COPENHAGUE – Reunión pública del SSAC
Miércoles, 15 de marzo de 2017 – 15:15 a 16:15 CET
ICANN58 | Copenhague, Dinamarca

PATRIK FÄLTSTRÖM: Les pedimos a los miembros de SSAC que por favor se acerquen aquí adelante y ocupen una silla que no esté ocupada todavía. Bienvenidos a todos. Son apenas unos minutitos pasados de las 3:15 de la tarde. Lo crean o no, no son las 8:00 del jueves, si bien tengo aquí mi café matinal. Me llamo Patrick Fältström. Soy presidente del comité asesor de seguridad y estabilidad. Hacemos la broma porque normalmente SSAC se reúne a la 8:00 de la mañana el jueves en una sala mucho más pequeña que esta. Esto representa un cambio de varias maneras. Tengo aquí a mi alrededor miembros del SSAC que no tenían otras responsabilidades hoy. Una de las principales responsabilidades cuando están en una reunión de la ICANN es participar en las sesiones y estar activos. No siempre todos pueden estar aquí acompañándome pero pensé que me podían acompañar y vamos a empezar por la izquierda con las presentaciones.

ROD RASMUSSEN: Hola. Rod Rasmussen.

TARA WHALEN: Tara Whalen, de Google, ingeniería privada.

PATRICK JONES: Patrick Jones.

JAAP AKKERHUIS: Jaap Akkerhuis.

ROY ARENDS: Roy Arends.

GEOFF HUSTON: Geoff Huston, de APNIC.

JIM GALVIN: Jim Galvin, vicepresidente de SSAC y Afilias.

PATRIK FÄLTSTRÖM: Patrick Fältström, presidente de SSAC.

RAM MOHAN: Ram Mohan, también enlace del SSAC con la junta directiva.

BEN BUTLER: Ben Butler.

WARREN KUMARI: Warren Kumari, de Google.

JOHN LEVINE: John Levine, representante de la Sociedad de Internet.

JEFF BEDSER: Jeff Bedser.

GREG AARON: Greg Aaron.

ROBERT GUERRA: Robert Guerra.

JULIE HAMMER: Julie Hammer, sin afiliación.

DANNY MCPHERSON: Danny McPherson, de VeriSign.

PAUL EBERSMAN: Paul Ebersman, Comcast.

CRISTIAN HESSELMAN: Cristian Hesselman.

PATRIK FÄLTSTRÖM: Tenemos también a algunas otras personas aquí que nos acompañan en la sala. Lo que vamos a hacer aquí es darles una reseña general de SSAC. Vamos a hablar del trabajo que tenemos en este momento en desarrollo. Vamos a hacer referencia también a algunos de los futuros hitos, las publicaciones que tenemos publicadas en SSAC desde ICANN 57 y también la interacción con la comunidad. Por eso tengo a tantos miembros del SSAC aquí a mi alrededor.

En este momento somos 31 miembros. Los miembros son designados por la junta directiva de la ICANN. Asesoramos a la comunidad de la ICANN y a la junta directiva en temas relacionados con la seguridad y la integridad de los sistemas de distribución de direcciones y nombres de Internet. Nuestro ámbito de acción está vinculado también con el trabajo que hace RSSAC y también con otros sistemas como los de nombres y números. Como ustedes pueden ver aquí en esta diapositiva, tenemos conocimiento especializado en muchísimas áreas. Lo importante acá es que cuando designamos a miembros nuevos de SSAC, que lo hacemos nosotros mismos, tratamos de asegurarnos de la mejor manera posible que SSAC en su totalidad tenga el conocimiento especializado que se necesita

para poder elaborar un buen informe. Hasta el momento, tenemos 91 publicaciones y, de hecho, la número 92 es la que se distribuyó esta semana pero todavía no fue publicada. Estas publicaciones están divididas en informes, documentos de asesoramiento y comentarios. Todas estas publicaciones juntas constituyen lo que SSAC cree que es verdad y lo que quiere decir.

Todos ustedes aquí en el público y otros pueden hablar sobre cuestiones de seguridad pero SSAC expresa en estos informes lo que considera que es lo correcto. Si nosotros pensamos en los valores fundamentales de la ICANN y en su misión, tenemos que tener en cuenta que estos son asegurar la operación segura y estable del sistema de identificadores únicos de Internet y preservar y ampliar la estabilidad, confiabilidad, seguridad e interoperabilidad global de la Internet.

Nuestra carta orgánica está estrechamente vinculada con la misión de la ICANN. Cuando presentamos el asesoramiento del SSAC a la junta directiva para su consideración, la junta directiva lo recibe y analiza ese asesoramiento. Puede tomar distintos cursos de acción. Cuatro en total. Puede utilizar ese documento y ese asesoramiento en el proceso de desarrollo de políticas. También puede pedirle al personal que implemente ese asesoramiento, implementando también un proceso de consultas al público. Puede también difundir ese asesoramiento a las partes afectadas o puede optar por una solución diferente.

Debe explicar en ese caso por qué no está siguiendo el asesoramiento brindado por SSAC. Una acción formal no significa que la junta directiva tenga que hacer lo que nosotros decimos. De hecho, nadie está obligado a seguir el asesoramiento de SSAC pero, como es el mejor asesoramiento del mundo, si no siguen nuestro asesoramiento, todo el mundo se viene abajo. El cielo se cae. Dios sabe qué otras cosas podrían ocurrir.

Todos ustedes, por supuesto, tienen que leer nuestros documentos de asesoramiento y si después creen que es correcto, tienen que seguirlo. El asesoramiento es algo independiente, que tiene fuerza por sí mismo. Tenemos varios grupos de trabajo actualmente que están abocados a hablar del tema de los datos y de WHOIS, el manejo del DNS, el manejo del espacio de nombres y los riesgos para los nuevos TLD en cuanto a su delegación. Esto tiene que ver con la publicación número 91. El SSAC90 y el 91 son dos informes que tienen que ver con estos temas. Es posible que haya otro trabajo que la ICANN saque también en relación con esto.

Trabajamos en los grupos en relación con los talleres de DNSSEC. Uno se hizo en el día de hoy y también tenemos el Comité de Miembros, que evalúa a los miembros de SSAC y los posibles miembros que solicitan pasar a ser miembros de nuestro grupo. Desde la última reunión de la ICANN publicamos

documentos, 85, 86, 87, que tienen que ver con las respuestas a los grupos de trabajo de la GNSO. El 88 y el 89 son respuestas a los comentarios de la ccNSO sobre el SSAC84, que tiene que ver con el proceso que tiene la ccNSO de revisión. Luego tenemos el 90, que es un documento de asesoramiento sobre la estabilidad del espacio de nombres de dominio y el 91, que tiene que ver con los indicadores de sanidad de la tecnología de identificadores. Esto es algo que nosotros ya mencionamos aquí en esta introducción.

Si ustedes se fijan en los hitos actuales y futuros, observarán que básicamente publicamos lo que esperamos tener en el trimestre cuatro del 2016 y lo que queremos lograr en el trimestre uno del 2017. Todavía no hemos finalizado. Estamos planificando ya un taller sobre DNSSEC para la ICANN 59 en el segundo trimestre de 2017. Vamos a trabajar también sobre el tema del espacio de los nombres y la ronda de los nuevos gTLD. Si entramos en mayor detalle analizando las publicaciones desde la última reunión de la ICANN y nos movemos hacia atrás en retrospectiva, en el SSAC 91 nosotros revisamos la presentación sobre los indicadores de salud y tecnología de identificadores, y respondimos al llamado a comentario público con respecto a las cinco enfermedades que podrían afectar la parte que corresponde a los nombres en estos identificadores únicos.

Nosotros también nos reunimos con personal de la ICANN. Hemos presentado estos comentarios, no solamente a través de este documento sino también con el proyecto que se encarga de estos indicadores. Nos reunimos incluso esta semana. Tenemos algunos problemas con la elección de la terminología que ahora ha sido levemente actualizada. También teníamos algunas dificultades con la falta de una distinción clara entre la recolección de datos y la extracción de conclusiones a partir de esos datos. En el SSAC90 tenemos asesoramiento sobre la estabilidad del espacio de nombres de dominio. En ese documento hacemos algunas observaciones y recomendaciones dirigidas a mitigar los riesgos claramente identificados.

En el 88 y en el 89, en estos documentos, aclaramos algunas de las cuestiones que habíamos planteado en el SSAC84 con relación al proceso EPSRP. Esto tiene que ver también con las respuestas a una evaluación con falla en la delegación de uno de los TLD en el proceso acelerado. Había cuestiones vinculadas con la posibilidad de confusión. Hubo toda una discusión entre la ccNSO y SSAC, y en el 89 también mantuvimos distintas reuniones entre la ccNSO y SSAC esta mañana y esta semana. Hemos avanzado un poco para hablar de este tema.

Estos son ejemplos o preguntas que a veces nos hacen para saber cómo priorizamos nuestro trabajo. Pensaba verlo rápidamente, a menos que hay alguna pregunta urgente, y luego

ustedes podrán tomar la palabra y hacer todas las consultas que quieran. SSAC prioriza el nuevo trabajo y elige el trabajo en el que quiere centrarse. Lo hacemos por cuenta propia. La diferencia para establecer prioridades tiene que ver con lo siguiente. Si tenemos una pregunta de la junta directiva de la ICANN, le damos prioridad más alta que a otras actividades, porque nuestra tarea principal es la de brindar asesoramiento a la junta directiva de la ICANN. También puede ocurrir que si hay consultas públicas que tienen también un plazo, en ese sentido tratamos de proporcionar un informe a tiempo para que llegue a emitirse dentro de ese plazo. Hemos tenido un grado relativo de éxito en esas presentaciones teniendo en cuenta los tiempos de estos periodos. También respondemos preguntas y brindamos recomendaciones sobre temas que nos llegan de otras unidades constitutivas de la ICANN.

Debo decir, sin embargo, que aquí perdimos un poco el camino porque tenemos temas perdidos que nosotros investigamos por nuestra propia cuenta sin que nadie nos los remitiera. Esto es lo que nosotros identificamos aquí en la ICANN cuando vamos siguiendo las listas de correo. Nosotros también trabajamos de esta manera, identificando algunas cuestiones que nadie más identifica.

Además, nos concentramos en el seguimiento que le da la junta directiva a nuestro asesoramiento. Para nosotros eso es

importante porque la junta directiva tiene que tomar acciones a partir de nuestro asesoramiento. Hemos estado siguiendo esto manualmente pero si hay algo que detectamos, lo conversamos y ambos estamos de acuerdo en que tenemos que tener un buen seguimiento y a veces no siempre ha sido así. Acordamos tener entonces un tracker para hacer este seguimiento. Es una interfaz de usuario en el tracker, que todavía no está lista. Esto permite que nosotros hagamos un seguimiento de la respuesta de la junta directiva a nuestro asesoramiento. Nosotros en SSAC, al igual que otros que puedan estar interesados en obtener un informe sobre el destino de nuestro asesoramiento y del de otros comités puedan usar un informe y pueda hacer la solicitud al informe porque ahora todo ese rastreo, ese seguimiento se hace de manera automática.

¿Cómo SSAC informa a la comunidad sobre su trabajo? Por ejemplo, en estas reuniones, donde les explicamos cómo trabajamos pero también puede ser que sea a través de la publicación de un informe, que es lo más importante. Tenemos una página web donde nosotros publicamos nuestros documentos. Vemos las estadísticas. Allí también vemos que en entre las páginas de ICANN que hay en ese sitio web, la página de los documentos de SSAC es la que es de más interés para todos nosotros y vemos también que es la de más interés para la mayor parte de la gente. Vemos que todos los que ingresan a

nuestra página web de documentos dedica por lo menos tres minutos a esa página, lo cual me parece que es interesante.

También tenemos una cuenta de Facebook. Tratamos de hacer algunos vídeos. Vídeos que damos a conocer junto con el equipo de comunicaciones de la ICANN. Tratamos de tener a distintos miembros de la ICANN en esos vídeos. No duden en comunicarse con nosotros si quieren que alguien haga referencia, haga una presentación sobre lo que tenemos. Consúltennos. Somos personas dedicadas a la seguridad y no a la comunicación. Le agradezco a Duncan por ayudarnos a entender cómo comunicar el trabajo que realizamos.

La última pregunta con respecto a cómo la comunidad puede hacer un seguimiento de la respuesta de la junta directiva al asesoramiento del SSAC es algo que se vincula con lo que acabo de mencionarles. Sin ayuda del personal de la ICANN es difícil tener acceso a ese seguimiento pero eso es lo que tenemos disponible por el momento. Les doy la palabra a ustedes ahora. Nosotros querríamos tener un poco de retroalimentación, comentarios de parte de ustedes sobre estas cuestiones. Vamos a abrir los micrófonos para que ustedes nos den sus opiniones y que también nos hagan la consulta que tengan y después veremos qué les respondemos. Voy a empezar por preguntarles si hay algún miembro de SSAC que quiera hacer una pregunta.

Creo que hay alguien a la izquierda que quiere hacer una pregunta.

ORADOR DESCONOCIDO: En los últimos seis a nueve meses, estuvimos diciendo que los ataques de denegación de servicio llegaron a una proporción muy importante. Continuamente nos dicen que la Internet de las cosas se está volviendo hostil. Esta no es la Internet con la que soñábamos. Ahora parece un lugar muy peligroso, perverso. ¿Qué hacemos al respecto? ¿Qué podemos hacer al respecto?

PATRIK FÄLTSTRÖM: Si están en el público y pueden contestar esto, acérquense al micrófono y van a poder participar en SSAC. ¿Hay alguien que quiera responder a esta pregunta?

JONATHAN MAKOWSKI: Gracias por el trabajo que están haciendo para ayudar a la comunidad. Tengo una serie de comentarios que quiero hacer y escuchar sus comentarios. Uno tiene que ver con DNS y si debe haber algunas guías o pautas con respecto a los sinkholes, hablando de la falta de precisión de WHOIS o el potencial de que se caiga el sistema. Sé que hay un gobierno que está trabajando para presentar la legislación en ese tema y me pregunto si ustedes están hablando de esto o si es un tema importante para

la comunidad desde el punto de vista de ustedes. Tengo otras preguntas pero empecemos por esta.

PATRIK FÄLTSTRÖM: Empecemos con esta. No sé si hay alguien aquí que pueda contestar esto. Rod.

ROD RASMUSSEN: Yo hablé de esto antes con Jonathan. Este tema de sinkholes fue la génesis de un grupo de trabajo que fracasó hace varios años pero quizá sea hora de volver a ocuparnos de esto. Yo no sabía que Suiza estaba tratando de desarrollar legislación sobre esto. Para aquellos de ustedes que no sepan qué es un sinkhole de DNS, es esto. Si un nombre de dominio o cualquier nombre de host se está utilizando para mandar malware o para tomar comando y control, si el dispositivo entra en nombre de dominio para buscar instrucciones y en base a esas instrucciones el servidor le dice lo que tiene que hacer. Lo que pasa si uno es autoridad de aplicación de la ley o investigador o una empresa de seguridad es que esos nombres de dominio son dados de baja por el registrador y en algún momento se vuelven a poner en el pool para que pueda ser registrado de vuelta ese dominio o quizá se llegue a un acuerdo con un registrador. Se toma ese nombre de dominio y se apunta a lo que llamamos un sinkhole. Las computadoras infectadas van a seguir comunicándose con

ese servidor. En ese caso, si hay comunicación, podemos saber qué computadoras están infectadas en alguna parte del mundo y, según nuestros objetivos y fines, podemos trabajar con las empresas de hosting, notificarlas o se puede usar esa información para notificación, se pueden usar ambos caminos.

Hay muchos ejemplos. Algunas empresas crearon todo su negocio en base a este tipo de datos que después venden como información que las personas pueden utilizar para protegerse y también se utiliza para otros fines menos serios, por eso tenemos la pregunta de cuán ético es todo esto. Hace un par de años había una empresa de seguridad que dirigía a los registradores y les robaba los sinkholes de otras empresas de seguridad y obviamente esta es una zona compleja, peligrosa.

El tema sigue siendo importante. Les voy a dar otro ejemplo de un sinkhole, es que se da cuando un autor de un malware escribe un algoritmo de generación de dominio. Aquí hay otro algoritmo que pueden recordar. Con este algoritmo de generación de dominio, lo que pasa, el ejemplo más famoso es el de Conflicker. ICANN ayudó mucho a luchar contra este problema. Lo que pasó en ese caso es que el algoritmo estaba allí y tenía toda una lista que iba desde un par de docenas a miles de nombres de dominio a los que trataba de llegar para obtener comandos. Esos eran dominios que en su mayoría no estaban registrados. Esto causaba muchos problemas pero era información muy útil para

la gente de seguridad porque no tenían que ir a un dominio que ya existía para manejar malware sino que podían simplemente registrar un dominio y hacer un sinkhole y obtener la misma información de todo esto.

Las políticas al respecto son bastante vagas y poco estrictas. Quizá haya escuchado hablar en otras reuniones de la ICANN de registrador de último recurso que se ocupan de las operaciones de sinkhole. Varios investigadores, organismos de investigación pueden utilizar este registrador para poner bajo esta registrador los dominios tóxicos y después utilizar reglas para usar esa información, pero esto está creciendo mucho. Quizá ya hayan escuchado hablar de Avalanche. Es algo que empezó en el año 2008. Ya se ha arrestó a la mayor parte de las personas que estaban tras este ataque. Se tardó como 10 años. Estos dominios fueron manejados por ese tipo de sistema. Por ahora es un área en la que se está trabajando pero si los gobiernos están interesados en regularlo, quizá debamos analizarlo y considerarlo.

DANNY MCPHERSON: Iba a decir un poco lo que dijo Rod. Tenemos actividades donde se dan de baja dominios. También hay algunas actividades de alto impacto que afectan a los consumidores como ransomware y diversos tipos de delitos cibernéticos y otras cosas peores aún.

El espacio de nombres se puede utilizar para navegar por Internet y no para realizar tareas maliciosas. Cuando se hacen actividades maliciosas, debemos hacer todo lo posible para proteger a los consumidores.

El registrador de último recurso es el que tiene el mayor poder de detener todo esto pero debemos encontrar la manera de ser más eficientes. También hay un grupo de trabajo de seguridad pública que considera cómo cambiar algunas cosas para resguardar y proteger a los consumidores. Además, hay algunos documentos que ya se han publicado sobre cómo opera la Internet y hay una especie de resúmenes que establecen demasiadas instrucciones. Lo interesante sería ver cuál es la información que se intercambia hoy en día y ver qué actividades se están desarrollando. Debemos trabajar con las autoridades de la aplicación de la ley para lograr un impacto estratégico a largo plazo.

Uno de los temas que preocupan hoy en día en mi trabajo diario, donde debemos proteger la infraestructura de equipos, seguimos [inaudible] equipos como firewalls y otro tipo de equipos. Cada vez tenemos más identificadores técnicos, nombres de dominio, direcciones de IP, firmas de archivo, etc. Muchos de estos elementos en algún momento sobre todo si no se pueden utilizar habría que ver cuáles son los efectos a largo plazo para poder limpiar todo esto. Eso es importante desde el

punto de vista de operación de la infraestructura. Aquí hay otros temas relacionados. Habría que tratar de colaborar con diferentes personas, ver cuáles son las capacidades contractuales de los diferentes actores y después trabajar también del lado de la seguridad de la Internet y ver qué pasa con las operaciones de los registros para ver cómo combatir juntos estas amenazas. Si hay algo que el SSAC debe decir o hacer, bueno, vamos a volver a analizarlo pero tuvimos un grupo de trabajo que se ocupó de esto y el tema era tan amplio y ahora se está volviendo mucho más problemático con el espacio global de nombres que también tienen problemas con la privacidad, por ejemplo.

PATRIK FÄLTSTRÖM: Gracias, Danny. ¿Alguien más quiere tomar la palabra? Lamentablemente, el miembro de SSAC que está trabajando específicamente con el registro que mencionó Rod no está aquí. Si no, le podríamos pedir más información. Muchas gracias.

DAN YORK: No tengo una pregunta. Más bien quiero decir que usted mencionó en su lista de actividades en curso los talleres DNSSEC. Quería decirles que este taller acaba de terminar. Muchos de nosotros estuvimos allí pero para los que no asistieron, hubo 100 personas durante todo el día y hubo unas presentaciones

importantes que invito a que los miembros del SSAC vean y analicen. Tuvimos un panel sobre la implementación de DNSSEC en Europa. Teníamos .DE, .DK, .IT. También estuvieron allí .CZ. También tuvimos una sesión sobre los ISP. Allí estuvo Paul, representando a Comcast. Explicó lo que estaban haciendo los ISP para prepararse para el traspaso de la KSK y tuvimos una serie de demos y presentaciones que mostraban cómo se utilizaba DNSSEC para proteger el correo electrónico. La parte más interesante de este taller es que había personas allí que participaban en diferentes proyectos que se reunieron para ver cómo estos proyectos podían interactuar mejor entre sí. También para aquellos de ustedes a los que les interesan las estadísticas, el señor van Rijswijk de SURFnet dio una presentación sobre la implementación de ECDSA y habló de la criptografía dentro de DNSSEC y mostró muchas buenas estadísticas.

Jeff, tus estadísticas fueron mencionadas muchas veces y esta persona también está interesada en coordinar un grupo para hacer una medición de la validación DNS a medida que nos acercamos al 11 de julio cuando tengamos la nueva clave. Por supuesto, todo lo que tiene que ver con esto. Están las grabaciones, están las diapositivas. Quiero agradecerle a SSAC por el apoyo que nos dan allí. Ha sido una muy buena sesión.

PATRIK FÄLTSTRÖM: Gracias, Dan. Quiero decirte que no tenemos ninguna intención de poner fin a esta cooperación. Tratamos de hacer exactamente lo contrario. Seguir cooperando.

MARIA HALL: Soy Maria Hall. Soy miembro de la junta ejecutiva de RIPE NCC pero también estoy a cargo del capítulo de SSAC en Suecia. Rod mencionó un tema que me resulta interesante. ¿Cuál es su nombre de vuelta? ¿Me lo puede repetir?

ROD RASMUSSEN: Rod Rasmussen.

MARIA HALL: Quisiera que usted me explique, usted o alguna otra persona del SSAC, un poco más sobre los desarrollos de la Internet de las cosas porque eso se relaciona con el tema que usted mencionó. Por supuesto, todo está conectado pero quisiera escuchar un poco cuáles son sus ideas al respecto. Como presidenta del capítulo de SSAC en Suecia, la semana pasada tuvimos una reunión de la junta directiva y hubo una sesión sobre la Internet de las cosas. Una persona habló sobre algún tipo… No sé si eran normativa o legislación, o algún requerimiento técnico con el que debían cumplir todos los proveedores, ya sea que vendieran

cepillos de dientes o heladeras. Hablaron un poco de todo esto. No sé si usted escuchó hablar de esto.

PATRIK FÄLTSTRÖM: Hemos estado analizando esto. Uno de los problemas más importantes que tenemos todos con la Internet de las cosas es que las personas compran los equipos, los conectan y después no los tocan. Mucho de esto significa que no se actualiza el software aunque encuentran bugs y hay muchos casos en los que no se puede actualizar el software aunque uno quisiera hacerlo. Este es otro tema de preocupación en cuanto a la legislación. Obligar a las personas es como decirles a todos los delincuentes que no tienen permiso de entrar en forma ilegal en las casas. No funciona tan bien esto. ¿Hay alguien más que quisiera agregar algo al respecto? ¿Danny?

DANNY MCPHERSON: Hay una serie de lugares donde están los problemas. Fue una buena pregunta. Deberíamos decir algo sobre esto en el foro público también, creo. Los operadores de registro que participan de esto en el ecosistema, ya sea en la infraestructura de la raíz o dominios de alto nivel o de segundo nivel, etc. Los que reciben los paquetes de los ataques y ataques a gran escala, todos debemos tomarnos esto muy seriamente y tenemos que mejorar la estructura, buscar nuevas maneras de colaborar y preservar la

disponible de esa estructura. Estamos en una red. Si uno está en el negocio de las redes, la confianza en la navegación, cuando ve un ataque como este, esto puede causar mucho daño. Es todo un problema. Las alianzas que pueden crear y ayudar a crear la ICANN y las comunidades que se ocupan de la seguridad son una parte de la moneda.

Por otro lado, todo el trabajo que ya tenemos de SSAC04 con anti-spoofing, que es una de las formas de ataque en algunos de los ataques basados en la Internet de las cosas, una serie de documentos de SSAC que se ocupan de todos estos temas relacionados con las actividades o los ataques DDoS. Los servidores de nombres son un ejemplo aquí. Algunos de los códigos de ataque atacaron estos servidores de nombres específicamente. No estoy seguro de cuántas de esas actividades realmente le corresponden a la ICANN pero creo que hay muchas personas en la comunidad que pueden afectar lo que está haciendo. Hay marcos de confianza de la IoT y hay muchas organizaciones como la Online Trust Alliance y otras que están trabajando en todo esto, por lo menos América del Norte y también a nivel global donde se están desarrollando mejores prácticas.

Creo que hay más dispositivos, vivimos en más lugares, habrá menos posibilidad de proteger a todos. Debemos tratar de aumentar las exigencias para mejorar la operabilidad, la

seguridad y para poder controlar los ataques especialmente en DNSSEC en el espacio de nombres y de números de Internet. Nosotros invertimos mucho en capacidad para poder defendernos de los ataques DDoS. También tratamos de celebrar alianzas para protegernos mejor y tomamos esto muy seriamente.

PATRIK FÄLTSTRÖM: Geoff.

GEOFF HUSTON: Hay dos cuestiones aquí. Por un lado la parte de software, donde vemos que no hay un mercado para el software de alta calidad sino que hay un mercado para las cosas baratas en la Internet de las cosas. Naturalmente, inherentemente es malo. Con cualquier reglamentación que tengamos, tendremos un efecto efímero. Estamos bloqueados en una situación donde el botnet más invasivo permanece allí y aparentemente nadie lo usó durante años excepto las cámaras de vídeo. Esto es algo que es muy malo y no hay forma de cambiarlo.

Lo que hemos observador es que hay dos protocolos que funcionan en Internet de hoy. Solamente dos: HTTPS y el DNS. Es por eso que el DNS es el punto de vulnerabilidad. No tiene sentido montar un botnet a menos que se pueda rentar por

horas y hacer algún control. El canal de control es el DNS. Se pueden utilizar millones de dispositivos para hacer algo malo y el DNS va a estar allí. ¿Cómo podemos hacer que el DNS envíe una señal de que hay algunos riesgos que interfieren con esos canales de comando y de control? Esto hace que todos se desesperen porque del lado de la oferta tenemos unas cifras enormes con cada vez más dispositivos que se conectan a Internet y va a aumentando todo el tiempo. ¿Qué podemos hacer? Esperar que podamos hacer algo productivo en el DNS para entender estos canales de control. Hacemos el intento. ¿Estamos ganando? No. Pero lo intentamos.

PATRIK FÄLTSTRÖM: Rod.

ROD RASMUSSEN: No voy a ser tan negativo, tan pesimista como Geoff. Creo que hay algunos aspectos que tenemos que mencionar para entender el problema fundamental. Cuando uno piensa en la Internet de las cosas, hay más cosas en Internet que las que teníamos antes. Un par de órdenes de magnitud más altos. Esto nos trae algunos problemas. El primero es la escala. Si aumentamos en Internet en un par de órdenes de magnitud en los próximos 10 años tendremos un problema de escala. El otro problema es el uso indebido de esa infraestructura. El tema con

estos dispositivos tiene que ver con los fabricantes del software que en realidad no son compañías de software, para nada. Están simplemente tomando bibliotecas, cosas así, vertiéndolas allí, incluyendo cosas que tal vez no deberían como parte de esa pila de tecnología y no están aplicando las buenas prácticas. Por todos los años que nosotros estuvimos trabajando y criticando a Microsoft, en realidad hoy están haciendo un muy buen trabajo pero no todos están haciendo lo mismo al construir esos dispositivos.

Hay muchos lugares donde se está haciendo una normalización ahora. Creo que hay cosas que se pueden hacer en la cadena de abastecimiento. Antes de ponerlos en Internet, ya tenemos que tener el nivel de seguridad. También creo que no vamos a resolver el problema a nivel de dispositivo porque tenemos una escala muy grande. Muchos más dispositivos que seres humanos en el planeta. Es difícil resolver pero hay algunos puntos de control. Hay puntos de acceso. Hay cosas que podemos hacer con la infraestructura y el hardware para buscar cosas que están conectadas a Internet en maneras que no deberían. ¿La tostadora debería estar comunicándose con alguien de Kazajistán, por ejemplo? Nadie está haciendo esa verificación. Hay pequeños pasos que podemos dar como administradores de infraestructura. Esperamos, por lo menos, reducir un poco estos

riesgos. No sé si hay alguien más que quiera decir algo. Warren está desesperado por decir algo.

WARREN KUMARI: Uno de los problemas es el término. Internet de las cosas, que significa básicamente lo que uno quiera que signifique esta semana y cambia la semana que viene. Como dijeron varias personas, hay muchos más dispositivos fabricados de la manera más económica posible porque quieren poder vender muchos más. Esto está apoyado por empresas que no tienen el software como su competencia central tecnológica. Esto también hace que junten distintos elementos y piensen que esto vuele.

Si hablamos de BCP, no sé si vamos a lograr mucho. Hay gente que está tratando de seguir las mejores prácticas pero está trabajando de esta manera con una recolección de componentes. Creo que tenemos que velar porque haya algún control en la cadena de abastecimiento para saber cómo ese dispositivo se está comunicando con otros. Si observamos estos dispositivos, se conectan a muchas cosas y es sumamente difícil entender por qué. Tienen vínculos, relaciones con muchas otras cosas. Si esto ocurre, hay que hacer tal cosa. Los servicios AWS, Amazon, por ejemplo, hay muchas cosas que son engañosas. Lo que tal vez podría ayudar a mejorar la situación es ver qué pasa con la CPE. Los fabricantes en general ya no hacen su propia

programación para CPE. Toman el software que ya existe como Tomato o algunos otros.

ORADOR DESCONOCIDO: ¿Qué es CPE?

WARREN KUMARI: Equipo Personal del Cliente. Por ejemplo, lo que uno compraría. Su firewall, su gateway. Los que desarrollan programas en realidad están usando el software que ya existe y cambian como la carátula en lugar de decir NETGEAR dicen Linksys, por ejemplo. Si pudiéramos crear un marco, un conjunto de herramientas que les permitiera a las personas rápidamente construir un dispositivo de la Internet de las cosas, algo que les permita descargar este software, seleccionar los módulos que quieren, poner su logo aquí y hacer ver como que uno tiene algo sofisticado, esto va a ser más económico que construir algo de cero. Si pudiéramos desarrollar una serie de herramientas, cadenas y marcos que puedan utilizar los fabricantes y que tengan incentivos para usarlo en lugar de desarrollarlo de cero, creo que podríamos lograr algún cambio en el sistema.

ORADOR DESCONOCIDO: Hace 25 años fundé una compañía de seguridad y en ese momento no íbamos a conectar la heladera o la tostadora pero

ahora hay dispositivos que son muy importantes y que no pueden tener ese parche por una cuestión de cumplimiento. Uno para demostrar que es seguro, pero tampoco se puede conectar con la máquina de radiografías en el hospital por cuestiones de seguridad. El otro extremo de la Internet de las cosas tiene que ver con que uno no puede parchear eso. Eso hay que tenerlo en cuenta. Hablamos de la seguridad de HTTPS, sí, pero nuestros clientes quieren la interceptación. Quieren poder ver eso. Quieren firewalls de próxima generación que identifiquen esos ataques y, una vez que desapareció toda la seguridad quieren ver una luz verde. Piensan que están seguros pero en realidad no está en verde porque estén seguros sino porque han sido interceptados. ¿Cómo lidiamos con eso?

PATRIK FÄLTSTRÖM: Con respecto al primer tema que tiene que ver con el otorgamiento de licencias y el cumplimiento, como usted dijo, esta es otra pieza del rompecabezas. Es por eso que yo creo, como presidente de SSAC, que nosotros en SSAC en realidad no hemos encontrado un punto de partida para poder atacar este problema. La base del problema es tan grande, es muy difícil. Hay que tratar de hacer alguna recomendación que ayude a mejorar las cosas pero es muy difícil. Si hablamos de documentos, el problema con la Internet de las cosas tiene que

ver con redactar un artículo que pueda tener los derechos de autor en una hora. La velocidad de las cosas nos afecta mucho.

Con respecto al segundo comentario que usted hizo, las conexiones de TLS, en SSAC emitimos una serie de recomendaciones con respecto a cómo emitir nuevos certificados de una manera más eficaz. Nosotros tenemos un mecanismo que estamos utilizando hoy. Respondemos a ITU-De que actúa como enlace para preguntar si sería bueno lanzar nuevos certificados de autenticación o no. eso aumentaría la cantidad de certificados y la respuesta que nos dieron es que no debería haber menos. También nos referimos a DANE. La conexión de TLS, ese túnel de encriptación, tiene un mecanismo que debería continuar extendiéndose punta a punta y con tecnologías como DANE y otras similares. Tal vez sea difícil encontrar esta información en nuestros documentos pero van a ver que tenemos un pensamiento, un hilo conductor cuando hablamos de los certificados en todos nuestros documentos. ¿Alguien más?

ORADOR DESCONOCIDO: Yo soy de la Universidad de Oxford. Cuando ustedes hacen investigación, ¿qué piensan que son las otras cosas que tenemos que abordar aquellos que hacemos investigación?

GEOFF HUSTON: Yo hago mucha investigación y admito que uno de mis principales problemas es entender la Internet. No de dentro hacia fuera sino de fuera hacia dentro. Es muy fácil medir la infraestructura y es muy fácil establecer un laboratorio pero usted y los miles de millones que hay como usted, ven la Internet de las cosas de otra manera. En particular, hay proyectos masivos que observan la penetración de IPv6 en toda la Internet. Casi en tiempo real. De la misma manera, si se hace introspección en el sistema de nombres de dominio, podemos ver cuántos de los usuarios en el mundo no van a ir a un nombre de dominio si está mal firmado con DNSSEC. Tiene que estar alerta DNSSEC y tiene que haber alguna diferencia entre la verdad y la mentira. Hay mucha validación en Suecia con DNSSEC. En mi país, Australia, casi nadie lo hace. Esto varía de proveedor a proveedor, de país a país. ¿Cómo se ve la Internet para todos los que están en el borde y miran hacia dentro? Esta es una de las grandes preguntas que yo tengo porque la Internet somos todos nosotros, no solamente las piezas que están en el medio. Somos todos los que estamos en el borde.

PATRIK FÄLTSTRÖM: Warren.

WARREN KUMARI: Creo que siguiendo lo que decía Geoff, hay que ver cómo varía Internet de un país a otro. Entender mejor a qué cosas podemos llegar y a qué cosas no, como función la censura o algo por el estilo. ¿Por qué no puedo llegar a una cantidad específica de sitios desde un país? ¿Qué es lo que no quieren que yo haga o qué es lo que no quieren que vea?

DANNY MCPHERSON: Una de las cosas que yo veo que tiene mucho interés desde el punto de vista de investigación es las dependencias sistémicas. Por ejemplo, el gráfico de tránsito en el DNS o la infraestructura de la nube donde hay tiempo de residencia. Si tenemos 300 ccTLD, 60 de ellos no tienen un servidor fidedigno de los nombres para ese país. Si pensamos en las operaciones en el espacio cibernético y tenemos ese tipo de situación, entendemos que hay muchas dificultades. La infraestructura con múltiples titulares. Vemos en otras tecnologías donde uno ocasiona un impacto y destruye la funcionalidad de servidores de miles de compañías. Yo creo que cada vez va a empeorar más a medida que pasamos a una mayor infraestructura a la nube, porque hay ganancia deficiente allí. Están las implicancias desde el punto de vista de la seguridad DNS y ese tipo de situación, y también tienen que ver con la infraestructura. También la seguridad nacional, el interés nacional van de la mano con la

continuidad de las empresas. Creo que estas dependencias sistémicas y la infraestructura es algo que tenemos que ver.

CRISTIAN HESSELMAN: Para los usuarios finales, para que tengan más control de la seguridad y las cuestiones de privacidad de los dispositivos que utilizan en su casa, esto se relaciona con la discusión que acabamos de tener. La hipótesis potencial podría ser que si hay una vulnerabilidad en la seguridad, pueden conmutar ese dispositivo, lo pueden apagar, sacarlo de la red y así protegerse. Los operadores en la infraestructura de DNS también podrían hacer lo mismo. Otro tema de investigación tal vez podría ser cómo los operadores de DNS y otras partes interesadas en la infraestructura podrían colaborar y compartir datos entre sí cuando se trata de cuestiones de seguridad.

PATRIK FÄLTSTRÖM: Siguiente, por favor.

WES HARDAKER: Estaba siguiendo la discusión y nosotros hicimos lo que ustedes hicieron, lo que normalmente hacemos. Agrupar las cosas en clasificaciones que son fáciles de identificar y de medir. Países, es un ejemplo. Un estudio interesante que podría hacer el SSAC es cuántas categorías mensurables hay allí que no tenemos en

cuenta. Tal vez podemos ver qué pasa hacia arriba con las validaciones de DNSSEC, por ejemplo. La realidad es que en el mundo no se respetan las fronteras de los países. Tenemos mediciones estándar y convencionales todavía que se basan en ella, ¿pero qué más podemos tener disponible? Podemos pensar en las escuelas primarias, en las universidades para ver qué otras ideas puede haber, qué otros indicadores podríamos medir si abordáramos estas cosas de distinta manera en los distintos países.

PATRIK FÄLTSTRÖM: Geoff.

GEOFF HUSTON: Ustedes van a ver que cuando analizan estas cuestiones, podemos ver que hay números autónomos también como identificadores únicos en este tipo de sistemas. Cuando publicamos información sobre esto, si lo hacemos por país, más personas leen las publicaciones que cuando uno las publica, con lo que llamamos números del sistema autónomo, bajo ese título. La manera de publicar nuestras estadísticas y nuestras conclusiones tiene que cambiar para que la gente las lea.

NICK SHOREY: Soy Nick Shorey. Soy del gobierno británico. Recientemente comenzamos a ver la Internet de las cosas y esta noción de seguridad por default, viendo las cuestiones de viabilidad, etc. Algo que estuve repensando, sobre lo que estuve reflexionando es qué hacemos cuando hablamos de la Internet de las cosas. Tenemos todas estas compañías adicionales que no se dedican a las TIC específicamente y que de repente construyen un dispositivo de comunicaciones e informática. Lo comercializan y esto se transforma en una moda. Me preocupa la tasa con la que aumenta la cantidad de dispositivos obsoletos. Realmente recibiré con agrado sus comentarios. Tal vez no ahora pero más adelante sobre buenas ideas para resolver este problema, donde cada vez tenemos más cosas en línea que son obsoletas y que ya venció su vida útil. No sé si me pueden orientar con respecto a estudios de investigación que existan en este sentido y que yo le pueda transmitir a mi gobierno.

PATRIK FÄLTSTRÖM: Warren.

WARREN KUMARI: Creo que no tengo una buena respuesta para usted. Tengo una que es un poco más deprimente. Estaba buscando un nuevo punto de acceso desde mi casa hace poco. Empecé a buscar un punto de acceso barato y fui a Alibaba, que es un mercado muy

grande en Internet y encontré unos 700-800 fabricantes diferentes que vendían lo que para mí era exactamente el mismo dispositivo. Uno puede conseguir precios baratos para ellos. Los fabricantes hacen algunos dispositivos y luego pasan a otra cosa y ya no hacen actualizaciones. Uno se queda con ese dispositivo sin ninguna actualización. Creo que tal vez podríamos ver la solución que aplicó Linksys hace un tiempo. Uno compra un router para su casa y dura unos dos años. Misteriosamente, tienen un problema con la alimentación y después uno va y compra otro. Potencialmente, cuando las cosas son lo suficientemente baratas, mueren por envejecimiento y hay que tirarlas y tal vez el nuevo no sea tan malo. Tal vez.

PATRIK FÄLTSTRÖM: Rod.

ROD RASMUSSEN: Hay dos cosas aquí. Si hablamos de alguien que venda su auto inteligente o su dispositivo inteligente, vende su casa y tiene allí Internet conectado, ¿cómo cambiamos la contraseña? ¿Hay un manual del usuario para todos los equipos electrónicos del hogar? Hay una buena noticia. Les voy a decir que se fijen en lo que hace la Online Trust Alliance porque ellos están recabando toda esta información. Están presentando comentarios sobre esto en muchos de los foros en todo el mundo que enfrentan

este tema. Tienen marco para ocuparse de estas cosas. Estos no son asuntos nuevos. La gente está tratando de decir durante muchos años: "Este es el código que deben seguir los fabricantes. Estas son medidas de los entes reguladores", etc. Y funciona de vez en cuando. No siempre estamos de acuerdo en todo dentro de SSAC pero de alguna manera se está trabajando seriamente para resolver este tema. Podemos hablar de esto después de la sesión.

PATRIK FÄLTSTRÖM: Robert.

ROBERT GUERRA: Para tomar lo que dijo Warren, Ondrej también es de SSAC. Yo sugiero que se fijen en TURRIS.CZ. Encontrarán un documento sobre la información para actualizar un router. Tienen que ver lo que está haciendo el ccTLD de la República Checa. Allí hay datos interesantes que podrán encontrar. Se están llevando a cabo algunas iniciativas sobre este tema. Hay algunos grupos que ya están considerando esto como un tema importante. Muchas gracias.

PATRIK FÄLTSTRÖM: Última pregunta del público hoy.

JAD EL CHAM: Buenos días. Soy Jad El Cham. Soy becario por primera vez en la ICANN. En primer lugar, muchas gracias por la presentación y por sus respuestas. Tengo una pregunta que ya planteé muchas veces en estos tres días pero nunca me dieron una respuesta concreta. Escuchamos hablar de la Internet de las cosas, los ataques DDoS, etc. Aparentemente nos olvidamos de que los nuevos tipos de ataque DDoS están basados principalmente en dos protocolos, DNS y NTP. Utilizamos estos servidores. En lugar de hablar de DDoS, se habla mucho de DDoS que refleja. Esto es lo que estamos viendo en nuestro mercado. No sé si están de acuerdo. Nosotros implementamos equipos de seguridad para nuestros clientes. Mi pregunta sería la siguiente. DNSSEC realmente se ocupa de muchas de las brechas de seguridad dentro del DNS pero me pregunto qué está haciendo la ICANN para crear conciencia acerca de esta falencia del DNS cuando se utiliza como reflector. Una de las respuestas que me dieron es que hay un grupo de tareas en la IETF que se está ocupando de esto pero también quisiera saber si la ICANN está participando en este tipo de actividad.

PATRIK FÄLTSTRÖM: ICANN es una organización como muchas otras, como por ejemplo Netnod, una organización que se ocupa de muchos

servidores raíz. Google opera otro tipo de infraestructura y todos como organizaciones participamos, por ejemplo, en el IETF y otras comunidades para desarrollar mejores prácticas sobre la forma de configurar y operar estos protocolos en los casos en los que haya falencias, debilidades, para ver cuál es el protocolo más difundido que se podría utilizar como un ataque para tratar de identificarlo. He visto muchos cambios respecto del tipo de vectores que utilizan los ataques DDoS pero lo que puedo decirle es que están utilizando direcciones de IP que tomaron a través de spoofing, otras que no se han tomado a través de spoofing. Todo depende de los botnets, de cómo están configurados.

Algunos de los botnets son tan amplios y son muy difíciles de encontrar, entonces a veces ni siquiera hace falta hacer spoofing de la dirección IP. En general, los ataques vienen de tráfico HTTP. No es ningún otro tipo de tráfico. También se da que algunos ataques de reflejo están utilizando estos protocolos simplemente porque se obtiene una amplificación. Por lo tanto, hay mejores prácticas sobre la forma de configurar algún tipo de servidor a fin de que algunos de los comandos de control no puedan ser reconocidos por el servidor NTP, etc. Se están haciendo muchas cosas al respecto. La ICANN, como organización que opera este tipo de elementos por supuesto participa como lo hacemos todos nosotros.

Con respecto al PDP, hay diferentes mecanismos, a nivel de las partes contratadas y de las no contratadas donde este tipo de elementos se toman en cuenta cuando se consideran los requerimientos para las partes contratadas y también las mejores prácticas de las que se está hablando en las diferentes unidades constitutivas de la ICANN. Con respecto a los temas de operación, la respuesta es que nosotros estamos participando en la comunidad de la ICANN y en el ecosistema de la ICANN y también participamos en los foros donde se tratan estos temas relacionados con las operaciones. No sé si alguien quiere agregar algo. Warren.

WARREN KUMARI: Supongo que los temas que usted menciona específicamente son los ataques de reflejo y todos exigen la capacidad de tomar direcciones fuente a través de spoofing. Hay un documento BCP 38 que dice que no debemos permitir que nadie utilice elementos que no se toman de la red que ustedes están administrando. Hay un documento, creo que es el número cuatro, que dice exactamente lo mismo. No hay mucho que la ICANN pueda hacer al respecto. ¿Quién está a cargo del programa MANRS? MANRS es un programa de la ISOC.

ISOC tiene algo que se llama MANRS que significa modales. Las redes pueden decir que tienen buenos modales si siguen las

guías de este manual de MANRS. Lamentablemente, la ICANN en sí misma no puede hacer mucho al respecto. La ICANN no tiene un martillo para golpear a los ISP a menos que la unidad constitutiva de ISP o la SO diga: “Realmente no podemos darles tranquilamente las direcciones de ISP porque no están implementando la protección contra spoofing”. Este es un problema que existe desde hace tiempo y sigue existiendo, dando vueltas.

PATRIK FÄLTSTRÖM: Gracias. Son las 16:15. Estamos terminando. Muchas gracias por asistir a esta sesión. Aparentemente a las 3:15 el miércoles es un mejor horario para hacer una reunión que el jueves a las 8:00 de la mañana. Muchas gracias. Ha sido una información muy útil para nosotros.

[FIN DE LA TRANSCRIPCIÓN]