BEIJING – Nueva Actualización de Seguridad, Estabilidad y Flexibilidad (SSR) de gTLD
Lunes, Abril 08, 2013 – 15:00 to 16:30
ICANN – Beijing, República Popular de China

MATT ASHTIANI: Damas y caballeros les pido que den la bienvenida al director de seguridad de ICANN Jeff Moss.

JEFF MOSS: En primer lugar necesitamos un micrófono. Podemos empezar entonces. Este es la actualización del comité de seguridad de estabilidad y flexibilidad, entonces lo que vamos a hacer es ver cuáles son los riesgos que están vinculados con el programa de nuevos gTLD.

Tenemos mucha gente acá en el panel y espero que ellos nos den sus ideas y nos hablen de los temas que les competen y al final de la sesión les vamos a pedir a ustedes que hagan preguntas y esperamos tener un fructífero debate sobre estos temas.

Entonces, queremos que esta sea una sesión muy interactiva. No vamos a tomar preguntas durante la sesión, lo vamos a hacer al final. Así que les pido por favor que guarden las preguntas para ese momento, el panel se va a quedar hasta el final.

Acá en el escenario con nosotros tenemos al vicepresidente de las operaciones gTLDs, Christine Willett. Tenemos el VP de IANA, Elise Gerich. Tenemos al jefe de seguridad de VeriSign, Danny MacPherson. El director de operaciones DNS de ICANN, Joe Abley. Tenemos al director

senior de seguridad y estabilidad y flexibilidad del equipo de seguridad, John Crain. También tenemos al presidente del SSAC, Patrik Faltstrom. Tenemos al jefe de Google, Warren Kumari. Y también a la analista de tecnología senior de ICANN Steve Sheng.

Vamos como todos sabemos a hablar de que la seguridad en ICANN es algo muy importante como lo hemos dicho varias veces. Esta en estatutos según fueron reformados el 20 de diciembre de 2012, entonces nuestra misión es coordinar a nivel global el sistema de internet y los identificadores únicos. Y en particular garantizar la operación segura y estable de estos identificadores.

Entonces como pueden ver, acá al frente tenemos el párrafo uno y dos en la declaración de misión, y esto es algo que tomamos con suma seriedad.

Como una organización de múltiples partes interesadas global, ICANN trata de facilitar la seguridad de estabilidad y flexibilidad de el sistema de identificador único de internet a través de la coordinación, colaboración y operación. Y esto obviamente no se limita a las funciones técnicas de ICANN.

Como dije anteriormente, nos vamos a concentrar en el nuevo programa de gTLD y tenemos tres funciones. La primera es el gestionado dentro de la organización de ICANN y es ahí donde ICANN tiene una responsabilidad operativa. El segundo es para ICANN la comunidad a la que tiene que asistir, esto tiene que ver con la comunicación. Y finalmente para que lo considere la comunidad global.

Ahí es donde tratamos de facilitar el diálogo, de generar un consenso. Entonces todo esto vuelve a facilitar coordinar y operar. Algo que quiero señalar y que resulta muy obvio es que no existe una cosa como el 100% de seguridad. En realidad se puede volver loco tratando de hacerlo, nada dentro del internet es 100% libre de riesgo, todos lo sabemos.

Entonces lo que tratamos es de gestionar el riesgo. Y los profesionales de la seguridad saben que siempre hay que pagar algo por ese riesgo, siempre hay que correr un riesgo y tratar de manejarlo. Parte de la situación es que sabemos cuál es el riesgo y tratamos de mitigarlo.

Vemos cuál es el costo, el impacto, tratamos de gestionarlo y obviamente disminuir el impacto lo más posible. Necesitamos un proceso que esté implementando para identificar y mitigar esos riesgos. Sabemos que hay riesgos en el nuevo programa de gTLD, tenemos que ser flexibles para tener un proceso que pueda adaptarse para esta seguridad.

ICANN como único operador va en coordinación con la comunidad. Es por eso que yo quiero tener la participación de la comunidad, porque si hay un problema todos nosotros vamos a tener que solucionarlo, ICANN no puede tener la solución mágica y resolver todos los problemas que se presentan.

En el sistema de DNS como dijimos es un sistema complejo, un ecosistema complejo. Pero es único que no esté pautado, porque tenemos décadas de operarlo. Cuando miramos al pasado la comunidad ha tenido varias expansiones, hemos sobrevivido cuando pusimos el DNSSEC con distintos tipos de registros de recursos, el TSIG, los registros

AAAA, el cambio en los protocolos de EDNS0, y no hubo ningún problema en el servidor raíz.

Hemos hecho la transición al enrutamiento al Anycast para que fuera más flexible el sistema, y también nos fue bien como comunidad. Entonces cuando tengamos problemas, o no tengamos problemas, tenemos que actuar juntos como comunidad y resolverlos todos juntos.

En la siguiente imagen pueden ver una actualización de lo que mostró Fadi con el programa de los nuevos gTLD, y quiero señalar esta parte inferior donde aparece el SSR. Quiero mostrar que en cada nivel de ICANN nosotros reconocemos que la seguridad de estabilidad y flexibilidad de la internet está en el puesto nº1 de prioridades. Todo se basa en esta base.

Entonces no hay forma de que la seguridad, estabilidad y flexibilidad de internet pueda poner el sistema de identificadores únicos de internet en peligro. Es por eso que Christine Willett, que estuvo hablando de la posibilidad de tener todo listo y en tiempo, le voy a pasar el micrófono.

CHRISTINE WILLETT: Acá tenemos entonces los bloques que hablan de los componentes del programa de gTLD. Empieza con las solicitudes que se presentaron en junio del año pasado, hablan del sorteo de asignación de prioridades, ya estuvimos hablando en la evaluación inicial o IE.

Y cuando miramos el futuro lo que nos falta para que estén operativos los gTLD, pasamos a la parte de los casilleros azules, que tiene que ver con los contratos y su aprobación. Una vez que los solicitantes pasen esta etapa de los contratos, están en la evaluación de pre-delegación.

Una vez que se pasa esta prueba se puede decir entonces que se completaron los programas, las responsabilidades. Y después emitimos una notificación al notificante y notificamos a IANA de que ya se han aprobado todos estos pases y ahí entonces se da una credencial de autenticación para decir que el solicitante puede ir a IANA y pedir directamente la delegación.

Después ya estuvimos hablando de lo que es el TNCH, que es el centro de información y protección de marca. Todos estos cambios van a estar operativos a partir del primero de Julio, después del periodo de registro como para que empiece a funcionar en Agosto.

Tenemos el URS, el sistema uniforme de suspensión rápida. También va a estar listo en Julio el EBERO, que es el registro de emergencia para operación del backend, también operativo a partir de agosto.

Estos son los componentes del nuevo programa de gTLD, como mencionan la guía del solicitante. Y este es nuestro cronograma para que estén listos y ya disponibles los nuevos gTLD.

Una vez que terminemos con esta etapa, y el participante haya pasado por todos estos pasos, se le va a pedir a IANA que haga la delegación de los nuevos gTLD. Después se va a hablar y va a hablar Elise Gerich, de la delegación de IANA.

ELISE GERICH: Muchísimas gracias Christine de hacer toda esta de la perspectiva de IANA de los nuevos gTLD es un procedimiento estandarizado. Las cosas que tenemos que hacer para estar listos para manejar cinco veces más

de gTLD que los que tenemos ahora, es hacer mejoras en el sistema de automatización que tenemos implementado, que se llama ARSM.

Fue lanzado en 2011, estamos generando con VeriSign y NTIA este nuevo sistema RZM que es el de zona raíz. También vamos a tener una memoria donde diga que alguien ha cumplido con todos los requisitos, y va a ser como una lista de verificaciones.

Estamos trabajando con el equipo de Cristina para que esa lista esté lista durante el nuevo proceso de gTLD. Y además contamos con personal adicional.

Básicamente como hablé antes de la automatización, nosotros hemos implementado un nuevo flujo de trabajo que permite crear nuevos gTLD. En el pasado teníamos muy poco gTLD que eran creados, y por ese motivo el proceso nunca tuvo mucha prioridad en la asignación de automatización.

Ahora que ya hemos terminado con las pruebas la semana pasada, y los hemos hecho también junto con nuestros socios en la RZM, sabemos que vamos a poder estar productivos para el primero de agosto.

La lista de verificación y de un informe. Como los solicitantes de gTLD tiene que cumplir con un proceso para tener distintos paneles de evaluación, y Cristina estuvo más de una hora hablando de eso y conoce mejor que yo, así como ustedes. Entonces se sigue adelante todo ese proceso y después va a haber una verificación, un casillero para verificar.

Una vez que esto esté realizado, se realizan todas las verificaciones en esos casilleros, se va a emitir una credencial. Y en ese momento pueden

llevar esa credencial y estos casilleros de verificación van a estar en línea y entonces pueden pedir la delegación al departamento de IANA.

Este es un prototipo, no es exactamente la forma que va a tener el sitio de IANA, quizás lo puedan ver. Pero básicamente lo que si dice acá al final es que pone la caracteres del nuevo gTLD, tiene el ejemplo que dice que cargan esto, tipea las credenciales que van a salir para el nuevo gTLD. En ese momento, ya iniciaron el proceso entonces de la delegación y en ese procesos lo que hacemos son las cosas estándar para todos los TLD.

Hacemos una verificación técnica una vez más para ver que los nombres funcionan correctamente, llegamos a los contactos que están en la solicitud para ver que sigan existiendo, y entonces una vez completado ese procedimiento sabemos que podemos trabajar y lo vamos a hacer junto con nuestros socios en el TIA y VeriSign en la zona raíz porque entonces sabemos que todo este sistema de automatización va a poder estar funcionando el primero de agosto.

JEFF MOSS: Una vez que se termina la delegación, quería hablar un poco del sistema de servidor raíz y el impacto que va a tener con todos estos nuevos gTLDs que se van a agregar. Esto también tiene que ver con cómo se va a escalar, medir, monitorear. Y también tenemos al director de operaciones DNS de ICANN que nos va a poder hablar, así como la persona de VeriSign, así que Dani.

JOE ABLEY: Lo que tenemos acá es algo que surgió en San Francisco. Lo que demuestra es el crecimiento del tráfico en la internet, que es independiente de los TLD. Nosotros esperamos que los nuevos gTLD tengan mucho más tráfico, que el tráfico en la zona raíz sea mucho mayor.

Lo que vemos acá, que quizás sea difícil ver, pero vemos un crecimiento por década en la delegación de la zona raíz. Vemos cien TLDs nuevos, un crecimiento modesto para los últimos diez años, y podemos ver cómo aumenta para el lado derecho, vemos que la zona raíz sigue siendo pequeña. Hay una gran experiencia entre muchos de los operadores acá en la audiencia que manejan el sistema raíz, y va a crecer mucho más que la zona raíz actualmente.

La zona raíz es importiva y también es importante ser conservador, porque esa zona tiene que ser estable.

JEFF MOSS: ¿Te parece que esto es bastante preciso, Danny?

DANNY McPHERSON: Sí, creo que es preciso. Hay que ver que los últimos catorce años aproximadamente hubo 76 delegaciones o algo acá, casi 5 por año. Y lo que ahora estamos esperando es tener, no sé, que va a haber 45 o algo así cada 36 horas.

Entonces es un ritmo diferente que vamos a tener. Si hablamos del 2009 por ejemplo se hizo un estudio en ICANN de las capacidades y las

distintas implicancias en el sistema de la zona raíz, para ver si se podía escalar.

Y una de las cosas clave que surgieron para abordar era la capacidad de generar sistemas que pudieran atender a todo el sistema de servidor raíz. Esto nos da una perspectiva central, concentrándose en el consumidor.

Y, sin que esto establezca la base, quizás en este caso vamos a tener que apretar un poco más el acelerador y sea un poco más riesgoso. El SAC 46 expresó esto en la recomendación 4 en el SAC 46 que hablaron de la necesidad de una alerta temprana, así como también un estudio del escalamiento de raíz. Quiere relación con las operaciones de de la raíz.

JEFF MOSS: Bueno, pero vas a tener que mantener tus puntos durante toda la sesión, no todos juntos. Entonces por favor andá de a uno.

DANNY McPHERSON: Perdón. En el estudio de escalamiento de raíz en el SAC 46, hubo un requisito para ICANN, como para que hubiera visibilidad en todo el desempeño de todo el sistema. Y creo que muchas de las recomendaciones que hizo el SSAC y sus expertos tenían que ver con este nuevo programa de gTLD y en la existencia de esa visibilidad.

Definitivamente tenemos que llegar a ese paso antes de acelerar completamente.

JEFF MOSS: Gracias Danny. Bueno Joe, ¿cómo se han recopilado esta estadísticas de la raíz L?

JOE ABLEY: Bueno, dentro del SSAC hay varias métricas pero sigue habiendo un debate y me parece que tenemos que decir que gran parte de ellos bastante estables. Hay métricas que fueron recopiladas por cada uno de los operadores de la raíz y fueron publicadas para ver cuál era además el desempeño de la raíz L.

Como dijo Danny primero hay que establecer una línea de base para saber cómo se opera y qué es lo que va a pasar con el crecimiento. Y cuando empiece el programa de gTLD, seguir monitoreándolo y ver cuáles son las soluciones. Como dijimos no pensamos que va a haber ningún problema, que es un sistema seguro y que lo operamos en forma conservadora.

Entonces el 3 de abril empezamos a publicar los datos, fueron recopilados en los dos mese previos sobre la base de la recomendación borrador inicial de la persona que es nuestro enlace con el RSSAC, que es Peter Cock.

Acá tenemos un ejemplo, si vamos una imagen para atrás. El anuncio habla de las estadísticas que se van a actualizar una vez por semana, todos pueden ir y rastrear los distintos aspectos de la zona L y también todas las métricas recomendadas por el RSSAC, que son las que recopilamos.

Entonces estas son las primeras estadísticas publicadas pero nosotros sabemos que va a haber otras estadísticas de otras raíces, no solo la L.

Acá tenemos por ejemplo estas imágenes gráficas que son dos bases de datos. Lo que demuestra es que el tiempo que lleva distribuir una nueva sola raíz en todo el sistema existente son 300 Anycast globalmente, incluyendo nodos en algunas áreas que no tienen mucha conexión. Y se tarda unos 4 segundos aproximadamente.

Sin dudas vamos a ver nuevas líneas que suben y que bajan porque tenemos que distribuir una zona en la internet y esto varía diariamente. Lo importante en este gráfico no son los primeros dos meses, sino hacer un seguimiento de los gráficos a medida que pasa el tiempo y a medida que nos acercamos a la delegación y después, para ver qué es lo que pasa con los tiempos de distribución para las nuevas zonas raíz en internet.

Para ponerlos en contexto tenemos un tiempo de distribución de 4 segundos para una zona publicada hace dos días, creo que 4 segundos en 12 horas no es demasiado. Hasta ahí hemos llegado en la actualidad.

Acá tenemos el tamaño de la zona raíz medida por diferentes medidas. Acá tenemos kilobytes, y lo que ven acá en Julio de 2010 es la firma de la zona raíz para ver cuáles son las claves en la firma y la expansión. Eso es lo que tiene que ver con la zona raíz pero podemos ver que en esta línea naranja va a seguir creciendo a medida que empiecen a delegarse los nuevos gTLDs. Le voy a pasar a John entonces.

JOHN CRAIN: Quiero mostrarles algunas otras estadísticas que tenemos en el sistema de servidor raíz. Hay un programa que está siendo operado por el operador RIPE NCC en Europa, realmente es muy grande. Y lo que

podemos ver, no sé si ustedes lo pueden ver acá, es mirar la ruta L (igual lo hacen con todos los servidores raíz), pero este es el de raíz L. Y vemos los tiempos de consulta a la raíz L, con qué velocidad lo puedo ver.

Cada uno de estos nuevos nodos.. es una forma de rastrearlo y ponerlos en bases de datos. Es una forma gráfica de mostrar los datos, son cosas que se miden. Pero de hecho hay algunos datos, hace algunos años que estamos recopilando estos datos, y no es que yo o ICANN lo esté haciendo. Sino que es un tercero que lo está haciendo, y obviamente vamos a compartir estas.

Estamos hablando de las estadísticas de la raíz L y vemos el formato de los datos, cuál es el formato de los datos que presentamos para mirarlos. No voy a hablar de todos los servidores raíz, lo vamos a hacer después. Pero estos son las rutas de los servidores raíz y las estadísticas publicadas por cada uno.

Yo creo que todos recopilan pero tienen interfaces públicas a las que pueden acceder para chequear esas estadísticas. No es el formato. No se trata solo de la forma en la que colaboramos, por ejemplo en la raíz F tenemos responsabilidad junto con ICANN, tenemos cartas de intención para saber cómo seguir adelante.

Y ellos no están diciendo, sí esta es nuestra responsabilidad, la estamos tomando con seriedad, vamos a colaborar. Y hay otros lugares como sitios web donde figura esto.

Estos operadores de servidores raíz vienen a las reuniones de ICANN, es gente responsable, participa de los comités asesores y los van a ver cada vez más en estas reuniones de ICANN. Pero es gente de operaciones

que lo que hace es operar el sistema de DNS y colaboran regularmente. Se reúnen cada 3 años para hablar de temas operativos.

JEFF MOSS: También hacen pruebas de los sistemas de respuestas.

JOHN CRAINE: Sí, también hace su colaboración sistema de colaboración, por ejemplo nuestros amigos de VeriSign son grandes socios y ayudan a financiar todo esto. Y hemos visto este tipo de cosas en el pasado, internet sigue funcionando. Así que no estamos esperando que las cosas desaparezcan o pase algo de un día para el otro cuando aparezcan los nuevos gTLD. No sé Danny si querés agregar algo.

DANNY McPHERSON: Sí. Quiero agregar algo. No vemos la raíz AIJ, que son dos de las tres raíces que operan VeriSign y definitivamente nuestra intención es que en la segunda mitad del año podamos tener sitios web con información pública. Hacemos una recopilación bastante exhaustiva de estas estadísticas y respecto de los aspectos contractuales operamos un contrato con el departamento de comercio de los EE.UU, desde el punto de vista del contrato con ICANN hoy en día hay mucho en la carta de compromiso que tiene que ver con el cumplimiento regulatorio.

La función de CSO de VeriSign tenemos 1385 controles de cumplimiento regulatorio que son monitoreados continuamente, auditados para la alta seguridad, etc, etc. Existen auditaciones y verificaciones continuamente, los monitoreamos y estamos seguros que respecto de

las obligaciones contractuales con ICANN todas son cumplidas y que resulta aceptable para una publicación de datos o demás perspectivas.

JOHN CRAIN: Estos mapas son servidores de raíz. Este parece como si fuese el último mapa, o como si fuese el que no estamos familiarizados, y nos muestra la extensión de los servidores de raíz.

A veces nos preocupamos si tiene o no tiene capacidad. Tiene mucha capacidad, no puedo decir exactamente cuánto, pero les puedo decir que la raíz L tiene 300 nodos y cada uno de ellos tiene una capacidad muy alta en cada una de las máquinas. Y tenemos mucha infraestructura para discontinuar estos operadores.

Si lo miramos a esto de acá a 6 meses, seguramente vamos a tener mucho más. Hubo varias cuestiones con los servidores de raíz, antes teníamos solamente 30 y esto está evolucionando. El sistema de servidores de raíz continúa evolucionando en el DNS y la internet también evoluciona.

Nosotros vamos a continuar y vamos a mantenernos con lo que sucede con esto.

JEFF MOSS: Vamos a pasar ahora a otra sección y vamos a hablar ahora sobre el enfoque de ICANN para hablar de los temas que no son conocidos. Son temas que fueron surgiendo que quizás nos agarraron un poco fuera de guardia, y tenemos que enfrentarlos.

Tenemos que tener programado un plan de mitigación. Para el próximo caso vamos a hablar sobre un informe con el que ustedes están muy familiarizados, que es el SAC 57, y que va a ilustrar la forma en la que ICANN quiere continuar con esta situación. Le voy a pasar ahora la palabra a Patrik Faltstrom, el es el presidente del SSAC.

PATRIK FALTSTROM: Muchas gracias. Antes de pasarle la palabra a Warren Kumari, que es quien nos van a explicar los detalles del SAC 57, les voy a explicar un poquito cómo llegamos a este informe.

Primero, SSAC está operando sobre la base de acciones y esto puede ser disparado por cuestiones externas que recibimos de la junta o cualquier otra parte de ICANN o de la comunidad. Pero también puede ser el caso que tenemos una acción autoiniciada, en la cual una persona de SSAC abre un ítem y habla de esa cuestión.

Esta es una de las cuestiones autoiniciadas. Warren, no sé muy bien qué es lo que hiciste cuando te enfrentaste a esto pero hablamos mucho de este asunto.

Otra cuestión que puedo decir de este informe específico es que todos sabemos que estas son las cuestiones que deben ser detectadas cuando hacemos una investigación y un análisis de riesgos sobre el que la gente habló antes. Pero todos también sabemos que sin importar lo profundo que sea este informe y sin importar cuánto asimilamos, todas son cuestiones difíciles que vamos a detectar. Por eso es importante ver cuál es el defecto.

La disponibilidad, la preparación tiene que poder ayudarnos a prepararnos y este es un ejemplo en el que nosotros detectamos este informe.

Lo primero que hicimos fue que en lugar de que el informe sea público inmediatamente, se lo pasamos al equipo de seguridad del ICANN porque pensamos que era serio y que ICANN tenía que tener una política de divulgación.

Hay varias cuestiones que tuvimos que ir mejorando a causa de este informe pero a causa de que lo hicimos el reclamo de la comunidad ya estaba ahí para ir avanzando. Con esto le voy a pasar la palabra a Warren Kumari que va a describir qué es el SAC 57.

WARREN KUMARI: Voy a ir muy rápido porque tengo mucho material y voy a ir explicándoles. Cuando uno hace un SSO o una conexión segura a través de un https, el navegador recibe una clave pública que está encriptada, y esa clave pública la incluye en un certificado que está certificado por una autoridad de certificación, está firmado.

La firma de esta autoridad de certificación básicamente compra la clave pública para la identidad, la identidad es algo así como www o algo parecido. Cuando el navegador la empieza a usar se asegura de que la firma sea correcta y que esa firma funcione, que el certificado sea válido, que no haya expirado. Y también que haya una conexión al certificado.

Cuando el CA entrega el certificado tiene que primero validarlo. ¿Cómo hace la validación el CA, especialmente con los certificados? Se envía un

email a una dirección, por ejemplo ejemplo.com con una dirección de email que ya existe en el WHOIS, y este email tiene un ticket y la persona que recibe el email responde al CA y controla.

También hay otro tipo de certificados que son de otra clase que se llaman internos y están diseñados para hacer otro tipo de cosas. Por ejemplo Microsoft Exchange, Active Directory otros tipos de servidores. Y la identidad de estos servidores es el.corp, o www.accounting o mail.test, y hacen certificados diferentes.

Y es el hecho de que la identidad no describe qué es lo que ocurre con el TLD. Pero también esto significa que el CA no tiene lugar para fijar el email de validación.

¿Qué sucede entonces cuando la etiqueta interna se convierte en un TLD? Una vez que se delega, ¿qué es lo que ocurre?

La respuesta corta es algo malo. Pasan cosas malas. Busca el certificado www.site que tiene que ser validado por una persona,.skill.forge

Y luego si yo presenté mi pedido al CA y me pusieron un cuadro que me dice que tiene que haber un nombre B que tiene que ser www.site va a haber una alertas, luego 3 o 4 horas más tarde me mandan un email y ahí ustedes pueden ver el nombre de la organización, que soy yo.

El tema que es el www.site agreguemos un nombre adicional que tiene que decir www.site y después algo más.site. ¿Qué puedo hacer entonces con esto?

Para demostrar yo delegué.site, me lo delegué a mi mismo y luego establecí un servidor web. Fui navegando en el zafari y me aseguré de

que aparezca el ícono con el candado. Y ahí dije, bueno parece que es válido, funciona. Luego lo hice también en Chrome, Explorer, Firefox.

Entonces, ¿cuáles son las otras implicancias que tiene esto? Puedo ir avanzando y ver la lista de los TLD a los que apliqué y recibo un certificado para estos TLD. Tengo que confiar en ese certificado y esperar que el TLD sea delegado.

Una vez que esto ocurra va a un Starbucks por ejemplo, a un hotel, a un dominio que está spoofeado o a cualquier otra persona que tenga un DHCP. Cuando alguien va navegando en esto le aparece el ícono del candado y luego hace lo que puede con el dinero.

Tenemos algunas recomendaciones a las que tenemos que llegar, en el foro del CA es un grupo de industrias que representa a la CA, también tiene que haber una política de debate sobre cómo hacer con esta información la comunicación, luego informar a las partes, tener un plan de contigencia, etc, antes de delegarlo.

Ahora le paso la palabra al equipo de seguridad que nos va a explicar cómo operamos.

JEFF MOSS: Le paso la palabra a Steve Sheng.

STEVE SHENG: Gracias Jeff. Con el SSAC tomamos este tema muy seriamente y después del informe de teleconferencia le comunicamos al equipo sobre el equipo de mitigación que se reunió antes del informe del SSAC. Entre enero y febrero eso fue lo que hicimos, tuvimos varias teleconferencias

con el presidente del CBA, la mayoría de los Cas los alertamos sobre este tema y nos invitaron a hablar en una reunión en febrero. Ahí es donde presentamos formalmente este tema ante ellos.

Ellos también tomaron este tema muy seriamente y quiero decir que esta cuestión de los certificados de nombres internos en el año 2010 aparecieron las fronteras. Creo que en este caso los CAs actuaron muy rápidamente, presentaron el 96 del cual voy a hablar en la próxima diapositiva.

La fecha clave es el 20 de febrero, hubo un procedimiento de votación y se aprobó esto, con lo cual el voto del 96 que fue pasado redujo la ventana de vulnerabilidad. Luego, una vez que finalizamos este asesoramiento como fue recomendado por el SSAC el 15 de marzo, notificamos este tema a todos los nuevos solicitantes de nuevos TLDs.

Vamos a la diapositiva anterior. Ballot 96 recomendó a los CA que dejen de emitir certificados internos inmediatamente y dentro de los 30 días después de que ICANN aprobó un nuevo TLD. ICANN firma un contrato con los operadores y tiene que cesar de emitir este tipo de certificado después de la publicación de un contrato, los CA tiene que revocar cada uno de estos certificados en un nuevo subfijo de TLD.

Después de las obligaciones enviamos un servicio de notificaciones a los CA para notificarles cuáles son las cadenas de caracteres que se solicitan y cuando un contrato se firma entre ICANN y un operador de TLD, nosotros enviamos una notificación a los CA para ayudarlos a descubrir estos plazos.

Hay algunos riesgos remanentes en estos asuntos, en las próximas diapositivas planeamos hablar sobre cuáles son estos riesgos y cómo estamos planeando mitigarlos. Quiero invitar a la comunidad a que nos dé sus aportes también.

El primer riesgo es que nosotros esperamos que la mayoría de las autoridades de certificación cumplan con el Ballot 96. Es posible que algunos CAs no cumplan con el Ballot 96 hasta que formalmente eso sea un requisito de auditoría, por ejemplo para WebCast, para America del Norte y ETSI para el estándar europeo, todos los CAs tienen que ser incluidos en la lista de la raíz.

La estrategia para esto es que nosotros comunicamos estos riesgos y activamente trabajamos con las partes que pueden ayudarnos. Algunas de estas partes con las que trabajamos son los navegadores, para que tengan una acción proactiva en pedirle a los CA que cumplan con el Ballot 96.

Creemos que este riesgo tiene que ser mitigado. El segundo riesgos es seguir varias razones, básicamente por cuestiones de perfomance de cumplimiento. Algunos navegadores no chequean entiempo real la verificación.

La revocación, podría ocurrir que un CA revoque un certificado pero si el navegador no lo verifica, todavía hay una ventana de vulnerabilidad en el cual el certificado aparenta ser válido.

Nuestra estrategia es comunicar estos riesgos, ya nosotros comunicamos esto junto con los navegadores y estamos discutiendo

con los navegadores sobre cómo abordar estos temas de la mejor manera.

Hay varias cosas que se están proponiendo, estamos siendo muy activos en el debate con ellos.

Tercero, es posible que exista una ventana de vulnerabilidad entre la firma del contrato de ICANN y un operador de TLD y el momento en que el operador de TLD activa el dominio de segundo nivel. Este gráfico muestra un cronograma. Si contamos 120 días es más o menos 17 semanas, si empezamos en la semana cero y firmamos el contrato en esa semana, después pasamos al testeo de predelegación. Hay luego un período de preregistro, y después viene el registro.

Creo que todo esto nos muestra que todavía puede existir una ventana de vulnerabilidad y sobre este tema realmente queremos buscar el apoyo de la comunidad sobre cómo nosotros como coordinadores tenemos que mitigar de la mejor manera este riesgo.

Como Jeff mencionó antes, y creo que Patrik también lo dijo, a veces es imposible anticipar todos los riesgos antes de tiempo. Lo que tenemos que hacer es estar listos para actuar y tener un proceso. Le voy a pasar la palabra a Jeff.

JEFF MOSS: Gracias Steve. Me gustaría que esto sea más largo, pero básicamente este es un flujograma de nuestras vulnerabilidades, nuestro proceso divulgado de vulnerabilidades que adoptó ICANN y que publicó en el mes pasado. Y que lo privatizamos al tema del SAC 57.

Queríamos asegurarnos de que funcionase y afinarlo un poquito. Esta es la manera en la que vamos a enfrentar la divulgación de las vulnerabilidades. Hay varias formas que podemos hablar de las divulgaciones.

Piénsenlo de este modo. Ustedes en la comunidad pueden encontrarse con un problema en el que hay un software de servidor de raíz o de nombre, y esa información se la podemos mostrar a ICANN. Nosotros vamos a utilizar este proceso para identificar cómo vamos a divulgar esta información a las partes afectadas.

En otra situación, ICANN puede ser la parte afectada. Ustedes pueden encontrar una vulnerabilidad en alguno de los servicios web o aplicación web y entonces ustedes vienen a nosotros y nos dicen “ICANN, yo quiero contarte un problema que encontré”. ¿Cómo va a funcionar esto?

Ustedes van a publicar mi nombre, va a ser transparente. Quizás no quiero que publiquen mi nombre, por eso nosotros vamos a ir siguiendo este proceso al divulgar nuestra propia vulnerabilidad.

Es una forma genérica de hablar de las notificaciones de los terceros y coordinarlo entre aquellos que no quieren ser puesto en contacto directo con las partes afectadas.

Este es un gráfico bastante nuevo que lo pusimos en nuestro SSR para nuestra comunidad, pero por si no pudieron verlo básicamente es una visualización de cómo ICANN tiene un enfoque general para enfrentar el riesgo y la comunicación con la comunidad.

Esta es nuestra diapositiva final en la presentación y ahora todos ustedes que han anotado las preguntas, es el momento de hacerlas. Sé que tenemos algunos representantes en la audiencia.

DANNY McPHERSON: Quisiera hablar de otra cuestión más antes de tomar las preguntas. Tengo un comentario sobre la diapositiva nº 45.

En realidad es la 44. Una de las cuestiones que yo quiero mencionar, y Warren habló de este punto en el CCNSO, o en las reuniones de ALAC, es que no me parece a mi que haya acuerdo…Patrik me puede corregir si estoy equivocado pero no creo que haya acuerdo respecto de si esto es aceptable o no en general.

Ciertamente para SSAC sí, pero para la comunidad yo creo que la ventana de vulnerabilidad es desconocida y de hecho hay una lista hasta el año 2016 porque hay muchas aplicaciones que no soportan la revocación y ciertamente hay que evitar que esas revocaciones funcionen.

Creo que es el punto que se presentó en la CCNSO y que hoy quería clarificarlo.

Otro aspecto que yo quería destacar y sé que ustedes están preocupados por esto, es que hay 4 cosas que uno puede hacer con el riesgo, puede controlarlo, puede mitigarlo o puede aceptarlo. Pero también puede transferirlo.

Cualquier cosa que hagamos nosotros que no aborde este tema plenamente es en última instancia una transferencia unilateral del

riesgo hacia el consumidor. Es decir, va a haber personas que consumen estas cosas que van a estar en este espacio de los nombres y que van a ser impactadas por esto.

Por ejemplo, una persona va y encuentra en Starbucks que hay cuestiones financieras o de salud y que están en ese gTLD. No me parece a mi que haya nada que ver con un ingrediente mágico, nadie va a resolver esto inmediatamente.

Tiene que haber un trabajo de coordinación con la comunidad. Y tenemos que ver cuáles son los frenos y contrapesos en el trabajo que vamos a ir poniendo en el trabajo que hizo ICANN en los últimos 3 meses como dijo Jeff.

Me parece a mi que este fue un enorme esfuerzo pero todavía hay un riesgo residual bastante importante. Tenemos que avanzar con esa transferencia y la vamos a terminar pasándola al consumidor.

En el estudio del RSST que hicieron Patrik y otras personas sobre el SAC 45, 46 y 57, hay mucha discusión sobre los estudios disciplinarios. Y esto dice que el DNS tiene que ver con el acceso a algo en internet.

Queremos que internet sea estable, segura y predecible. Los usuarios normalmente no acceden a un contenido en el DNS y entonces por eso tienen que ir a otro lado. Los sistemas dependientes de Windows están atados al DNS global para la estabilidad y seguridad, y es una obligación para nosotros que no hagamos sistemas unilaterales sin la coordinación que impacten en la seguridad, estabilidad y flexibilidad del sistema.

Ese es el punto que quería mencionar, gracias.

JEFF MOSS: Gracias. También quería decir que tenemos algunos representantes en la audiencia sbore los operadores de raíz, tenemos a las personas de los taxis y a otros que son parte de la comunidad.

Vamos a avanzar entonces a la parte de las preguntas y voy a ceder mi micrófono, si pueden mencionar su nombre y de donde provienen.

JEFF NEUMAN: Habla Jeff Neuman, soy de NeuStar. Tengo una pregunta, le hice esta pregunta a Falstrom…creo que fue ayer, me estoy confundiendo un poquito con los días porque eso fue capaz hace dos días.

Hubo una presentación de SSAC al consejo de gNSO, en ese momento el señor Falstrom dijo que el SSAC no estaba asesorando a la junta, no le estaba asesorando que retrase el programa de gTLD y al parecer por lo que ha dicho parece que hay un riesgo significativo.

Nosotros hemos escuchado esto y me parece que mi pregunta está más bien dirigida al señor McPherson, ¿tiene usted alguna propuesta concreta sobre la mesa para mitigar este tema? Es decir, ¿cuál le parece a usted que tiene que ser el próximo paso? ¿Cuán rápido puede hacerse eso? Y si usted está llevando a cabo el proceso para mitigar esta cuestión, ¿qué es lo que usted va a hacer?

DANNY McPHERSON: Yo estudiaría los problemas y tendría un equipo de expertos de ICANN, un equipo interdisciplinario. Me parece interesante que en los últimos dos o tres meses cuando las personas que estaban mirando esto

seriamente y decían que había un programa de los gTLD, queríamos saber cuáles eran las implicancias.

La gente decía, ¿qué significa si este TLD es delegado y si yo utilizo esta información en mi red? ¿O cuál es el nivel de visibilidad que tenemos en los sistemas de raíz y si es que tenemos alguna capacidad de alerta temprana que nos permita identificar cuáles son las amenazas? Va a haber acaso una suposición de que esto va a ocurrir.

Yo no tengo un ingrediente mágico, si sé que hay mucha gente en la comunidad y se ha hecho un gran trabajo en coordinar con todos estos sistemas independientes que confían en el DNS, que se basan en el DNS y vamos a tener que hacer cierto trabajo en cuanto a los plazos y en todo lo que tenga que ver más allá de eso.

Esto es un esfuerzo comunitario para determinar todo esto y si existe alguna demora, desde mi organización, si fuese mi decisión yo ciertamente consideraría las implicaciones de todo esto y personalmente yo no utilizaría ningún gTLD si pensara que para mis transacciones financieras o para mi salud esto se viera afectado. Yo no lo utilizaría y no utilizaría esa infraestructura.

Sería algo más estable, sabemos que tenemos algo que sea más estable, más seguro y que tenga una mejor perfomance.

PATRIK FALTSTROM: Quisiera hacer una aclaración. Yo respondí una pregunta doble, por un lado si SSAC estaba trabajando en algún seguimiento de este trabajo y la respuesta es no. Y en segundo lugar, si había alguna acción con respecto a la carta de VeriSign y la respuesta es no.

¿Podemos aclarar con respecto algo, esto es con respecto a todos los TLD,.corp,.home?

Yo sé que el problema podría ser ampliarlo a todo esto, en teoría eso sería así, pero me preocupa si es un subconjunto o todos.

DANNY McPHERSON: Creo que podría hacer un poquito más problemático, probablemente hay distintas opciones con el uso de los TLDs y también vamos a ver algunas cosas, hay otro tipo de dependencias, como señaló Bill Smith. Creo que la respuesta corta es que hay distintos niveles.

¿Y qué pasa con los datos de los observatorios? Nosotros vimos.corp,.home, cosas que uno vería normalmente como consultas en la raíz pero también mucho para.ads, no sabíamos qué sería eso. Queríamos saber si esto tenía que ver con los servicios directorio.

No sé si sería imposible manejar esto a menos que tuvieran una muestra representativa de todos los CA para saber lo que se ha emitido. ¿Y qué pasa con los caracteres internacionalizados no?

Le voy a dar el micrófono a Chris.

CHRIS WRIGHT: Soy Chris, de ARI Registry Services.

Tengo una pregunta similar a la de Jeff pero un poco diferente. La sesión fue maravillosa porque nos muestra todas las cuestiones de SSR que tiene que ver con respecto a los TLDs. Y lo han simplificado para que nosotros lo entendamos.

Lo que no obtuve en esta sesión y quería era el entendimiento del ICANN con respecto a cuál es el plan a partir de acá, cuáles son las actividades que va a llevar adelante la ICANN para abordar estas cuestiones, cuáles son los plazos para esas actividades, cuáles son las métricas para poder indicar que están conformes y es seguro seguir avanzando, cuáles son los objetivos específicos que se quieren lograr y cuál es el impacto general que tienen todos estos aspectos sobre el programa de los gTLD.

Entonces diciéndolo de manera un poco menos política que Jeff, quisiera saber si la opinión del ICANN es que los problemas de seguridad han sido mitigados a esta altura y que ahora estamos en un nivel de riesgo residual y que es aceptable y satisfactorio para ser transferido.

JEFF MOSS: Corríjanme si me equivoco pero las cuestiones técnicas que se mencionaron aquí están muy bien comprendidas por la comunidad técnica y ninguna sorprendió demasiado.

Sin embargo si nosotros nos fijamos en lo que ocurrió en el último mes verán una mejora continua en todos los aspectos. Por ejemplo, había preocupación de que el ICANN tenía un sistema para notificar a las CAs cuando se firmaba un contrato. Ese sistema está activo desde hace varios días, estaba la preocupación de que no se había seleccionado ningún proveedor de EBERO y sí se han seleccionado.

Entonces tenemos una lista para hacer un seguimiento de cada uno de estos temas y para reparar también tenemos un plan de respuesta. Los estamos captando de a uno.

Las áreas en las que el ICANN está operativa, donde nosotros podemos controlar nuestro destino, esto bueno cae bajo mi responsabilidad. Estamos colaborando con la comunidad, por ejemplo con la situación de SAC 57, estamos haciendo mucho trabajo en colaboración.

Y por ejemplo con los fabricantes de los buscadores no les podemos decir nada con respecto a eso a menos hasta que lleguemos a una conclusión con ellos. Tal vez de ese lado no se esté haciendo nada y bueno, ahí va a haber que llegar a una solución y vamos a hacer el anuncio.

Pero esto no es lo único que estamos haciendo. No sé si alguien quiere agregar algo al respecto. Muy bien, ahora Jeremy.

JEREMY ROWLEY: Quería felicitarlos por haber aprobado el mecanismo de información de vulnerabilidades, y sería mejor si lo hicieran más transparente para el público porque nosotros descubrimos este problema no mucho antes de que ustedes recurrieran a nosotros y no estábamos seguro de abordarlo o no, porque no sabíamos si podíamos manejarlo o no como una objeción.

O sea que si hay un mejor lugar para informar ese tipo de objeciones creo que es una ventaja. En respuesta a la pregunta anterior, este es un problema con todos los gTLDs de que puede haber un ataque considerando que se puede considerar cualquier dominio, pero tiene que estar el requisito.

Y existe este mismo potencial para todos, pero hemos visto los cuatro principales TLDs que son.corp,.ads,.mail y.bank, que son los más

problemáticos. Entonces quería comentar brevemente sobre el problema de la revocación, creo que esto se ha solucionado a medida que se van instalando o implementando las sentencias de OSP en todo lo que tenga que ver con OCSP Stapling.

Es una cuestión de activar los clientes del lado del servidor y luego tienen que pasarlo a (audio). Hay muchos grupos de la industria que están impulsando implementar esto como una opción.

JEFF MOSS: Tal vez sea una mitigación que están sugiriendo que trabajemos con los fabricantes servidores para poder activar por defecto OCSP stapling.

JEREMY ROWLEY: Sí, creo que hay muchos que están impulsando eso y creo que eso sería muy bueno, haría todo más rápido. Gracias.

BILL SMITH: Bill Smith, de PayPal. PayPal envió una carta al ICANN sobre básicamente las principales tres dominioes de primer nivel, que representan el 10% del tráfico a la raíz. Para las solicitudes de resolución de DNS es un número bastante considerable. Nuestra sugerencia fue no hacer la delegación porque esto podría ocasionar cierta preocupación.

También nos preocupan otros nombres pero más que nada nos preocupan estos. Y el impacto de transferir este riesgo de manera eficaz, porque estas cosas si no se pueden resolver las cosas no podrían ocurrir, y de repente encendemos el botón y el 10% de las solicitudes de la raíz para resolución terminan en el lugar equivocado.

Y esta es la práctica de estos TLD de estos últimos años. Entonces consideramos que es una cuestión muy seria, felicitamos al ICANN por haber hecho una respuesta tan rápida, nuestra preocupación es que no se ha hecho lo suficiente.

Mi pregunta en realidad tiene que ver con cómo nos aseguramos entre todos los que participan en el sistema DNS, las autoridades de certificado de seguridad y todos los otros sistemas que están allí, que esto funciona. Porque podemos estar hablando de los proveedores de buscadores, que eso es maravilloso que lo hablemos pero tal vez hay muchos otros que hacen aplicaciones que no utilizamos para conectarnos al internet.

Entonces todavía tenemos todas esas cosas de las cuales preocuparnos. O sea que este es un problema que es conocido de hace bastante tiempo y mi pregunta es: ¿cómo nos aseguramos de no repetir este tipo de situaciones?

JEFF MOSS: Tengo una pregunta para usted. En primer lugar, quiero hacer un comentario. No ha habido una decisión final en nuestra respuesta a la carta de que el ICANN no iba a continuar investigando. O sea que en lugar de ser una decisión binaria, delegar o no delegar, ¿usted ve alguna alternativa intermedia? Tal vez no delegar durante dos años para que la gente tenga tiempo de repararlo.

BILL SMITH: Voy a hablar a título personal porque Paypal puede tener otra opinión al respecto. Yo creo que la respuesta es sí, creo que n tenemos que ser

binarios pero si vamos a hacer algo tiene que inclinarse por el no delegar y que lleve más tiempo, por lo menos para estos tres TLDs. Y tenemos que ser cautelosos con los otros, para ver qué podemos hacer.

Y, como señaló Jeremy, el problema aquí es que no tenemos ideas porque no hay registros a los que tengamos accesos para ver qué conjuntos se han emitido como TLDs privados para todos estos dominios de primer nivel o cualquier otra cadena de caracteres que esté por ahí.

Entonces es un problema que nos va a acompañar durante un buen tiempo, aún cuando tomemos alguna medida de inmediato. Creo que se pueden hacer elecciones entre no delegar nunca y delegar en forma inmediata, pero más del lado de no delegar. O sea que hay que estar del lado más conservador. Creo que esto tiene más sentido, sobre todo para cosas como.corp.

EL 10% las solicitudes para la raíz van a corresponder a esos y no van a ser válidas. Entonces si se resuelven se van a resolver en el lugar incorrecto.

JEFF MOSS: ¿Alguien tiene algún comentario?

PATRIK FALTSTROM: Quiero agradecerle por este comentario y también por participar en este diálogo, porque al igual que usted mencionó en su carta, hablo de SAC 57 que la dimos a conocer en noviembre de 2010 cuando SSAC

habló de estos temas y sí, hablamos con Chef y con otros a ver si teníamos que revisar SAC 45 para ver algunas otras áreas grises.

Creo que es realmente muy bueno que esto ocurra en la comunidad, que vengan a los micrófonos y nos ayuden a resolver los problemas de manera conjunta.

RUBENS KUHL: Rubens Kuhl, de.br. Una pregunta para Steve Sheng y posiblemente Warren. ¿Han considerado ustedes la modificación de los buscadores? Por ejemplo emitir una fecha para el certificado, y si la fecha de emisión del certificado es anterior a la fecha real que sabemos en que se hizo la delegación del TLD, ¿esto es un certificado interno? Entonces ahora podemos omitir ese certificado porque no se ha hecho la delegación del TLD, ¿esa es una opción?

STEVE SHENG: Gracias por la pregunta, esta es una de las alternativas que se nos propuso. Lo hizo un proveedor de buscadores, así que estamos tratando de ver toda la cuestión de viabilidad en este sentido porque es importante que cuando las cosas se delegan que esto se les transmita a ellos. Entonces todavía estamos estudiando esta posibilidad.

Algo que debemos recordar es que hay muchas personas que están utilizando y Eses sobre Windows Xp, hay muchos que están utilizando sistemas Legacy, sistemas heredados. Si nos fijamos hay 850 referencias a los certificados y 870 a los TLS.

Así que son todos protocolos, como el AAA, el iMERI, y esas cosas.

MIKEY O'CONNOR: Hola Jeff. La mayoría de las personas me conoce aquí como esta persona que trabaja en el foro del grupo de trabajo, pero yo también soy propietario del nombre de dominio corp.com, y cuando yo hago el enrutamiento para ese nombre de dominio encuentro mucho tráfico. Tanto tráfico que en 20 minutos saturo todo el ISP.

Entonces lo que quiero decir es que todo ese tráfico se puede analizar y les puedo decir que no son solicitudes web, sino que son todo tipo de cuestiones de directorios, de intercambios, de servicios. Puertos de nombres que se utilizan para hacer cosas extrañas, es una cantidad horrenda de tráfico. Y eso no es lo que está ocasionando el problema en la raíz, esa es la versión.com. Entonces solamente me puedo imaginar lo que ocurren cuando se apruebe.corp para las direcciones en internet.

Así que me sumo a Bill de Paypal y también ofrezco una cadena de caracteres para analizar, para quien quiera analizar.

JEFF MOSS: ¿No creen que esto tiene que ver con autocompletar.com con.corp? No, si ustedes se fijan en la documentación el default es corp.com. Esto es simplemente un ejemplo del tipo de problema con el que pueden toparse cuando entren a.corp, que se usa convencionalmente.

Pero durante muchos años el frontpage de Microsoft utilizó este nombre como default por omisión, entonces esto es un buen ejemplo del tipo de problema que esto podría afectar.

Si nos fijamos en el servidor de correo para.corp, me lleva muchísimos minutos para recibir un mensaje, responderlo… algún nombre que contiene presentaciones SCC antes de ser liberado. Lo que me desespera, porque el servidor del DNS me devuelve todo un tipo de cosas y me afecta a mi y a un montón de personas más, yo soy bueno pero si una persona con malas intenciones utiliza esto podría hacer muchísimas cosas y nosotros no nos enteraríamos.

JEFF MOSS: Gracias por ofrecernos esto a nosotros para investigar y no a una organización de delincuentes, porque ellos seguramente te pagarían más.

MIKEY O'CONNOR: Sí, con gusto voy a ofrecerlo pero este es el tipo de problema que podría presentarse pero implica muchísimo tráfico.

JEFF MOSS: Gracias, ¿alguien más quiere responder al respecto?

ANDREW SULLIVAN: En la sesión anterior a esta tuvimos una presentación sobre las pruebas de pre delegación y sugirieron que necesitábamos un poco de interacción entre quienes hacían las pruebas y los que estaban siendo sometidos a las pruebas, porque no es un proceso totalmente mecánico de aprobar o desaprobar.

Y acá veo que se hace la observación que de repente nos estamos dando cuenta de que falta muy poco tiempo para entrar en operación y nos empezamos a preocupar. Y me pregunto si estamos descubriendo de que todo esto es un poco más peligroso de lo que pensábamos que iba a ser. Lo vamos a activar y la gente va a empezar a darse cuenta de los riesgos reales apenas ahora, unos pocos meses antes de empezar.

Entonces con este problema el CA ya de por sí es bastante malo, me pregunto si el panel tiene algo para decir con respecto a los riesgos generales en esta área, si estamos reconsiderando nuestra postura con respecto a hacer la re-delegación de tantos TLDs, teniendo en cuenta todos estos factores.

CHRSTINE WILLETT: Yo puedo hablar con respecto a la parte que tiene que ver con las pruebas de predelegación, el deseo de tener más interacción entre los que hace la pruebas y los solicitantes como parte de la predelegación se basaba en la necesidad de asegurarnos de que los solicitantes eran capaces de proveer la documentación necesaria para comenzar las pruebas.

No tenía que ver conuna falta de automatización o con una prueba automatizada que no funcionaba. Era una cuestión de comunicación, tal vez un problema idiomático. Entonces estamos haciendo el esfuerzo para cambiarlo y ser mucho más claros y específicos con respecto a la información y documentación que se requiere.

Yo no he tenido ningún comentario sobre las pruebas automáticas o las herramientas automáticas que hayan sido problemáticas, esto tiene que

ver con la parte de su pregunta vinculada a las pruebas de predelegación.

JEFF MOSS: Quisiera decir que esta no es la primera vez que expandimos el espacio genérico, sino que es la tercera vez. Hay muchos problemas que existen desde que agregamos el nuevo G, un nuevo genérico al sistema. El tema es que el tamaño del espacio ruteable está aumentando muchísimo y ahora podemos tener solicitudes como.bank que pueden ser más atractiva a algún cliente que.info.

Pero los problemas que enfrentamos ahora son los mismos que siempre tenemos, nada más que ahora somos mucho más conscientes de ellos.

DANNY McPHERSON: Quería responderle a Andrew y a Christine. Desde la perspectiva operativa tenemos muchísima infraestructura y conocimiento institucional relacionado con la operación de registros en mi compañía. Vimos que en mucha de la documentación para las pruebas de pre-delegación era problemática, por decirlo de buena manera.

Hay una carta de febrero y otra de marzo y hay un intercambio entre Akram y todo el grupo de registros de partes interesadas, y esto refleja el interés que esto había suscitado.

Pero simplemente delegar una zona dentro de nuestra compañía tenemos 110 tareas que están vinculadas con el minuto, es decir esto es lo que pasa. Y ese rigor es muy importante cuando establecemos

secuencias y las unimos con un plan de proyecto dentro de nuestras operaciones internas.

Entonces esperamos el mismo tipo de rigor también en todos los aspectos que tienen que ver con las pruebas de predelegación, obviamente estamos mejorando y nos encanta ver estas mejoras y esperamos seguir viéndolas.

Con respecto al punto que mencionó Andrew, estoy de acuerdo. Hasta que uno hace un esfuerzo explicito de decir, cuáles son las dependencias, estas son las implicancias de los cambios que estamos hacindo en este sistema para los sistemas que los usuarios quieren utilizar para acceder a contenido y otras cosas.

O sea, hasta que uno se toma esos minutos para ver eso, no se da cuenta de todas estas cosas. Y esto es un artificio lo que estamos viendo. Lo estamos viendo un poco tarde porque hay muchos que dicen, estas son las implicancias de mi operación, porque no todo el mundo sigue a DNS o ITF o ICANN en sus operaciones diarias.

Para nosotros y para muchas de las personas aquí, nosotros nos dedicamos a las redes y al DNS. Pero para aquellos que no lo hacen la situación es completamente diferente.

JOE ABLEY: Pensé que había comentado sobre un aspecto del escalamiento con respecto al sistema raíz, pero es importante saber que tenemos cambios estructurales que se han producido en el pasado más grandes que los de ahora.

Ahora vemos un cambio en la zona raíz a un tamaño, que en términos absolutos todavía es bastante pequeño. No estamos hablando de agregar registros ni de cambiar los protocolos, ni de cambiar todos los (mal audio). Aquí estamos hablando de seguir manejándonos con una zona raíz un poco más grande.

Me imagino si tenemos.info acá vamos a tener.bank en otro lado y todos van a usar el mismo software. Creo que es importante lo que dijo Danny, que tenemos que tomar todas las precauciones necesarias para establecer esta línea de partida, hacer la medición de desempeño y seguir los cambios en la zona raíz.

A medida que vamos cambiando el sistema raíz, si nos fijamos estos cambios son bastante pequeños. Otra cosa en la que estamos trabajando es en este sistema tan importante y esperamos que las implicancias realmente sean mínimas.

JEFF MOSS: ¿Patrik?

PATRIK FALTSTROM: También quisiera sumarme a lo que acaban de decir, que no solamente estamos haciendo estos cambios en la zona raíz sino que también estamos viendo ccTLDs que se están activando. Pero esto no ha tenido ningún problema.

WARREN KUMARI: Quiero responder a algo que dijo Jeff. Sí hemos lanzado nuevos gTLDs antes, pero ¿cuál ha sido la postura cuando tenemos algún problema?

Por ejemplo con.info, ¿cómo reconoció la gente esto cuando se lanzó? Creo que las inquietudes que estamos viendo ahora tienen que ver con las interacciones del DNS mismo y otros sistemas.

Es como este estudio interdisciplinario que pedía SSAC.

JEFF MOSS: Esto tiene que ver con las cuestiones de aceptación universal en el lenguaje del ICANN.

WARREN KUMARI: Esto es parte del tema de.info. Pero tiene que ver con la interacción entre el DNS y las solicitudes. Sí, tiene que ver con aceptación universal pero también es una cuestión interaplicación.

Tal vez ahora estemos más cerca de resolver el tema de la aceptación universal.

JEFF MOSS: En esas situaciones tal vez la ICANN puede operar más como un facilitador o como un coordinador, pero no controlamos cómo python hace la resolución o cómo Microsoft Application busca un nombre. Pero podemos decirles que pensamos que había un problema aquí y queremos la ayuda de esos expertos.

Y como opera ICANN tiene una influencia en forma directa, entonces creo que puede cumplir ese rol de coordinador o facilitador.

PAUL STAHURA: Soy Paul, de Donuts. Me interesa el informe de SSAC que hizo un relevamiento en el 2010 si no me equivoco.

JEFF MOSS: ¿Es el informe del observatorio?

PAUL STAHURA: Sí, es de hace unos años.

JEFF MOSS: Sí, ha sido actualizado.

PAUL STAHURA: Estoy aquí para informar los resultados. Nosotros nos fijamos en los resultados en la zona.com y net y tomamos todos los nombres allí y observamos 25 millones de certificados y de esos certificados analizamos cada uno de ellos y vimos cuál era el rótulo de primer nivel, y vimos que había 51 nuevos gTLDS propuestos allí.

51 TLDs que aparecen entre esos 25 millones. También vimos que el más grande era.corp, al igual que mostró el relevamiento. Y luego vimos los subdominios dentro del.corp y encontramos 102 subdominios únicos exclusivos en ese espacio gigante de.corp. Solo 102.

Y después en 42 subdominios offline era el tercero, Inc era el cuarto. Tengo toda una lista de.corps aquí, para.corp por ejemplo encontramos park.corp, digilove.corp, hay 102 de estos. Entonces ¿por qué no los bloqueamos durante un tiempo? Tal vez hasta el 2016 como dijo alguien.

Los bloqueamos. No hay que bloquear todo el espacio a nombre de corp, sino que dejamos de otorgar certificados. Y creo que así podemos reverlo en el futuro.

JEFF MOSS: Gracias.

DANNY McPHERSON: El artificio interesante aquí es que SAC 57 lo que se resaltó, me encantaría ver los resultados de ese informe pero estos son certificados de nombres internos. Se supone que no se tienen que utilizar en internet. Los que ustedes encuentran en internet son aquellos que la gente está filtrando hacia la internet, o sea que eso es un nivel bastante bajo.

Y si se hacen las correcciones correctas tendríamos otros niveles de magnitudes. Si nos fijamos en el corpus de CA es imposible identificar los certificados que han sido emitidos para esas cadenas.

PARTICIPANTE: Sí, pero me sorprende la cantidad.

DANNY McPHERSON: Sí, es cierto.

JEREMY ROWLEY: El problema de Bill Smith se vincula en cierta forma, pero es diferente al problema del CA porque estas redes están configuradas para que sean internas, para que no puedan ser solucionables porque son redes

internas o sea que hay muchos conflictos en internet con todos estos servidores internos que están configurados.

Cuando uno entra a un café y se encuentra con todos estos nombres de gTLD que no esperaba. Y esto es diferente a los certificados que son emitidos para stock, porque los CA pueden ocuparse de la cuestión de los certificados pero lo que yo quiero saber es qué pasa cuando uno apunta estas redes que han centrado todas sus operaciones de forma interna, ¿cómo se pueden reconfigurar para evitar todos estos problemas?

No creo que se haya llegado a esa solución, ustedes lo identificaron en el informe pero hablaron con los otros corredores de CA pero quisiera saber si alguien ha hecho algo al respecto.

JEFF MOSS: ¿Alguien quiere responder? Patrik.

PATRIK FALTSTROM: Creo que lo que está señalando es muy válido. Aunque sea una situación en la que uno de esos dominios ya está cubierto internamente, puede ocurrir que el resultado sea diferente dependiendo de si la solución del nombre de dominio ocurre dentro o fuera de esa zona interna. Si hay una red fuera o también qué pasa con la conexión.

Esto es algo que estamos analizando por supuesto en SSAC pero como dije antes no es un punto de acción, estamos hablando aquí y tal vez

puede ocurrir que consigamos uno de esos disparadores que nos genera una solución.

Yo creo que una de las recomendaciones en SAC 45 era esa difusión externa que podía verse afectada. Hasta el 2011 la documentación mostraba que se utilizaban servidores internos de nombres para distintos propósitos, para intercambio por ejemplo y para ver cartelera. Y hablamos de 2016 porque se decía que no se podía hacer ese cambio porque necesitaban tiempo para conseguir el dinero y cambiar sus redes y cambiar toda la funcionalidad.

O sea que me gusta toda su idea de hacer que no sea una cuestión intermitente. Sí se puede delegar pero se va a delegar en el 2014 o en el 2015 cuando tengamos la oportunidad de resolver el tema de los certificados de los servidores internos, pero no se puede dejar el tema allí durante dos años.

Y esto les da tiempo a todo el mundo a cambiar y hacer la transición.

JEFF MOSS: Entonces esencialmente lo que estaba diciendo es cuando el cliente viene y dice el certificado va a vencer en dos meses, quiero conseguir otro., ustedes por la difusión externa van a decir no no puede comprar esto, tiene que traernos un plan.

PARTICIPANTE: Sí, y esto fue adoptado en el 2001, es un requisito para tratar de mitigar ese problema en ese momento. Normalmente vienen dos días antes de que venza el certificado y dicen ay, necesito conseguir otro certificado

para el servidor porque sino voy a tener inseguridad en toda mi operación.

JEFF MOSS: Entonces ustedes se han estado comunicando a lo largo de todo este tiempo.

PARTICIPANTE: Sí. Desde el 2011 está el requisito de que esto es necesario con los CAs.

WARREN KUMARI: También debería mencionar que hacer que alguien cambie para lo que necesita el servidor del nombre es un mucho más fácil que hacerlo cambiar toda la infraestructura para renombrarlo.

Es mucho más fácil cambiar.corp en todas partes, es mucho más difícil hacerlo con.corp y cambiarlo a foot.com.

PARTICIPANTE: Hay un estudio cuyos resultados son muy interesantes donde muchas personas que piensan que estos nombres de servidores internos son requeridos tal vez sea un poco denso, pero quisiera saber si pueden resumir cuáles son las acciones que están comprometidos a adoptar y cuáles va a tomar la ICANN.

Fadi dijo que iba a detener el programa si había preocupación sobre estabilidad y seguridad. Obviamente muchas personas sugieren que esto se haga. Entonces ¿cómo se avanza? ¿Cómo el ICANN va a avanzar, y qué puede hacer la comunidad para ayudar?

JEFF MOSS: ¿Alguien quiere responder o lo hago yo? Me imaginé que me iban a dar la palabra a mi.

Como mencioné antes estamos haciendo un seguimiento de todos los riesgos que se han planteado, algunos que se identificaron en forma interna, que no vinieron de la comunidad, y si nos topamos con un problema como el de los servidores internos y los certificados que tiene un impacto a escala mundial, eso nos puede llevar a una pausa.

Si no podemos mitigarlo eso sería un tema lo suficientemente serio como para considerar si tenemos que modificar nuestro programa. O sea que tenemos que tomarlo caso por caso, y lo que le pedimos a la comunidad es que haga lo siguiente.

Si piensan en la naturaleza de los problemas de lo que estamos hablando, el tema del certificado es un síntoma de un problema que se está expandiendo por todo el espacio de las direcciones enrutables. Y estoy seguro de que ustedes no se les puede ocurrir todos los problemas pero la gente que está en la comunidad tal vez se da cuenta de una situación a la que tenemos que prestarle atención.

Entonces justamente lo que les pido es que les hago un llamado para que nos ayuden a identificar cualquier otro problema del que ustedes tengan conocimiento, no quiero que ustedes digan “ah si, yo sabía de este problema hace 5 años” y nos lo digan dos minutos antes de entrar en actividad.

Entonces si es necesario tener un proceso coordinado lo pueden hacer, si quieren hablar conmigo en privado también lo podemos hacer. No vamos a descartar nada hasta haberlo investigado.

PARTICIPANTE: Basándonos en lo que acaba de decir, ¿puedo llevarme como conclusión que ICANN siente que todos estos temas han sido abordados correctamente?

JEFF MOSS: Actualmente no hay ningún tema que nos impida seguir adelante.

DANNY McPHERSON: Yo como persona y como operador estoy en desacuerdo. Creo que hay una cantidad significativa de riesgo residual que ha sido trasladado unilateralmente a los usuarios, a los consumidores de internet.

Y si nos fijamos una de las promesas del programa de los nuevos gTLD era que íbamos a tener TLDs que iban a estar seguros de una manera mucho más eficaz, y yo creo que esto no es así. Entonces mi solicitud es que ICANN mire este aspecto, sabemos que hemos andado a los saltos pero creo que lo que se ha hecho hasta ahora realmente aborda todas las cuestiones.

JEFF MOSS: Entonces, ¿cuál es el peor de los problemas?

DANNY McPHERSON: Cualquiera de los individuales y obviamente todos en conjunto. Ninguno de estos temas ha sido abordado realmente.

Yo ya he hecho una manifestación, pero bueno hemos tenido un debate de 90 minutos donde dijimos que la reasignación no sucede, que puede pasar por otras cosas, qué pasa con ciertas bases de nombre. Entonces en última instancia no podemos simplemente como comunidad asumir las obligaciones y responsabilidades del DNS y un DNS independiente y transferir ese riesgo a los consumidores.

JEFF MOSS: Entonces en el ejemplo de la RACP, en el OSP ¿el navegador qué va a hacer? ¿una revocación de la OSP?

No va a haber delegación, ¿o hay mitigación, hay desafíos para que los servidores realicen esto como una conducta por default?

STEVE SHENG: Yo no estoy de acuerdo en cuanto a que la revocación no funciona.

WARREN KUMARI: Creo que no vamos a poder sacar todo el riesgo que existe. DNS es un sistema interrelacionado y muy complejo, hemos hecho cambios entonces hay cosas que van a salir mal en algún lugar.

Puede ver cuándo se hace una lista negra de varios nombres, porque hay varios nombres que quedan bloqueados. Entonces el tema es cuánto riesgo podemos aceptar para hacerlo y quién lo va a asumir.

¿Están listos los que lo deben asumir a hacerlo? ¿Estamos en la posición correcta para hacerlo?

JEFF MOSS: ¿Alguien tiene algún otro comentario? Porque sino entonces cerramos esto.

Entonces esta fue la sesión inaugural en la comunidad. Si a ustedes les parece que esto resultó útil, realmente lo podemos hacer en todas las sesiones que siguen de ICANN. Y me gustaría que levanten la mano a quien le pareció que fue útil

Bueno, claro que podemos mejorarlo, obviamente. Podemos tomar las preguntas por adelantado para entonces poder abordar las preocupaciones de cada uno. Así que espero verlos nuevamente en Dortmund y poder tener una reunión de este tipo. Muchas gracias a Mike (audio).

MIKEY O'CONNOR: Bueno yo no voy a empezar a volver loco al resto pero acá tengo otra perspectiva distinta de la que marcaron.

De cierta forma el programa de nuevos gTLD es un nuevo producto que ofrecen varios proveedores. Entonces yo soy un ISP, yo estoy en el lugar donde las cosas se conectan. Si algo se quiebra, no van a llamar a ICANN, no van a llamar a Donuts, me van a llamar a mí.

Y yo como ISP les estoy pidiendo a ustedes que garanticen que el producto que ustedes quieren vender funcione bien, porque la última vez no funcionó y entonces me echaron la culpa ami por eso. Entonces

yo tuve que gastar mucho dinero en el centro de atención al cliente.

Esta vez sería bueno que el producto funcionase mejor. Quienes están ofreciendo este producto quieren ver todas estas ganancias dentro del DNS, a mi me parece que recibir ingresos es algo muy bueno pero este producto no parece estar listo, a l menos a mi no me parece. Y existen ejemplos de los que se estuvieron hablando, como dije yo el.corp.com. Entonces yo soy el que está ahí afuera, y digo no seamos demasiado osados al respecto para no darle a los que ofrecen el producto que tengan que hacer los arreglos.

Yo no voy a ir hablar con el navegador, ICANN lo tiene que hacer porque ese producto es de ustedes entonces son ustedes los que tienen que hacer que el producto sea bueno y funcione en el mercado. Perdón por la interrupción.

JEFF MOSS: Muchísimas gracias a todos.