ICANN75 | Reunión General Anual – Sesión conjunta: ALAC y SSAC
Domingo, 18 de septiembre de 2022 – 13:15 a 14:30 KUL

YEŞİM SAĞLAM: Vamos a dar comienzo a la sesión. Por favor, comenzad con la grabación. Hola. Bienvenidos a la sesión conjunta entre el ALAC y el SSAC. Soy Yeşim Sağlam y seré la coordinadora de la participación remota para esta sesión. Por favor, tengan en cuenta que esta sesión se está grabando y que se rige por los estándares de comportamiento esperado de la ICANN. Durante esta sesión, las preguntas o comentarios que se envíen al chat serán leídos en voz alta si se encuentran en el formato adecuado tal como se les indicó en el chat.

Participar mediante audio es posible. Deben esperar hasta que se mencione su nombre. Luego deben habilitar su micrófono de Zoom. Para quienes están en la sala principal, por favor, levanten la mano en Zoom. Cuando se mencione su nombre, por favor, habiliten su micrófono de mesa. Para el beneficio de los demás participantes, por favor, mencionen sus nombres para el registro y hablen a una velocidad razonable.

Los participantes en la sala pueden tomar un receptor y utilizar sus propios auriculares para escuchar la interpretación. Por favor, recuerden quitarse los auriculares cuando utilicen el

micrófono de mesa para evitar cualquier interferencia. Los participantes conectados remotamente pueden acceder a la interpretación mediante la barra de herramientas de Zoom. Ahora sí, con eso quiero darle la palabra a Jonathan Zuck, quien es el vicepresidente de ALAC. Gracias.

JONATHAN ZUCK: Hola a todos. Bienvenidos luego del receso del almuerzo. Bienvenidos a una de nuestras sesiones favoritas, la reunión conjunta del ALAC y el SSAC. Muchas veces experimentamos mucha inestabilidad en ALAC. Siempre les agradecemos que tengan una presencia tan estable en la sala con nosotros. Es un placer tenerlos aquí con nosotros y creo que tenemos ya una alianza natural teniendo en cuenta el alcance de nuestro trabajo y nuestro interés de continuar avanzando en pos de los usuarios finales en relación a los temas de seguridad y estabilidad cuando surgen. ¿Sabemos si Justine está conectada?

Bien. El primer tópico de la agenda tiene que ver con las preguntas en relación con el uso indebido del DNS. Hay preguntas que fueron generadas por el grupo reducido de la GNSO sobre uso indebido del DNS y básicamente nos dijeron qué necesitan que hagamos. Es decir, como GNSO, qué es lo que está dentro del alcance de la GNSO en relación a los procesos de

desarrollo de políticas. Nosotros respondimos con una serie de ideas y una serie de conceptos.

Recientemente, en los últimos dos días, han creado una respuesta preliminar a esas preguntas. Lo que voy a hacer en este momento es darles la palabra a los miembros del SSAC para que efectúen su presentación y luego le voy a dar la palabra a Justine para que comente sobre las reacciones pertinentes. Me gustaría ahora darles la palabra a los miembros del SSAC y también hablar un poco sobre el uso indebido del DNS con todos ustedes. Rod mencionó la idea de esta hoja de ruta del uso indebido del DNS así que eso es lo que vamos a hacer. Le voy a pasar la palabra ahora.

ROD RASMUSSEN: Gracias, Jonathan. Felicitaciones por su nueva designación y gracias al ALAC por darnos la bienvenida una vez más a esta sesión. Tenemos mucho interés en proteger Internet y a los usuarios por eso siempre es bueno reunirnos. No sé si Andrei quería decir algunas palabras. Está conectado en forma remota. Andrei, ¿quiere comentar algo?

ANDREI KOLESNIKOV: Buenas tardes tras el receso después del almuerzo. Creo que ese es el horario. Gracias, Rod, por darme la palabra. Quisiera

comentar sobre la agenda. Hola, Jonathan. Hola, SSAC. Hola, miembros del ALAC. Es un gusto verlos a todos nuevamente. Con la agenda vamos a comenzar con las preguntas en relación al uso indebido del DNS porque habitualmente esto nos lleva a las presentaciones del SSAC, a las presentaciones que hacen sus miembros y las preguntas aparecen y habitualmente no tenemos tiempo de responder estas preguntas que surgen durante las reuniones. Por eso la agenda luce así. Jonathan piensa que tendríamos que comenzar con la presentación de los temas más importantes del SSAC. Podemos empezar de esa manera. Es una forma tradicional de empezar pero depende de ustedes, colegas, cómo vamos a avanzar con la agenda del día de hoy.

Me gustaría mencionar los tópicos. La colisión de nombres. Jim y Matt van a hablar del tema. Esta fue una pregunta muy común que fue presentada por Russ. También vamos a hablar de la difusión externa a nuevos miembros del SSAC. Es un tema tradicional. También vamos a hablar del acceso a los datos que va a presentar Steve Crocker y vamos a hablar del [SAC014], si tenemos tiempo. Vamos a comenzar entonces porque el tiempo comienza ya a correr.

ROD RASMUSSEN: Muchas gracias, Andrei. Vamos a avanzar tan rápidamente como sea posible. Espero que podamos explicar los diferentes gráficos.

Le voy a dar la palabra a Matt Thomas, quien va a hacer un resumen del NCAP. El uso indebido del DNS es un tema de debate. Luego vamos a hablar de la hoja de ruta junto con Jonathan. Matt, le cedo la palabra para que nos dé una breve actualización sobre el proyecto NCAP.

MATT THOMAS: Soy el copresidente del NCAP junto a James Galvin. Quiero darles una breve actualización del proyecto de coalición de nombres. Nos reunimos hace unos meses con el ALAC para darles una presentación muy detallada respecto al trabajo que se ha hecho con respecto al estudio dos del NCAP. Aquí les voy a contar un poco más, quiero darles más información de contexto.

Como todos ustedes saben, el NCAP está en curso desde hace varios años. Este proyecto fue estructurado en tres etapas diferentes. El estudio uno, que ya se completó hace unos años. En este caso tenía que ver con la finalización de un repertorio de toda la información en relación a la colisión de nombres. Luego hubo una versión revisada del estudio dos que estamos llevando a cabo actualmente.

El estudio dos específicamente se centra en dos objetivos. El primero tiene que ver con brindar cierto asesoramiento a las preguntas de la junta directiva que se le planteó al SSAC en relación a los problemas relacionados con la colisión de

nombres y también asesoramiento sobre cadenas específicas como por ejemplo .CORP y .MAIL en la ronda del 2012.

El grupo de debate del NCAP se reúne regularmente para abordar estas cuestiones y también ha estado realizando nuevos estudios de investigación en conjunción con el contratista técnico que fue contratado a través de la ICANN, que está a cargo de investigar los informes de colisión de la ICANN que recibimos en relación a la ronda de 2012. Hasta el momento nuestro grupo de trabajo cuenta con unos 25 miembros, lo que incluye 14 miembros del SSAC. Tenemos 23 miembros observadores de la comunidad y actualmente nos encontramos trabajando en el estudio número dos. Siguiente diapositiva.

Hay dos publicaciones recientes que surgieron de este grupo de debate de NCAP que están sometidas a comentario público. Una es un estudio de colisión de nombres en .CORP, .HOME, .MAIL, así como interno, LAN y local. Se agregaron a otras cadenas de caracteres porque al momento del estudio se recibían más de 100 consultas por día para los servidores de las zonas A y J. Se inició un estudio de los datos del DNS y de los servidores raíz. Esto ha evolucionado a lo largo del tiempo. También dieron algunas ideas con respecto al trabajo que se realizó y nuestros hallazgos siguen avanzando. Esto nos permitió entender cómo las alteraciones del ecosistema del DNS han cambiado a raíz de distintas cuestiones en el ecosistema del DNS y los protocolos.

Luego hay un estudio de perspectiva de consultas de DNS para dominios de alto nivel que no existen. En este caso la idea es comprender datos preliminares y cómo estos datos se pueden recabar para evaluar la cuestión de la colisión de nombres. Esto nos permite brindar algunas ideas y analizar la heurística para determinar cómo estas mediciones se pueden utilizar para evaluar los riesgos y también qué cuestiones hay que aplicar cuando se implementen estas medidas para .CORP, .HOME y .MAIL. Siguiente diapositiva, por favor.

Algunos de nuestros hallazgos principales incluyen lo siguiente. En primer lugar, las colisiones de nombres siguen siendo un problema creciente y complicado. El estudio indica eso. También el estudio determina que la causa raíz de estos problemas de colisión de nombres siguen surgiendo de los problemas originales que fueron identificados en la ronda del 2012 y en los protocolos de descubrimiento de servicios que son los factores que contribuyen a este problema.

También hemos identificado una serie de cuestiones como por ejemplo mediciones de diagnóstico crítico. Estas son básicamente una serie de herramientas que nos permiten evaluar el riesgo específico o daño específico que podría causar la colisión de nombres teniendo en cuenta los parámetros y datos que hemos observado. Esto implica también un estudio de perspectiva para poder brindar esos puntos para poder

comprenderlos. CDM son las mediciones diagnósticas críticas y cuáles son las ventajas a la jerarquía del DNS.

El principal hallazgo que vemos en relación a estos CDM es que son una función de diversidad y volumen, y que los vectores incrementan la dificultad en trazar los riesgos que pueden implicar la colisión de nombres, lo cual también se incrementa. Esta investigación en conjunto con otras presentaciones de la industria y de la comunidad identificaron otras medidas u oportunidades de mejora para poder tener plataformas de medición que puedan extender la ayuda a los solicitantes. En este caso esto sería un gran beneficio para la comunidad porque al menos les dará una idea de qué se trata antes de iniciar el proceso de solicitud dando información sobre estos hallazgos preliminares en materia de colisión de nombres.

Ahora hablemos un poco más de estas mediciones de diagnóstico crítico. Para quienes recuerden el informe JAS y la ronda del 2012 recordarán que se calificaron ciertas cadenas de caracteres. Esas mediciones de diagnóstico crítico eran las que se utilizaban en ese entonces. La primera prácticamente abordaba el tema del volumen de las consultas. El volumen de consulta no es un único indicador de un verdadero riesgo o daño sino que puede ser un indicador que nos lleve a determinar algo. También se analizaron otras propiedades o características u otras dimensiones como por ejemplo la diversidad, la diversidad

de múltiples aspectos como por ejemplo las direcciones IP, la distribución de ASN, el tipo de consultas que se consultaban y todas en combinación brinda una posibilidad de mejor describir el impacto potencial o el daño que puede causar una cadenas de caracteres en colisión. Por supuesto, estas medidas de calidad no son las únicas mediciones en materia de colisión de nombres y esto tiene que hacerse cadena por cadena. Siguiente diapositiva.

¿Dónde se encuentra ahora el grupo de debate de NCAP? Actualmente nos encontramos en el desarrollo de los resultados del estudio dos. Estamos en el paso de establecer un flujo de trabajo estable para darle a la junta directiva un mecanismo para poder evaluar las colisiones de nombres que se suceden. Esto está en consonancia con el asesoramiento a las preguntas de la junta directiva y también a lo relacionado con las cadenas .CORP, .HOME y .MAIL.

Tenemos como objetivo que este informe que estamos preparando salga a comentario público en el cuarto trimestre del 2022. Aquellos interesados en unirse y contribuir, tenemos las reuniones del grupo de debate de NCAP que se suele reunir los miércoles. También tenemos la lista de suscripción a la que pueden suscribirse para hacer el seguimiento de lo que ocurre. Les agradeceríamos que se unieran a nuestra lista. Estamos cerca del final de la publicación del informe dos y siempre

valoramos todo feedback y comentarios adicionales. Muchas gracias.

JONATHAN ZUCK: Gracias, Matt, por esta presentación. Esta es un área que está generando interés en la comunidad At-Large. ¿Hay alguna pregunta? Tuvimos una muy buen presentación antes del CPWG sobre este informe pero quizá este sea un tema nuevo para algunos de los que están aquí presentes. Si alguien tiene alguna pregunta, adelante. Que alguien me diga por favor si hay preguntas en Zoom, ya que no pude conectarme a Zoom todavía.

¿Piensan que el resultado neto será un sistema de calificación o algo así para poder calcular los riesgos que nos permiten hacer un ranking o será algo más complejo? Una serie compleja de evaluaciones de riesgos que podrían utilizarse para luego proponer medidas de mitigación o ese tipo de cosas. Cómo piensa que va a ser en última instancia.

MATT THOMAS: Es una buena pregunta. Creo que será más bien la última opción que usted mencionó. Hay un componente fundamental al que el grupo de debate ha llegado. Es un problema de gestión de riesgo. Entender los riesgos y poder hacer un perfil de los riesgos

y tratarlos de esta forma será el mejor curso de acción de aquí en adelante, tanto para la junta directiva de la ICANN como para poder avanzar. Lo que esperamos hacer en el grupo de debate es poder brindar alguna de estas protecciones y el contexto que hará que esto sea un proceso repetible, sostenible.

JONATHAN ZUCK: ¿Piensan que de esta forma se logrará una mitigación suficiente como para hacer la delegación?

MATT THOMAS: No voy a dar mi opinión ahora. Puede unirse a la lista de suscripción y ahí podrá emitir su opinión.

JONATHAN ZUCK: Gracias. ¿Alguien tiene alguna otra pregunta? ¿En Zoom hay alguna pregunta? Le doy la palabra a Rod.

ROD RASMUSSEN: Muy bien. La siguiente diapositiva, por favor. Ya hablamos antes del enrutamiento pero ahora tenemos una presentación más linda, más completa, con más detalles. Russ, ¿podría dirigir la presentación? Russ está conectado de forma remota y va a hacer esta presentación.

RUSS MUNDY: Hola a todos. Espero que hayan tenido un buen almuerzo en Kuala Lumpur. Son todos bienvenidos a esta breve presentación sobre SAC121. Como ya se dijo, vamos a ver una reseña de lo que venimos haciendo y un informe casi publicado. Gracias a nuestro fantástico personal de apoyo ahora tenemos una serie de datos mucho mejor que nos permite describir el contenido del informe. Espero que algunos ya lo hayan podido leer. De lo contrario, el objetivo es darles ahora un resumen general. Levanten la mano o hablen directamente si tienen alguna pregunta en cualquier momento durante mi presentación. La descripción general está aquí y cubre los principales temas que vemos en pantalla. Ahora pasemos a la siguiente diapositiva.

Esta imagen en particular surge del documento propiamente dicho y es una descripción de los distintos pasos. Llevó un poco de tiempo recordar todos los pasos pero espero que sea comprensible para todos. Es un ejemplo en el que alguien se conecta. Podría ser con un teléfono celular. Alguien pregunta dónde está XXX y esa consulta, esa pregunta inicial es una pregunta en el DNS que luego va al resolutor del DNS. Llega al resolutor del DNS pasando por esa burbuja que ven en la parte inferior, AS1, AS2, AS3, hasta que finalmente llega al resolutor D.

El resolutor D luego hace lo que nosotros llamamos recursión en el DNS. Es decir, tiene que ver a cuántos servidores tiene que hacerle esa consulta. En este caso el resolutor del DNS D va al servidor autorizado DNS y llega pasando a través del sistema autónomo tres y el sistema autónomo seis.

La parte inferior es una indicación de cómo fluyen los paquetes y la parte superior por encima de la línea negra ilustra el protocolo de DNS propiamente dicho. La respuesta al servidor autorizado DNS 2 es pasar por AS1, AS2, AS6 y luego vuelve al resolutor recursivo D, quien luego lo vuelve a enviar al cliente C que hizo la pregunta o consulta inicial. Esto pasa por AS3, AS2, AS1 hasta llegar al cliente.

Este es un ejemplo. Si lo pensamos, es increíble con qué rapidez ocurre esto porque esto ocurre cada vez que hay una consulta del DNS. Los paquetes van y vienen, y no solamente están involucradas en la respuesta sino también son utilizados por el sistema de enrutamiento. Pasemos ahora a la siguiente diapositiva, por favor.

Este es un ejemplo de un tipo de ataque. En este caso el ataque se produce en AS1. Cuando el cliente C envía su solicitud para llegar al resolutor D, de hecho no llega al resolutor D y, si llega, recibe una respuesta más rápida del resolutor malicioso M que

está en la parte inferior de la página. Hace esto mediante un secuestro de enrutamiento.

Si llega a ese círculo rojo y luego vuelve al cliente C, la dirección es distinta de la que vendría del servidor autorizado legítimo. Si retrocedemos una diapositiva, fíjense aquí. Pueden ver que la dirección es diferente. Este es el resultado de un secuestro de enrutamiento. La siguiente diapositiva, por favor.

¿Alguien tiene alguna pregunta acerca de estos temas? Estos conceptos son sumamente importantes. Esta no es la única forma en la que el secuestro de enrutamiento afecta al DNS pero es un buen ejemplo de la forma en que genera un impacto. Pasemos a la siguiente diapositiva ahora, por favor.

El secuestro de enrutamiento potencialmente más conocido que generó un alto impacto es lo que a veces llamamos MyEtherWallet/Route53. Este es el secuestro más conocido. En este caso se trató de un grupo de delincuentes. No sabemos quién. Creo que nunca fueron identificados. Lo que lograron hacer fue hacer un secuestro que es similar al que vimos en la diapositiva anterior. Lo que hicieron para secuestrar la ruta fue secuestrar una ruta más específica. El sistema del DNS se vio afectado. Lo que hicieron en este caso fue insertar rutas más específicas para los servicios de DNS de MyEtherWallet y con su DNS malicioso y con toda su maquinaria maliciosa a la que

apuntaban las rutas más específicas lograron robar 150.000 dólares en unas dos horas.

El otro impacto fue que cuando los delincuentes roban dinero mediante el secuestro de rutas, yo digo que ese es un evento en cascada porque hay otras personas que después se van a ver afectadas por lo mismo. Pero además del dinero que robaron, que fue bastante… 150.000 dólares en dos horas está bastante bien. Es una muy buena inversión. Además de eso, debido a este secuestro básicamente dejaron fuera de la ruta 53 y del servicio de DNS a todos los demás usuarios porque lo que hicieron fue lo siguiente. Cada vez que se hacía una consulta al DNS, excepto que viniera de MyEtherWallet, volvieran a la fuente. Aquellos que usaban el servicio de DNS de Route53 no obtenían la respuesta. Creo que hay una pregunta. Adelante. Adelante.

HADIA ELMINIAWI: Gracias. Mi pregunta es qué es un ataque de BGP. ¿Es un incidente de uso indebido o un ataque malicioso? ¿Cómo lo llamarían?

RUSS MUNDY: Yo lo llamaría de ambas formas porque ambos protocolos fueron afectados. El primer ataque fundamental afectó el sistema de enrutamiento pero para que fuera eficaz también tuvieron que

básicamente dar respuestas del DNS incorrectas. Dar respuestas incorrectas a las consultas es un problema que existe en relación con el DNS desde hace muchos años. La gente que no utiliza DNSSEC es muy vulnerable a este tipo de ataques que se pueden hacer de diferentes formas. Probablemente este ha sido básicamente un ataque de BGP pero también un ataque al DNS. ¿Responde esto su pregunta? ¿Le resulta claro?

HADIA ELMINIAWI: Sí, gracias.

ROD RASMUSSEN: Hay una pregunta en el chat.

RUSS MUNDY: Gracias, Rod. No la había visto. Sí. AS4 también está involucrado en el ataque. Probablemente. No tengo la certeza absoluta pero probablemente sea así. El sistema de enrutamiento propiamente dicho está diseñado de forma tal que tenga información que algunos describen como rumores pasados de una persona a otra que confían entre sí y que quizá no deberían confiar. Es decir, hay algunas cosas que hay que hacer para mejorar la seguridad de BGP pero las vulnerabilidades de BGP también existen desde hace muchos años. ¿Responde esto su pregunta?

ROD RASMUSSEN: También está Sander que quiere hacer una pregunta.

RUSS MUNDY: Adelante.

SANDER STEFFANN: Hola. Usted dijo que recibieron un cert fail para todas las demás consultas. Eso afectó el tiempo que llevó identificar al secuestrador. Supongo que si daban datos adecuados para todos los demás dominios, quizá habría llevado más tiempo hasta que lo identificaran. ¿Puede ser?

RUSS MUNDY: Creo que probablemente tenga razón. Estas son especulaciones. En realidad, si uno hace este tipo de ataques, entonces por lo general llevará más tiempo hasta que alguien pueda identificar lo que está ocurriendo. Es posible que sea así. ¿Hay alguna otra pregunta? Muy bien.

JONATHAN ZUCK: Parece que no. Adelante.

RUSS MUNDY: Gracias, Jonathan. Pasamos a la siguiente diapositiva, por favor. Muy bien. Aquí tenemos una serie de diapositivas con mucha información. Lo que identificamos aquí, en el documento propiamente dicho, es que hay una serie de lugares donde pueden producirse esas interacciones y una serie de razones por las cuales muchas de las vulnerabilidades que existen podrían mejorarse si existieran todos los mecanismos de seguridad, si estuvieran implementados. Por ejemplo, el mecanismo para identificar el servidor que está dando una respuesta frente a una consulta. Hay muy pocos resolutores que usan esta funcionalidad. DNSSEC es algo muy sólido que evitaría este poisoning del DNS pero la mayoría no hace validaciones de DNSSEC y en el documento mostramos que si se sigue a esto la consulta no llegaría al resolutor recursivo y así es como se podría evitar este secuestro.

Pueden ver que hay una serie de lugares donde se pueden implementar protecciones para reforzar la seguridad, y la tecnología en muchos de los casos está disponible para hacerlo. Simplemente no se lo utiliza hoy en día. ¿Alguien tiene alguna pregunta con respecto a esta diapositiva? Muy bien. Pasemos a la próxima, por favor.

Bien. La secuencia de este ataque en particular es la siguiente. Una de las razones por las cuales utilizamos este ejemplo en particular es porque es un ejemplo de lo que los delincuentes

hacen en la vida real. Esto les permite ver la secuencia de eventos muy claramente. El resultado, como pueden ver en la parte de las consecuencias, es un robo y muchas personas que utilizaban estas zonas del DNS que se quedaron sin servidores del DNS durante unas horas. Siguiente diapositiva, por favor.

Esta parte habla sobre cómo se pueden hacer las cosas para poder mejorar la seguridad del sistema de ruteo. Una de las cuestiones que tenemos que tener en cuenta y que hizo el grupo de trabajo cuando se reunió dentro del SSAC es hacer una serie de preguntas para ver si era posible mejorar a través de procesos internos. En este caso estamos agregando seguridad en las partes técnicas. Lo que más se escucha es la seguridad del BGP, lo cual es bueno en tanto y en cuanto haya testigos y muchos bajo ataque.

Si algo está bajo ataque o se comete un error y dice: “A ver, me equivoqué. No debería haber hecho esto”, bueno, en ese caso la realidad es que en la mayoría de los casos no se puede discernir si fue algo intencional o no intencional. Hay un indicador muy sutil y es con qué rapidez se resuelve el problema una vez que se identifica la cuestión y quiénes están causando el problema si es que se sorprenden y solucionan todo rápidamente o no o si están haciendo un ataque agresivo y de repente terminan desapareciendo sin siquiera acusar recibo de esa actividad. Eso

apenas se puede diferenciar porque a primera mano todos los casos parecen similares en Internet.

El otro aspecto a tener en cuenta y que es sumamente importante en cuanto a la mejora de la seguridad del enrutamiento es tener una política de enrutamiento exacta para las operaciones. Si la operación es una operación de ISP mayormente o si uno tiene operaciones centradas en el DNS aun así seguramente tengan que tener cierto routing o ciertos servicios y deben comprender cuáles son los requisitos de la política de enrutamiento para garantizar que estén vigentes y que se implementen.

El otro aspecto realmente importante en la mejora de la seguridad del routing o ruteo tiene que ver con la solidez de las operaciones. En este caso hablamos de diferentes documentos y lo que mencionamos aquí quizá es algo que ya han escuchado. Hay un grupo de operadores que se reunieron y que crearon algo que se denomina MANRS. En este caso es la sociedad de Internet que ha promovido y que ha avanzado en este proyecto. Este es un documento que contiene muchos principios en materia de principios y de seguridad operativa. Estos son los tres aspectos que hay que tener en cuenta para hablar de una mejora en todas estas áreas. Esto es lo que puede ayudar a mejorar la solidez del sistema de ruteo. Siguiente diapositiva, por favor.

Bien. Una de las cuestiones a tener en cuenta en relación al BGP son los registros de enrutamiento. Esencialmente son base de datos que brindan un mecanismo para que los operadores puedan colocar su información y que la puedan compartir con otros y que puedan tomar información para utilizarla en sus sistemas. Hay una serie de limitaciones existentes. Hay una serie de registros de enrutamiento que existen. Tienen diferentes tipos de información entre los registros pero no tienen mucha robustez ni mucha fortaleza. Pasemos a la siguiente diapositiva, por favor.

La infraestructura de clave pública de recursos permite tener un mecanismo verificable y criptográfico que permita a los receptores de la información de enrutamiento saber si esa información se origina correctamente y si fue autorizada para ser originada o no.

ROD RASMUSSEN: Adelante. Siga, por favor. Continúe.

RUSS MUNDY: Siguiente diapositiva. Creo que hay algunas preguntas que han surgido. Bueno. Voy a hablar de esto muy rápidamente. Es una forma diferente de ilustrar lo que tiene que ver con la mejora de la seguridad. Este es un enfoque un poco más detallado. En

general, los operadores necesitan una infraestructura y necesitan llevar adelante actividades de monitoreo internas y externas a sus sistemas. Tienen que coordinar con otros operadores y tienen que tener también una cooperación establecida y saber qué hacer cuando algo no funciona. También deben seguir los principios de MANRS. Es algo que se recomienda realmente. Siguiente diapositiva, por favor.

Hoy por hoy existen anomalías en materia de enrutamiento que se llevan a cabo prácticamente todos los días. Suceden habitualmente. A veces cientos de veces en un mismo día. Para poder mejorar la robustez del sistema de routing o de enrutamiento se requiere el trabajo de toda la comunidad de diferentes maneras. Tenemos personas que operan los ISP en diferentes partes del mundo pero también se puede contribuir y también particularmente comprender más de la cuestión para poder llevar adelante las cosas necesarias para fortalecer la seguridad. Esto se basa en los puntos que vemos en la diapositiva. Tenemos una pregunta. Adelante, por favor.

JONATHAN ZUCK: No sé. Siva.

SIVASUBRAMANIAN MUTHUSAMY: ¿Me escuchan? Esta diapositiva muestra que la organización debe monitorear las raíces, ¿pero hay un proceso que nos permita monitorear las raíces? Si yo veo que hay ASN que están comprometidos, ¿hay alguna manera de mejorar la raíz? Si van a decidir monitorear por ejemplo todo el enrutamiento que se lleva adelante en Internet y mejorar ese sistema mediante algún proceso, ¿hay algún proceso implementado para eso?

RUSS MUNDY: No. No hay ningún proceso implementado. No hay una única manera para hacerlo. Tenemos los principios de MANRS en los cuales los operadores tienen un sistema y aplican cuestiones que tienen que ver con el DNS o el enrutamiento pero tienen que adaptar el monitoreo a sus propios sistemas si es que necesitan saber si sus sistemas están siendo utilizados de manera errónea o de manera abusiva a nivel interno o a nivel externo. La coordinación es parte de la respuesta. Por ejemplo, saber con quién se contacta uno, con quién habla uno. Es así como funcionan las cuestiones y se han realizado varias pero esto implica miles de actividades y en realidad, en mi opinión, no hay una única manera de hacerlo y nunca habrá una única forma de hacer esto para el sistema de enrutamiento.

SIVASUBRAMANIAN MUTHUSAMY: Si me permite responder muy brevemente, los diferentes operadores y los diferentes niveles de expertos pueden tener alguna instancia en la cual deseen asegurar el enrutamiento. Algunos otros pueden no tener la experiencia o pueden no tener ni siquiera idea sobre cómo resolver esta cuestión. Quizá habría que crear un organismo como MANRS que pueda tener un rol en relación a asegurar el sistema de enrutamiento o a identificar cuestiones que puedan afectar. Eso era lo que yo quería sugerir.

RUSS MUNDY: Sí, puede haber ciertas capacidades de fuente abierta que existan y en ese caso no hay que gastar grandes cantidades de dinero. Quizá uno pueda invertir cierto dinero y tener un monitoreo de mejor calidad. Esa ya sería una decisión comercial. Lo que nosotros sí tenemos como parte de las recomendaciones y no tenemos en realidad ninguna recomendación para la junta directiva pero sí hemos hecho recomendaciones para los operadores de que adquieran el conocimiento necesario para poder efectivamente monitorear y responder a los ataques de enrutamiento que suceden dentro de la infraestructura. Para poder hacer eso hay que poder responder. Además, me gustaría agregar que este documento es quizá el documento más extenso. Tiene un anexo donde hay mucha información sobre la seguridad de ruteo y es el documento más completo que he visto.

Hay mucha información, muchos puntos disponibles en los anexos al documento que también van a ayudar o a contribuir a que se pueda aprender más y que se puedan encontrar respuestas a las diferentes cuestiones que surjan. Creo que esta es la última diapositiva que tengo para presentar.

JONATHAN ZUCK: Muchas gracias, Russ. Es un documento interesante desde el punto de vista de la intersección y dónde se encuentra esta intersección, ya sea en la comunidad de la ICANN o de la organización de la ICANN. Esto surge como algo que tenemos que analizar y ver si es un tema general para la comunidad y quizá tengamos que pensar, utilizar los canales de comunicación para poder tomar esto como un recurso para hacerle llegar a la comunidad de recursos. No sé si para la comunidad de la ICANN o la organización esto quizá sea un documento para ayudar a la comunidad y a la organización a mitigar estas cuestiones.

ROD RASMUSSEN: Habrá una sesión al respecto, creo que es el martes, para ver si la organización de la ICANN puede diseñar algo para la comunidad de operadores. Básicamente esto está dentro del espacio del DNS y todo lo que se está haciendo en materia de enrutamiento tiene que ver con esto. Hay mucho conocimiento en relación a los riesgos. Creo que sería de utilidad para los colegas de la

comunidad prestar atención a esto porque hay incidentes recurrentes.

También tenemos la oficina de OCTO, que ha estado haciendo creación de capacidades en este sentido. Ese es un debate que vamos a tener también con el equipo de comunicaciones oportunamente y con la organización de la ICANN. Lo que planteamos aquí es información particular que Russ ha compilado para poder brindarles a ustedes este resumen.

JONATHAN ZUCK: Si quieren leer más, hay mucha información sobre este tema. Vamos a pasar a la presentación de Julie rápidamente.

ROD RASMUSSEN: Le vamos a dar a Julie su tiempo. Después Steve Crocker tiene un minuto para hablar sobre SSAD. Después vamos a saltear uno de los temas. Después vamos a hablar del tema del que usted quería hablar. Julie, adelante. Un breve resumen, por favor.

JULIE HAMMER: Gracias, Rod. La siguiente diapositiva. Como ustedes saben, definimos las habilidades que buscábamos en SSAC. Queríamos saber cuáles eran las habilidades con las que ya contábamos en SSAC para diferentes propósitos, para la evaluación de nuevos

miembros, para autoevaluación, para actualizaciones. También usamos esto para identificar aquellas áreas en las que necesitamos nuevos miembros. Queremos compartir en particular con ustedes las brechas, aquellas áreas en las que necesitamos nuevos miembros. Precisamos miembros que vengan con esas habilidades. Debemos también, al mismo tiempo, aumentar la diversidad en distintas áreas, especialmente la diversidad geográfica. África, América Latina y Asia-Pacífico. Potencialmente también nuevos miembros que tengan formación académica y que puedan aportar habilidades analíticas. La siguiente diapositiva.

Si conocen personas o si ustedes son una de esas personas que tienen habilidades en alguna de estas áreas, por favor, contáctense con nosotros. Vamos a hacer un trabajo de difusión externa a lo largo de los próximos meses. Vamos a buscar a aquellos que estarían interesados en trabajar en SSAC que han expresado su interés. Vamos a considerar las solicitudes. Por favor, miren las habilidades que estamos buscando. Esta información está en nuestro sitio web. Si conocen a alguien que tenga estas habilidades, por favor, derívenlos a nuestro grupo. Si les interesa, contáctense con Rod, conmigo o con cualquier miembro del maravilloso equipo de personal de apoyo a SSAC.

ROD RASMUSSEN: Gracias, Julie. Si tienen alguna pregunta, contáctense con nosotros. Vamos a seguir porque no nos queda tiempo. Steve Crocker, ¿usted está disponible para hablar brevemente acerca de lo que hemos hecho con el programa piloto y el sistema piloto?

STEVE CROCKER: Yo siempre estoy preparado. Creo que tenemos una diapositiva solamente. Les voy a dar un panorama general. Como creo que todos saben, la ICANN ha estado lidiando con el problema de WHOIS o el problema de datos de registración. La situación actual es la siguiente. Hay una versión liviana de SSAD que se llama divulgación de WHOIS y que al parecer apunta a desarrollar e implementar el sistema lo más rápidamente posible. Es un sistema de incidente que envía las solicitudes a los registradores. Hay muy poco contenido en cuanto a describir cómo van a manejar los registradores estas solicitudes.

Hay una parte distinta donde el grupo de trabajo del proceso acelerado de desarrollo de políticas de la GNSO ha estado tratando de definir cuál es la revisión de las especificaciones temporarias. Están evitando cuidadosamente toda especificación que tenga que ver con cuáles serán las reglas para poder acceder a los datos no públicos.

Hay mucho por hacer por delante porque cuando se haya terminado de hacer todo seguiremos teniendo el problema de quiénes son los usuarios, qué necesitan y cómo van a acceder a esos datos. Esos debates se han postergado cuidadosamente. Estamos en una situación algo incómoda. Esa es mi situación del punto en el que estamos.

ROD RASMUSSEN: Excelente. ¿Alguien tiene alguna pregunta para Steve, para mí o para cualquier otro miembro de ALAC y de SSAC?

JONATHAN ZUCK: Dónde estamos. ¿Estamos en algún lugar? Esa es la pregunta. Si me permiten, quisiera darle la palabra a Justine o a Alan. Perdón, Alan Greenberg quería hablar antes. No había visto su nombre. Le pido disculpas. Alan, adelante.

ALAN GREENBERG: Muchas gracias. Un comentario muy breve. Quiero agradecerle al equipo de SSAC que han hecho un trabajo increíble. Han presionado mucho a los distintos grupos para que se enfoquen en los temas reales. Realmente valoro el esfuerzo y lo que él ha volcado aquí. Gracias, Steve.

STEVE CROCKER: Gracias. Creo que sería un buen momento y sería útil que ALAC expresara enfáticamente qué es lo que se necesita. Alan ha participado activamente y todos los grupos de trabajo tienen sus propias reglas pero el panorama general, la situación general es que todo esto no se está reuniendo de forma útil. ALAC es una de las organizaciones principales que representan a las personas que necesitan los datos. La gente que tiene los datos son las partes contratadas de la ICANN. Los registros, los registradores. Ellos no tienen dificultades en organizarse y sin tratar de decir nada que sea especialmente negativo con respecto a ellos, ellos se centran comprensiblemente en cómo minimizar los riesgos y los gastos. Cómo brindarles datos a las personas que los necesitan con fines legítimos no forma parte de su actividad central y no le dedican demasiado tiempo a pensar en estas cosas y a tratar de ayudarnos a organizar todo este tema y especificar cómo podríamos resolver esta cuestión de una buena forma.

ROD RASMUSSEN: Esa es la opinión personal de Steve.

ALAN GREENBERG: Sí, sin duda.

ROD RASMUSSEN: No es la posición oficial del SSAC. Seguramente alguien tendría opiniones muy interesantes al respecto. Es cierto que se está dedicando mucho trabajo pero, como dijo Steve, hay intereses contrapuestos y cuando hay intereses contrapuestos es necesario reunirse para encontrar una solución y el acceso a los datos por parte de los organismos de seguridad es uno de los temas principales en este tema pero esto no está ocurriendo. Tenemos que reunirnos todos juntos para ver cómo resolver este problema. Vamos a continuar con este tema por nuestro lado y seguramente ustedes también. Creo que esto nos lleva hacia el tema de uso indebido del DNS.

JONATHAN ZUCK: Exacto. Queremos que nos den un breve resumen de cuál es la respuesta del equipo reducido. Perdón. No estaba mirando quién había levantado la mano en Zoom. Adelante.

SÉBASTIEN BACHOLLET: Quería volver a uno de los temas que mencionaron. Es justo preguntarles a todos los participantes de la comunidad de la ICANN, pedirles que participen. Creo que el problema es que si no resolvemos el problema de las personas físicas y las organizaciones nosotros, como usuarios finales, estamos en problemas. Yo estoy hablando como europeo. No entiendo por qué no está indicado claramente en el GDPR, por qué se indica y

se habla de datos de personas individuales y no organizaciones. Podemos tratar de resolverlo de otra forma pero no entiendo cómo un usuario final podría pedir acceso a los datos, a datos que deberían estar accesibles naturalmente. Gracias.

JONATHAN ZUCK: Gracias, Sébastien. Este es un debate en curso. Lamentablemente el GDPR está redactado de forma tal que dice que lo permite pero no lo exige. Estas conversaciones aún continúan.

ROD RASMUSSEN: Brevemente. Desde el punto de vista técnico esto es legal. Es un tema de interpretación. SSAC no se siente cómodo hablando de este tema pero solo quiero decir que desde el punto de vista técnico, esto se puede resolver.

JONATHAN ZUCK: Muy bien. Adelante. Queremos llegar al tema de uso indebido del DNS.

HADIA ELMINIAWI: Un comentario breve acerca de la parte técnica porque siempre se nos dijo durante el EPDP que no hacíamos esta diferenciación

por temor a cometer errores porque las soluciones técnicas son riesgosas. No están garantizadas.

ROD RASMUSSEN: Cuando yo hablo de técnico me refiero a almacenar los datos, preservar los datos. No a tener una máquina que identifica si estamos hablando de una persona jurídica o una persona física.

JONATHAN ZUCK: Sí, hay temas de validez de los datos y también todo ese tipo de cosas. Muchas gracias. Volvemos a los temas de nuestra agenda. Justine me pasó debidamente los resultados del equipo reducido de la GNSO pero dado que ella entró en la sala quisiera pedirle a ella que nos describa brevemente el resultado de todos estos temas.

JUSTINE CHEW: No sé a quién estoy representando ahora. En términos del resultado del equipo reducido del consejo de la GNSO sobre uso indebido del DNS hubo una sesión esta mañana. Creo que fue esta mañana o ayer. Ayer, perdón. El informe probablemente esté en su etapa final. Todavía está siendo redactado. Todavía es preliminar. Básicamente hay cuatro recomendaciones que se van a presentar. Las cuatro recomendaciones, creo yo, tienen que ver con metas generales. Una vez más, cuando tengamos la

reunión con la GNSO yo quisiera ver qué opinan acerca de este tema, si piensan que es suficientemente específico, si están satisfechos pero quería decir que en la primera sesión de trabajo de la GNSO Rod y Julie estaban presentes y ustedes plantearon la posibilidad de trabajar juntos. Esto es algo que yo iba a plantear en la siguiente sesión, cuando tuviéramos la actualización de políticas de ALAC.

Desde el punto de vista de los procedimientos posteriores, porque sabemos que el grupo de procedimientos posteriores tenía una recomendación, era un proyecto holístico que abarcaba toda la comunidad pero tenemos distintos esfuerzos que están llevando a cabo en distintas partes y creo que también se mencionó hoy. Tenemos diferentes componentes, diferentes grupos que están haciendo diferentes cosas. No necesariamente cosas malas. Hacen cosas buenas pero, una vez más, trabajan en una especie de silos y esto siempre ha sido un problema en la ICANN, que todos trabajamos en silos.

Lo que usted le ofreció a la GNSO hoy en cuanto a tratar de crear un marco en el que todos podamos trabajar juntos y podamos unir los diferentes elementos, los diferentes componentes, yo quisiera invitarlos, invitar a ALAC a participar en este proyecto. Creo que ALAC seguramente querría apoyar este proyecto.

JONATHAN ZUCK: Sí, gracias. Creo que la respuesta del equipo reducido de la GNSO a estas preguntas fue muy general e implica derivar la conversación a otros en lugar de iniciar un PDP o algo así. Una vez más, creo que esto sugiere la necesidad tal como usted mencionó, Rod, de contar con una especie de hoja de ruta para poder delinear los pasos que tienen que tener lugar. Creo que nos interesaría mucho llevar a cabo este tipo de proyectos.

ROD RASMUSSEN: Si me permiten, quiero ponerlos al tanto a los colegas del ALAC, porque nosotros tuvimos esta conversación con mis colegas de las otras SO y AC. Es interesante, según mi observación dentro de ICANN, que hay una muy buena comunicación con los presidentes. Es decir, estamos todos muy coordinados pero se puede hacer mucho cuando hay mucho trabajo en curso en los subcomités.

Por supuesto, a veces hay que quitar las manos y no tocar las políticas. Lo que vamos a debatir con la junta directiva, y esto surge de la inspiración que nos dieron sus preguntas, la idea es compilar un plan, una hoja de ruta, un plan estratégico para llevar estas metas generales que tienen que ver con el uso indebido del DNS y llevarlas a nivel general de la comunidad y decirles: “A ver, es así como vamos a hacer esto. Estos son los esfuerzos que estamos llevando adelante hoy por hoy”. En la

GNSO, hoy hubo también cuestiones similares y hubo un acuerdo respecto a eso particularmente porque va a publicarse el informe del equipo más reducido.

Nuestro objetivo entonces es ayudar a la junta directiva y también a todas las unidades constitutivas y quizá crear una especie de marco de proyecto para poder abordar diferentes aspectos del problema y esto también nos va a forzar a todos a determinar qué queremos abordar y si esto está dentro del alcance de nuestra comunidad o no. Lo que quiero mencionar es que para aquellas cuestiones que pensemos que no están dentro de nuestro alcance, no tenemos que pensar de quién es el problema y tirarles la pelota sino que tenemos que trabajar agresivamente. Quizá deberíamos reconsiderar si es o no realmente nuestro problema, nuestra cuestión a resolver. Esa es una observación personal de toda esta cuestión. De eso estamos hablando y es de lo que vamos a hablar mañana y en las sesiones siguientes.

Esto está liberado, por así decirlo, a los miembros de la junta directiva. Vamos a ver luego y después vamos a tener que coordinar el trabajo conjunto con lo que está haciendo el GAC, con lo que está haciendo la GNSO, con sus diferentes esfuerzos. También el trabajo que están haciendo otras partes u otras unidades constitutivas, las partes contratadas. Es decir, la idea

es reunir todos esos esfuerzos y, como comunidad, ponernos de acuerdo sobre cuál es el plan.

Otro beneficio también sería mostrar que la comunidad de la ICANN en general es quien está abordando esta cuestión y tiene un plan, tiene métricas y tiene entregables porque ahora en el mundo hay mucha gente que habla y dice: "Apareció este problema y la ICANN no está haciendo". No, no. Nosotros trabajamos y trabajamos mucho pero no podemos mostrar resultados si no tenemos una historia para contarles. Eso lo podemos hacer a través de las métricas y eso sería interesante. Es todo de mi parte.

JONATHAN ZUCK: Gracias, Rod. Se trata de eso básicamente. La cámara de partes contratadas trabaja muchísimo. De hecho, tiene el Instituto del Uso Indebido del DNS y la cámara de partes contratadas es un grupo separado en cuanto a que ahora por ejemplo están teniendo una reunión específica del tema para poder determinar también cómo van a organizar sus reuniones.

Yo diría que el próximo resultado neto de estos esfuerzos es intentar lograr una definición un poco más acotada del uso indebido del DNS dentro del ámbito de la ICANN. Esto es lo que tenemos que lograr. Garantizar que podamos llegar a esa definición. Hasta cierto punto fue la postura del ALAC donde se

decía que no era necesario definirlo para mejorar pero se nos dijo que si acotamos la definición vamos a empezar a hablar de las definiciones pero, al mismo tiempo, la definición cada vez se torna más compleja. Hay que ser cuidadoso respecto de los términos que utilizamos y cómo procedemos. Creo que ese sería parte del debate de la conversación.

La otra parte del debate o de la conversación son los datos. Esta es una comunidad que genera datos. La ICANN en sí tiene el DAAR y también tiene listas negras y tiene datos que resultan interesantes de rastrear. El Instituto del Uso Indebido del DNS ha logrado sus propias métricas para medir el uso indebido del DNS y se centra en los nombres de dominio maliciosamente registrados. De alguna manera el secuestro de nombres de dominio ha sido empujado fuera del alcance de la ICANN. Rod, tenemos que ver también hacia dónde va esto porque tenemos nuestros proveedores de hosting y hay una gran superposición entre las actividades de los registradores y los proveedores de hosting.

Por ejemplo, tenemos revendedores como Tucows y una comunidad relativa a esto donde se venden los dominios a diferentes personas. También podrían ser los mejores para poder gestionar estas cuestiones de los nombres de dominio pero la pregunta es si simplemente les decimos que esto no nos interesa, que no es nuestro problema, o si vamos a incorporar

más personas. Si vamos a tener más influencia dentro de los registradores para que se gestione esto en la comunidad. Es decir, si les pasamos la pelota directamente y la arrojamos fuera de la cancha porque esto no tiene nada que ver con nuestra misión o si realmente abordamos la cuestión de manera efectiva.

Quiero ver si hay algún comentario o alguien quiere tomar la palabra. No veo que haya ninguna tarjeta levantada. Tampoco veo manos levantadas en la sala de Zoom. Los invito a todos a que lean el informe preliminar que va a publicar el equipo reducido de la GNSO en materia de uso indebido del DNS. Se centraliza en los nombres de dominio y nosotros nos centramos también en ese tema en nuestra respuesta a la pregunta. La respuesta fue sí, nos tenemos que focalizar en eso pero en realidad no teníamos como objetivo excluir otros temas. Si hablamos de las registraciones a granel y los volúmenes de operaciones, creo que hay cierta respuesta a alguna de las cuestiones que se han planteado y tenemos que garantizar también que estemos al tanto y reconozcamos estas respuestas. Pero bueno, tenemos que trabajar de forma conjunta con ustedes en esta hoja de ruta. Gabriel Andrews tiene la palabra. Adelante.

GABRIEL ANDREWS: Gracias, Jonathan. No sé si tengo que hacerles esta pregunta a ustedes o a los colegas del SSAC. Nosotros mencionamos cuestiones como por ejemplo la complejidad del mercado de revendedores y la complejidad que tiene el tema para los registradores y otras partes que tienen intereses comerciales en esta cuestión. También los servicios de representación y privacidad. Me preguntaba entonces hasta qué punto existe un buen mapa u hoja de ruta para determinar si estos sistemas que se implementaron oportunamente siguen siendo válidos o si requieren una actualización. No sé si los colegas pueden responder esa pregunta, si están al tanto.

ROD RASMUSSEN: Creo que aquí podemos hablar de un mapa de mercado, un mapa de infraestructura. No sé si la ICANN ha hecho algo parecido a eso porque todo se complica rápidamente y es necesario entender qué tipo de compromiso implica cada cosa, qué proveedores están involucrados con determinadas reglas. A veces se torna en una especie de árbol de decisión donde una cosa depende de que otra cosa no se haga o son dos cuestiones que toman un camino diferente. Hay gente que sí tiene estos mapas de mercado disponibles pero sería un proyecto también a tener en cuenta, si es que no lo han hecho. Podríamos tener algún mapa de decisión. Llámenlo como quieran. Podría ser un mapa de uso indebido para abordar determinadas cuestiones y

que nos permita tener algo del estilo académico. Creo que sería algo interesante de tener para poder ayudar a informar esos esfuerzos de coordinación y de planificación porque todavía existen ciertos malos entendidos que son fundamentales en todo este tema sobre quién tiene la responsabilidad y en qué sentido.

JONATHAN ZUCK: Eso es verdad. Nos preguntamos si tendría que haber una frontera respecto de lo que consideramos el ámbito de la ICANN o no. Ahora el personal me está indicando que nos hemos excedido un poco de tiempo. Les pido que les agradezcamos a los miembros del SSAC, a Rod, a Matt, por venir.

ROD RASMUSSEN: Gracias por invitarnos.

JONATHAN ZUCK: Vamos a continuar entonces hablando del tema.

[FIN DE LA TRANSCRIPCIÓN]