de que tiene quizá otro nombre de dominio que lo puedes poner en algún tipo de señalización y luego las cosas se pueden complicar un poco más pero eso también se ha hecho posible ahora con un dominio .ZIP.

Creo que el riesgo de todo esto es el mismo riesgo de estos archivo versus los de .ZIP. No estoy diciendo que hay que perdonar esto pero no tenemos que preocuparnos tanto por estos TLD y con la idea de que estas cosas se puedan cruzar. Creo que el TLD en particular no va a causar daños.

ROD RASMUSSEN: Preguntamos a John Levine. John, ¿por qué no intervienes?

JOHN LEVINE: Sí. Creo que tengo que refutar algunas cosas aquí. El tema es que Microsoft tomó una decisión incorrecta hace décadas cuando usó el nombre de un archivo como un indicador de seguridad. Puedes hacerlo con archivos .M0V. Hay cosas malas que pueden pasar. Coincido con Peter. Creo que todo lo de ZIP y MOV, eso evita que a veces pensemos que hay algo serio que se está dando y todo el problema básicamente es tratar de hacer la seguridad con nombres y eso nunca ha funcionado. Eso ya dejó de funcionar hace décadas. Aunque es razonable decírselo a las personas, por si tienen un software mal diseñado. Creo que no es viable tratar de hacer esto de esta manera porque hay cosas que hoy no son nombres de archivos y mañana lo pueden ser. De hecho, hay cosas que son nombres de archivos en otras partes del mundo donde no vivimos. Creo que tenemos que preocuparnos de cosas mucho más importantes que estas.

JUSTINE CHEW: Estoy de acuerdo con el caballero. Creo que podemos tratar esto como si fuera un uso indebido del DNS.

GREG SHATAN: Creo que muchas de las cosas que mencionó Peter no son las cosas que nos preocupan o hasta qué punto estamos preocupados por estas cosas. Como usuarios generales vemos una cierta cantidad de tipos de archivos, ves .DOC, .PPT, .ZIP. Estas extensiones de archivos son el 99% de las extensiones que vemos. Gracias a Dios nadie ha solicitado registrar .PPT. No queremos explotar esa confusión para que alguien haga clic sobre lo que cree que es un archivo comprimido y en lugar de eso los manden a un dominio en la web oscura. Creo que son cosas irrelevantes, como dice Peter, pero nunca estaban ni siquiera contempladas en la mesa.

PATRICK FELTZ: Tenemos que tener separar el tipo de archivo del nombre del archivo. Si eso se hace, entonces el problema no está del lado del TLD sino en la aplicación que hemos elegido. Esto tiene que ver con las compras, las aplicaciones y los requerimientos.

[GREG SHATAN]: No vamos a detener nunca a la gente para que dejen de enviar archivos .ZIP.

WARREN KUMARI: Dándole seguimiento a lo que dijo Patrik, lo que aparece en su lector de correo diciendo que esto es bla, bla, bla .ZIP, el hecho de que aparezca en el lector del correo no quiere decir que sea un archivo ZIP. Puede decir: “Aquí hay una foto de mi gato” y puede ser otra cosa. Se lo puede estar mandando desde un enlace que diga

megustaelqueso.net. No podemos asumir que lo que aparece en el enlace o en el cuerpo del mensaje es el mismo tipo de archivo que se va a cargar. Asimismo, puede tener algo que diga: “Vaya [food.net]” y cuando hacen clic el usuario es llevado a evil.net. Les hemos dicho esto por décadas a los usuarios.

JONATHAN ZUCK: A veces te ponen una URL y está tapando la verdadera.

WARREN KUMARI: Sí y no, porque los ejemplos que se han mostrado con las URL y .ZIP no son texto ASCII. Son un ataque homónimo, es Unicode.

JONATHAN ZUCK: URI. Va a parecerse a la URL.

WARREN KUMARI: Es exactamente lo mismo que con microsoft.com, donde la o está en cirílico. Es Unicode. Básicamente ahí se le muestra que está en Punycode o en algo similar.

ROD RASMUSSEN: Tenemos que ir cerrando. Hemos tenido conversaciones muy interesantes. Como ven, estamos llegando a las conclusiones. ¿Tenemos tiempo para eso? No, no mucho. Okey. Mis disculpas. Con gusto podemos hablarlo aparte.

JUSTINE CHEW: ¿Están los expertos en IDN del SSAC? Si pudiese hablar con ustedes unos cinco minutos, sería excelente.

ROD RASMUSSEN: Excelente. Perfecto.

JONATHAN ZUCK: Gracias por venir. Siempre es bueno tenerlos aquí. Esperamos poder trabajar con ustedes sobre la campaña informativa de DNSSEC.

[FIN DE LA TRANSCRIPCIÓN]