SAN JUAN – GAC: reunión con el PSWG
Martes, 13 de marzo de 2018 – 08:30 a 09:30 AST
ICANN61 | San Juan, Puerto Rico

CATHRIN BAUER-BULST: Buenos días a todos. Muchísimas gracias por estar aquí, en este salón, en lugar de quedarse afuera en el Caribe con el sol y el hermoso clima. Muchísimas gracias por dedicar este tiempo a la reunión del grupo de trabajo de seguridad pública. Esta es la reunión oficial de este grupo del GAC. Mi nombre es Cathrin Bauer Bulst. Soy una de las dos copresidentas. Estoy aquí con Laureen Kapin. Tenemos dos puntos importantes para tratar en el orden del día. Vamos a hablar entonces del plan de trabajo del PSWG y después vamos a hablar del trabajo que estamos haciendo con la oficina del director técnico y la herramienta del DAAR. Le vamos a dar la posibilidad al resto de los miembros del PSWG a hablar.

LAUREEN KAPIN: Yo estoy en la Comisión de Comercio Federal de Estados Unidos. Obviamente, estamos concentrándonos en lo que es la protección al consumidor. Les agradecemos a todos estar en la primera sesión del día. Tenemos esta sesión desde las 8:30 a las 9:30. También van a escuchar decir: “Después de las 9:30 ustedes van a seguir”. Sí, es verdad. Vamos a cambiar de tema. Nos

vamos a concentrar después en lo que tiene que ver con el sistema de WHOIS y el GDPR. Vamos a tener una dosis muy grande de este grupo de trabajo durante hoy a la mañana. Espero que todos se queden para la próxima sesión y que les resulte interesante.

IRANGA KAHANGAMA: Hola. Yo también estoy en Washington D.C. con el FBI. Voy a trabajar también y voy a hablar de alguno de los temas que tienen que ver con el abuso del DNS, que tiene que ver también con el DAAR. Vamos a ver algunas presentaciones y vamos a ver algunas formas en las que nosotros podemos dar respaldo a las políticas, a las recomendaciones o hacer algún aporte activo a esta iniciativa del DAAR. Realmente nosotros creemos que va a ser beneficiosa para toda la comunidad de Internet. Vamos a seguir hablando un poco después sobre todo esto.

CATHRIN BAUER-BULST: Muchas gracias, Iranga y Laureen. Laureen me acaba de hacer una buena sugerencia que es para quienes sean miembros del grupo de trabajo de seguridad pública. Les pido que levanten la mano porque tenemos muchas personas en la audiencia que tienen interés en nuestro trabajo y que quizá también a medida que continúe el día y la semana pueden estar interesados en hablar con nosotros. Les pido por favor que levanten las manos

los miembros del grupo para que todos los reconozcan y sepan dónde están.

LAUREEN KAPIN: Esta es la gente. Si ustedes tienen preguntas, no solo somos los que estamos en el frente sino que tenemos muchos miembros y todos ellos están dispuestos a hablar y responder sus preguntas.

CATHRIN BAUER-BULST: De la reunión del domingo, ustedes saben que vamos a adoptar el plan de trabajo para el próximo periodo de este grupo de trabajo. Hablamos de ello en un nivel más alto el domingo pero hoy vamos a profundizar un poco más, a ver si alguien tiene algún comentario final para hacer antes de adoptar el comunicado del GAC al final de esta reunión. El primer objetivo estratégico tiene que ver con la mitigación del abuso del DNS. Iranga tiene aquí algo para decirnos sobre los distintos puntos.

IRANGA KAHANGAMA: Gracias, Cathrin. Como mencioné anteriormente, este es uno de nuestros principales planes de trabajo. El objetivo es que la ICANN esté en una mejor posición para tratar este uso indebido del DNS. Sé que hay muchos informes. El CCT ha dado el suyo y creo que es uno de los grandes programas que tenemos en este

momento. Les pido por favor que vayan un poco a la derecha con la pantalla.

Como dije, hay varios proyectos de información sobre las actividades vinculadas con estos temas. También tenemos el índice de salud del mercado de gTLD, lo que tiene que ver con la iniciativa de datos abiertos de la ICANN. Esto también tiene que ver con ponerle ciertas cifras a este abuso, a esta salud a nivel macro. Estamos en una mejor posición para informar sobre estos usos indebidos. Voy a saltear un poco. Estamos generando principios. La idea es tener una línea de base para entender algunos mecanismos genéricos que acepten todas las partes de la comunidad, que todos nos podamos poner de acuerdo en eso, que los acordemos como grupo.

En lo que hace al trabajo nuevo, uno de los temas de los que estuvimos hablando es el SSAC. Ellos tienen varias iniciativas también que resultan interesantes y nosotros querríamos participar formalmente con ellos. Creo que en esta reunión hay una sesión a las 15:15 mañana. Es una reunión abierta a la que dijeron que todos podían asistir. Va a ser interesante ver en esa reunión algunos de los aspectos de seguridad sobre los que ellos están trabajando, los servicios de registración y los aspectos técnicos vinculados con ello. Creo que tiene que ser muy importante, sobre todo por las consideraciones vinculadas con el GDPR.

Hay gente que está muy orientada a la seguridad ahí. La idea sería establecer una relación un poco más formal con ellos para tener un ida y vuelta. Es básicamente esto lo que estamos tratando de lograr. Obviamente, podemos recibir todas sus ideas. Hay varios temas que son candentes y que tienen que ver con el abuso del DNS. Nos queda poco ancho de banda en este momento pero creo que estamos funcionando bastante bien con el trabajo que estamos haciendo. Es un tema que vamos a mantener como de alta prioridad.

CATHRIN BAUER-BULST: Antes de que Laureen vaya al tercer punto que tiene que ver con las medidas de protección al consumidor quiero recordarles a los miembros del GAC que ustedes tienen una copia de este plan de trabajo como anexo a los documentos que se le dieron y como anexo al punto 11 que debatimos el domingo en el orden del día. Pueden ir y pueden ver este plan en ese anexo.

LAUREEN KAPIN: Hablando un poco de las medidas de protección del consumidor, este ha sido un tema… El equipo de revisión de la confianza, elección y competencia de los consumidores se ha concentrado en estas medidas de protección. Este tema es una continuación del trabajo que ya iniciamos y que es luchar por políticas que protejan al público en línea. Este es el objetivo general o el más

importante de esta parte del plan de trabajo. Nosotros participamos en distintas revisiones pertinentes también. Hemos entablado una coordinación con distintas partes de la organización ICANN, sobre todo lo que es seguridad y cumplimiento contractual y también con la comunidad, para hablar de estos temas, porque todos tienen un interés en mantener un entorno que sea seguro para los consumidores y además que los consumidores confíen para seguir utilizando la Internet.

Hay distintas partes interesadas en distintas áreas de trabajo que incluyen los procedimientos posteriores a la introducción de los nuevos gTLD. También lo que es un PDP en realidad. También la acreditación de servicios de privacidad y representación. Distintas áreas de trabajo que van a continuar.

CATHRIN BAUER-BULST: Voy a hablar de los siguientes puntos que son sobre responsabilidad y que están en la página siguiente. Tienen también que ver con la explotación del abuso del DNS. Cuando hablamos de responsabilidad, lo que estamos buscando es alguien que lleve adelante este punto. Hay distintas áreas de trabajo que tienen que ver con la seguridad pública y que son pertinentes al trabajo del GAC y también al trabajo del grupo de trabajo sobre seguridad pública. Lo que queremos es mejorar la

capacidad que tenemos porque somos muy pocos los que compartimos la carga de este trabajo. Si algunos de ustedes quieren participar en algo importante e interesante le pido que se nos acerque después de esta reunión.

LAUREEN KAPIN: Sí. Aquí es cuando nosotros les pedimos a ustedes que nos ayuden a ayudarlos.

CATHRIN BAUER-BULST: Respecto de la responsabilidad, vamos a hablar un poco más en detalle en la segunda media hora de esta reunión porque, como decía Iranga, anteriormente estamos tratando de identificar fuentes de datos que nos puedan ayudar para evaluar la política existente en forma más confiable y también hacer las selecciones adecuadas para las nuevas políticas, como pueden ser cualquier ronda posterior que exista para los nuevos gTLD. Tenemos que tener las fuentes de datos correctas, los datos correctos disponibles para estar en una mejor posición cuando los necesitemos. Después hablamos de cómo evitar la explotación del DNS para perpetrar un abuso. Aquí nos vamos a tratar de concentrar en identificar los distintos tipos de usos indebidos o abusos. Obviamente, nos vamos a beneficiar de la interacción con el SSAC. También del lado de política ver cómo podemos ser más eficaces y evitar parte de esto.

Este trabajo también incluye un área de trabajo que tiene que ver con la lucha del abuso contra los niños y, sobre todo, queremos ver qué es lo que pasa con la eficacia de las medidas de protección propuestas por el GAC en su momento, para proteger sobre todo a los niños en los lugares que vienen con determinada asociación como confianza y puede tener que ver con el .KID o .KIDS. Hay una expectativa legítima de los usuarios de que esto sea un lugar seguro para los niños. Las medidas de protecciones que se adoptaron en el comunicado de Pekín tienen que ser válidas en términos de eficacia. También podemos pensar adaptarlas para las próximas rondas de nuevos gTLD. Hay un área de trabajo, y no voy a hablar mucho más aquí, pero esa es el área de la que quiero hablar y también sé que el equipo italiano del GAC se ha concentrado mucho en estos temas.

Antes de cerrar todo esto, querría saber si alguien tiene algún comentario para hacer o alguna idea para formular. Vamos a seguir con el siguiente objetivo estratégico que se concentra en el RDS particularmente. Tiene que ver con el WHOIS y el acceso a los datos de registración.

LAUREEN KAPIN: Como dije, esto lo voy a dividir porque vamos a hablar de este tema con mayor profundidad, como dije anteriormente, después

de la pausa para el café. Esto es nada más que para señalar, para que ustedes sepan que el sistema del WHOIS y todos los beneficios y las responsabilidades asociadas son parte de nuestra área de trabajo y nos hemos concentrado en ello en este último tramo de trabajo.

CATHRIN BAUER-BULST: Esto nos lleva entonces al PDP de RDS de siguiente generación. Habló Alice Munyua la otra vez de esto. No sé si quiere decir algo hoy al respecto. ¿No? Perfecto. Es algo que continua en marcha. Después tenemos la exactitud de los datos de registración. Ustedes también saben que hace tiempo que se está hablando de esto. Ahora hay alguna implementación como para verificar lo que es la sintaxis en la exactitud de la registración de los datos. De lo que la comunidad no habló todavía es de verificar la identidad del registratario. Sigue habiendo, desde el punto de vista de la seguridad pública, la verdad es muchas posibilidades de mejorar la calidad, sobre todo en los datos de registración de GDPR. En el mundo del ccTLD creo que todavía hay posibilidades de que esto sea más confiable sin tener mayores costos. Vamos a ver cómo estos esfuerzos pueden realmente traducirse en el mundo de los gTLD.

IRANGA KAHANGAMA: Quiero agregar algo. Es muy importante dentro del plan esta sección porque tenemos que pensar que el GDPR también nos pide una exactitud en los datos y eso es parte de nuestra responsabilidad. Necesitamos tener los datos. No nos hemos concentrado porque ahora estamos tratando de mantener los datos y el acceso pero tenemos este segundo paso que es que realmente sean exactos estos datos que tenemos. Tenemos que tener esto presente porque va a ser una herramienta muy importante y es algo que va a tener que incorporarse en la siguiente versión del WHOIS porque son los requisitos del GDPR, ser un poco más exactos.

CATHRIN BAUER-BULST: Gracias, Iranga. El último punto en este segundo objetivo estratégico es la verificación de la implementación. Es decir, cómo es el cumplimiento de la misión de la ICANN en relación con los RDS. Lo importante aquí es que tenemos un equipo de revisión y se ha nominado a través del GAC a la representante de Estados Unidos, al representante de la INTERPOL y a mí para participar. Tenemos que ver entonces qué es lo que va a pasar cuando nos reunamos en la siguiente reunión de Panamá. Laureen, por favor.

LAUREEN KAPIN: Este es el objetivo estratégico dos. ¿Alguien tiene algún comentario sobre todos estos puntos incluidos en este objetivo estratégico? Entonces vamos a pasar al objetivo estratégico tres que es como los fundamentos que tienen que ver con generar una operación flexible y eficaz del PSWG. Esto tiene que ver con nuestro marco de organización y nuestros procedimientos. Van a ver que aquí hablamos de desarrollar un plan de trabajo que es el primer paso. Después fortalecer el liderazgo. Como mencionamos el domingo, nosotros queremos tener un gran reservorio, por así llamarlo, porque hay muchos temas importantes y queremos que la gente se concentre en estos distintos puntos.

También queremos fortalecer la cantidad de miembros que tenemos. Una de las ideas es que estuvimos hablando con las autoridades del GAC. Es alentador que todos los miembros del GAC consideren nominar y difundir y llegar a las autoridades de aplicación, expertos de seguridad pública dentro de su gobierno porque esta gente existe en cada uno de sus países, gente que conoce mucho sobre lo que es la investigación en la línea de fuego como saber y detectar actividades criminales, sobre todo cuando estamos hablando del DNS. Sabemos que esto a veces se vuelve muy técnico, muy complejo y ustedes tienen expertos en el país con los que pueden consultar. Nosotros los alentamos a que lo hagan formalmente, que se pongan en contacto con ellos,

que los nominen como asesores del grupo de trabajo de seguridad pública. Pueden participar en las llamadas telefónicas. Pueden participar en la lista de distribución de correos electrónicos. Si existen los recursos, pueden venir a las reuniones también. Es importante que todos participen activamente en todos estos temas que tienen que ver con seguridad pública. Quería resaltar ese punto.

Después también somos un comité asesor y somos un grupo de trabajo del comité asesor gubernamental. Tenemos que asegurarnos de que nos estamos comunicando uniformemente y coherentemente con el GAC, con sus autoridades para que sepan en qué estamos trabajando. Nosotros les vamos a decir si hay algún tema candente que requiera de la acción rápida de ustedes. Tuvimos un ejemplo recientemente porque les pedimos que analizaran cosas que eran complejas, que lo hicieran con mucha velocidad. No es la situación ideal pero desafortunadamente es la situación en la que nos encontramos y queríamos entonces estar seguros de que estábamos haciendo todo con la mayor eficacia posible. Ponerlos al tanto de lo que está pasando, darles una alerta para que ustedes revisen algo que tenga que ver con el PSWG y recibir los aportes de ustedes para trabajar con ustedes y que el producto final refleje una posición de consenso del GAC. Ese es nuestro plan.

Al respecto, también tenemos siempre presente que queremos escuchar lo que ustedes tienen que decir sobre lo que hacemos bien y lo que podemos mejorar. Les pido que no tengan vergüenza, no sean tímidos porque queremos hablar con ustedes en los pasillos, por teléfono. Cada vez que ustedes crean que hay que hacer algún ajuste, estamos aquí para escucharlos. Este es el objetivo estratégico tres del plan de trabajo. Querría recibir comentarios o preguntas al respecto. Jason, por favor.

CANADÁ: Buenos días. Soy Jason, miembro del PSWG en representación de Canadá. En Abu Dabi se dio a conocer que este era un grupo relativamente homogéneo en el sentido de que había muchos de América del Norte y de Europa occidental pero quisiera decir que nos gustaría diversificar la composición de nuestro grupo. Si ustedes cuentan con personas que consideran que serían buenos candidatos para trabajar con este grupo de trabajo de seguridad pública, acérquense a nosotros. Les podemos decir cómo hacerlo, cómo participar. Cuanto más diversos seamos, más fuertes seremos.

Creo que ese es el mensaje que queremos transmitir. El hecho de que hay muchos de América del Norte y de Europa occidental no significa que no queramos tener las opiniones de otras partes del mundo. Realmente nos gustaría contar con ellas. Acérquense a

nosotros y los podemos ayudar a que se sumen o que alguien de sus autoridades de seguridad pública se sume a nosotros.

CATHRIN BAUER-BULST: Gracias, Jason, por resaltar esto. Realmente es muy importante. Quisiera agregar que cuanto más diversos seamos, más vamos a reflejar la composición del GAC en pleno. Esto es muy importante para nosotros ya que somos un grupo de trabajo que los ayuda a ustedes a hacer su labor y funcionaríamos mejor si pudiéramos reflejar las distintas posiciones que existen en el GAC también en el grupo de trabajo.

Gran parte de la tarea que hacemos no se realiza en estas reuniones. Tenemos llamadas mensuales en todo el grupo. También llamadas semanales entre quienes están encargados de algún tema en especial. Normalmente lo hacemos a través de la sala de Adobe Connect. Si ustedes quieren designar a un experto que ya sabe que no va a poder asistir a las reuniones, eso no es clave, no es lo más importante. Por supuesto, es mejor si pueden estar en las reuniones presenciales de vez en cuando pero la mayor parte del trabajo que hacemos se hace fuera de estas reuniones a través de una participación remota. Quiero alentar a todos a los que les preocupa también desde el punto de vista de los recursos invertir tiempo en el trabajo de este

grupo, que eso no los va a impedir participar, el hecho de que no puedan estar físicamente en las reuniones.

Me voy a detener a ver si hay algún comentario más sobre este punto tres o si alguien está tan entusiasmado y quiere ahora ya sumare o incorporarse a nuestro grupo. Si no hay más comentarios sobre este tema, vamos a pasar al objetivo estratégico cuatro que en realidad tiene que ver con hacer difusión externa y acercarnos a otras partes interesadas de la comunidad fuera de este ámbito.

Estamos evaluando qué es lo que estamos haciendo en nuestro plan de trabajo y uno de los puntos principales es asegurarnos de que al fijar nuestras prioridades estas sean las correctas. Para ello, por supuesto, tenemos que hablar con aquellos de ustedes que están aquí en la sala y también con otros que están fuera de ella para ver qué es lo que los está afectando en cuanto a las políticas que se están desarrollando y cómo está funcionando la implementación de las políticas actuales y cuáles son las oportunidades para hacer mejoras, los grandes problemas que pueden estar surgiendo y que quieren que nuestro grupo trate y dé su opinión o le informe al GAC al respecto.

También estamos trabajando para desarrollar una toma de conciencia de nuestro grupo por parte de los organismos gubernamentales, para que todos los países con los distintos

organismos estén al tanto de que estamos aquí y que podemos hacer aportes. No se trata solamente de las fuerzas de policía. Hay muchas cuestiones vinculadas con la seguridad pública que pueden incorporarse y reflejarse en el trabajo que hacemos en nuestro grupo.

Por supuesto, estamos trabajando también para bajar las barreras a la participación. Es decir, estamos tratando de brindar mejor información. Tal vez estén familiarizados. Cuando uno le explica qué es lo que ocurre en la ICANN a otra persona o se duermen o después dicen: "Se terminó ya el tiempo para la reunión". Es muy desafiante tener las contribuciones correcta porque uno dice: "¿Qué decimos en esta reunión? ¿Qué van a hacer en este otro tema?" Hablamos y avanzan las cosas pero nos está llevando tiempo llegar a alguna conclusión. Por muchos motivos, puede resultar muy difícil que las personas estén al tanto de lo que ocurre aquí, entiendan la importancia de lo que se discute aquí y a su vez estén en condiciones de identificar por qué les importa y cómo podrían contribuir a ese debate.

Estamos trabajando en distintas maneras de reducir esas barreras a ese acceso a través de boletines, resúmenes breves que cuentan lo que ha ocurrido aquí, para que nuestro trabajo sea más accesible para aquellos que no están empapados a diario de las cuestiones de gobernanza.

Tuvimos muy buenos aportes durante nuestras reuniones entre las reuniones de la ICANN porque hay muchos organismos que normalmente no participan en este trabajo y que nos hicieron muy buenas preguntas sobre por qué nos ocupábamos de determinadas cosas y nos compartieron cuáles eran las ideas que tenían para que nosotros nos acercáramos a ellos. Estamos trabajando para poner en práctica esas ideas. Como pueden ver aquí, también hay más espacio para que haya más voluntarios que se sumen a nuestro esfuerzo. Me siento como que estoy tratando de recaudar fondos aquí.

LAUREEN KAPIN: Iranga va a hablar acerca de algunos esfuerzos de difusión externa que tenemos en esta reunión.

IRANGA KAHANGAMA: Gracias, Cathrin. Tal vez este sea el lugar adecuado para brevemente mencionar que estamos tratando de empezar a hablar con SSAC en mayor profundidad para explicarles qué es lo que hacemos. Ellos también tienen un trabajo muy interesante y en el transcurso de nuestras actividades también hablamos con los registradores y los registros sobre las cuestiones que tienen que ver con RDS y con WHOIS, ver cuál es su visión de cómo se están desarrollando todos estos debates. Ese es el tipo de acciones de difusión externa que estamos haciendo. Con OCTO

por supuesto es algo que vamos a hablar en unos minutos aquí y también vamos a hablar de DAAR. Hay mucha creatividad en este ámbito. Si tienen alguna idea de comunidades a las que vale la pena tratar de llegar, por favor, hágannoslo saber.

CATHRIN BAUER-BULST: Gracias, Iranga. Con respecto a conocer mejor otras partes de la comunidad, les quiero recordar que hay un evento social que tenemos esta noche con los registradores. Creo que comienza a las 6:30 en la terraza. Por favor, súmense a nosotros si quieren participar y conocer a otras partes de la comunidad mejor. Creo que con esto concluimos. No sé si hay alguna otra idea creativa o alguien que quiera tomar la palabra aquí. De lo contrario, con esto concluimos nuestra revisión del plan de trabajo. Si tienen algún comentario adicional o alguna pregunta más o sugerencia para que le hagamos modificaciones a este plan de trabajo, por favor, acérquense a uno de nosotros o envíennos un email hacia fines del día de hoy. De lo contrario, daremos por entendido que esto está cerrado y le transmitiremos esto al GAC para que sepa que se aprueba este plan de trabajo.

Muy bien. Esto significa que podemos pasar a la segunda parte de nuestra reunión, que tiene que ver con la conversación sobre OCTO y DAAR. Muy bien. Veo que David se está acercando.

Gracias por tomarte el tiempo para venir, para que entendamos este tema. Sé que estás muy resfriado. Lo lamento.

DAVID CONRAD: Buenos días a todos. Les pido disculpas por esta voz que tengo porque estoy un poco resfriado. Tal vez tosa de vez en cuando. Estoy aquí remplazando a John, que parece que lo pasó muy bien después de la gala de ayer. Esto no es el resultado de la gala, como estoy yo hoy. Pasemos a la siguiente diapositiva.

Estoy seguro de que la mayoría de ustedes están familiarizados con lo que es DAAR. Para los que no lo conocen, DAAR es un sistema de información que estamos desarrollando con la ayuda del grupo de amenazas cibernéticas para tratar de identificar el abuso, el uso indebido, sobre todo esas instancias que fueron identificadas por el GAC en el comunicado de la reunión de Pekín, que tiene que ver con el farming, que es algo que hemos visto en la ICANN, y también con el spam.

¿Cómo se diferencia DAAR de otras herramientas que ya están disponibles? Se diferencia por la cantidad de datos que nosotros recabamos. Básicamente tenemos distintas corrientes de datos acumulados y los datos se recolectan y se guardan para poder hacer estudios históricos y nos vamos a focalizar en la multiplicidad de tipos de abuso que podemos ver donde se genera información que es transparente y reproducible para

facilitar la comunicación para que se puedan desarrollar políticas dentro de la comunidad de la ICANN. Yo ya hablé de esto. Lo que es importante destacar en este caso es que nosotros otorgamos licencias a una gran parte de los datos que utilizamos para DAAR y tal vez puedan o no estar disponibles estos datos en algunos casos.

¿Para qué se puede usar este sistema DAAR? Obviamente, el objetivo principal es poder reportar aquellas actividades que representan una amenaza a nivel de los registradores o de los TLD, hacer estudios de las amenazas de seguridad o de la actividad en las registraciones de dominios. Puede ayudar a los operadores también, a los registradores y a los registros y a los operadores de backend a considerar cómo pueden manejar sus reputaciones y sus sistemas antiabuso. También nos permite a nosotros hacer un estudio de las conductas de registración maliciosas y también apunta a asistir a las comunidades de seguridad operacional. Siguiente diapositiva, por favor.

Uno de los conjuntos de datos que utilizamos son los datos de zonas TLD. Se recolectan todos los datos de las zonas de TLD para la analítica de los registros de gTLD. Básicamente utilizamos el servicio de datos de zona centralizado y donde es posible hacemos también transferencias de zona. DAAR solamente va a usar nombres de dominio que aparecen en la zona. No vamos a intentar buscar las bases de datos de los

registros o los registradores antes de que estos nombres estuvieran incluidos en zonas. Actualmente tenemos unos 1.240 gTLD, lo cual nos lleva a 195 millones de dominios aproximadamente. Varios ccTLD se han acercado a nosotros para decirnos que quieren participar en esta iniciativa DAAR. Hay que ver exactamente cómo los podemos incorporar al sistema DAAR.

DAAR también utiliza WHOIS. Solamente utilizamos una parte muy pequeña de WHOIS, más que nada los datos de los registradores, pero esto puede ser bastante problemático dado que DAAR se focaliza en intentar desarrollar un sistema que sea reproducible para cualquiera. No generamos ninguna información que esté disponible internamente dentro de la ICANN. En realidad, estamos utilizando información que está disponible de una u otra manera al público. Como resultado de ello, estamos tratando de extraer información para millones de dominios a través de los servidores existentes de WHOIS y, como muchos de ustedes sabrán, esto puede ser realmente un desafío desde el punto de vista de la velocidad con la que nos podemos mover.

Si nos fijamos en los conjuntos de datos de amenazas, utilizamos varios. Tratamos de identificar de manera única los datos para que no haya muchos falsos positivos. Utilizamos los conjuntos de datos de abusos de URL o de dominios múltiples para poder

en realidad ver más que nada lo que se asocia con phishing, la suplantación de identidad, malware, hosting, botnet y spam. También tratamos de generar histografías y cuadros gráficos con el foco puesto en DAAR y en reflejar cómo aquellos que están fuera de la comunidad de la ICANN ven el ecosistema de los nombres de dominio. Siguiente diapositiva, por favor.

Dentro de OCTO, nosotros no componemos nuestras propias listas de bloques de reputación. Presentamos un acumulado, una imagen compuesta de los datos que están disponibles a través de entidades externas. Estas entidades generan esas listas que bloquean las amenazas. DAAR recolecta todos los mismos datos de abuso que se informan a la industria. Por lo tanto, no estamos generando nada nuevo aquí.

Una de las inquietudes en común que tienen muchas personas es que nosotros estemos generando nuevos datos que tal vez no sean exactos pero en múltiples ocasiones hemos reiterado que esto es lo que los operadores de correo, los prestadores de servicios de Internet utilizan a diario. No estamos creando nada nuevo aquí.

Los criterios para incluir estas listas de bloqueos de reputación en el sistema tienen que tener una clasificación de amenaza que se condiga con nuestras propias amenazas de seguridad. Tiene que haber evidencia de que esas comunidades de seguridad y

operativas confían en esas listas RBL para la exactitud y la claridad del proceso. Tiene que haber también reputaciones positivas en la bibliografía académica y estas listas RBL tienen que estar ampliamente aceptadas en las comunidades de seguridad operativa. Esto en general queda demostrado a través del hecho de que estos datos están incorporados en los sistemas de seguridad comerciales y los productos comerciales que son utilizados por los operadores de redes para proteger a sus usuarios y dispositivos y que están también utilizados por los proveedores de correo electrónico para proteger a sus usuarios del spam y de otro tipo de ataques.

Las RBL que utilizamos son bastante ubicuas. Tienden a bloquear más que el correo electrónico comercial no solicitado. Se utilizan los navegadores por ejemplo. Google Chrome utiliza la lista APWG. Se utilizan también en sistemas que proveen contenido y también en sistemas de nube. Por ejemplo, [inaudible] utiliza USRBL. Amazon utiliza otro. No recuerdo qué significa AWS aquí pero AWS WAF utiliza estas listas RBL para bloquear el abuso, los ataques volumétricos y Google también bloquea las URL maliciosas y el fraude en las palabras de la publicidad en AdWords. También tenemos RBL en el DNS que ahora utilizan las zonas de política de recursos en los resolutores. Hay otros que proveen RBL en formato RPZ.

Más detalles sobre cómo se utilizan estas listas de bloqueo. No estamos aquí usando cosas que sean experimentales. Eso es lo que queremos mostrarles. Esto es algo que ya está siendo utilizado en los servicios comerciales y en producción. Hemos estado también trabajando con los estudios académicos para revisar la información y las prácticas que están utilizando para ver cómo los investigadores pueden llegar a información de confianza y hay una serie de estudios e informes académicos sobre los RBL que nosotros estamos utilizando para DAAR.

El conjunto de datos de RBL que estamos utilizando ahora son las listas de dominios únicamente SERBL. También la lista de bloqueo de dominios que se llama Spamhaus, el grupo de trabajo antiphishing. Aquí tenemos a la derecha toda una lista compuesta de lo que se utiliza para identificar el software malicioso.

DAAR no identifica todos los tipos de abusos. No hay ningún proveedor de reputación que pueda ver todos los tipos de abusos. Cada uno tiene su propia vista del abuso que se produce en Internet. Distintas RBL se focalizan en distintas cosas específicas. Ese es uno de los motivos por los cuales nosotros hacemos esta acumulación de todas las RBL, porque queremos tener una vista más integrada, más compuesta de todas las cosas que se ven en Internet.

Normalmente recibimos una pregunta y es por qué estamos informando los dominios que son spam. En el comunicado de la reunión de Hyderabad del GAC, el GAC expresó su interés de tener información sobre el uso de spam. Desde nuestra perspectiva, la mayor parte del spam, del correo indeseado, se envía a través de medios duplicados o ilegales en general a través de botnets. Ya no se asocia únicamente el spam con el contenido que tiene que ver con el correo electrónico. Hay spam en términos de enlaces de tweets. También hay spam en Facebook y en otros sistemas de mensajería. El spam, de hecho, es uno de los medios principales a través de los cuales se implementan otras amenazas, como las que se mencionaron en el comunicado del GAC de la reunión de Pekín.

Vemos el spam como un servicio en la nube. El caso de la botnet de Avalanche, por ejemplo, les dio registraciones de dominio a sus clientes para facilitar la transmisión de spam. Lo que usamos en DAAR son los nombres de dominio que se encuentran en los mensajes de spam. Es decir, aquellos donde la gente hace clic para poder disparar así la descarga de un software malicioso o algo por el estilo. Lo que es más importante, la reputación del dominio de spam, influye en cuán extensivamente o agresivamente los administradores de correo electrónico de seguridad aplican filtros. Hemos visto que los administradores

de los sistemas primero se focalizan en el spam porque es un indicador muy bueno de los dominios comprometidos.

Nosotros ahora en el sistema DAAR que ya está en etapa de producción y lo estamos utilizando desde hace tiempo internamente, no hemos publicado informes que genera el DAAR porque queremos hacer las cosas bien, no rápido. Lo que tenemos es una revisión de un tercero independiente de la metodología del DAAR para recopilar los datos. De estas revisiones, una acaba de terminar ayer. La segunda va a terminar en un par de días. Vamos a pasar estos informes a la comunidad. Si los informes nos dan alguna sugerencia de cambios obviamente vamos a implementar esos cambios y nuestra intención es que estas revisiones nos ayuden a dársela al SSAC para que el SSAC entonces nos diga qué es lo que tenemos que hacer con la metodología que utiliza DAAR.

En este momento, los informes internos que tenemos y estos gráficos que pueden ver son nada más que internos. Nuestro objetivo en este momento es que empiecen a estar disponibles a la comunidad para poder hablar entonces de términos de política antes de la reunión de Panamá sobre lo que tiene que ver con el uso indebido del DNS. Ustedes pueden ver que todos los gTLD tienen al menos un nombre de dominio donde se registró un abuso. Hay distintos colores, lo pueden ver, como para ver cómo se informó en este caso este uso indebido y cómo

varió a través del tiempo. Obviamente el spam es el líder pero también vemos phishing, malware y botnets.

Dentro de OCTO, nosotros tomamos esta información que genera el DAAR y hacemos estos gráficos de burbujas. Si tuviéramos animación, ustedes van a ver cómo suben y bajan estas burbujas, cómo crecen y se achican, pero sí se ve ahora y es muy aburrido. Aquí muestra entonces que los dominios con phishing son los más importantes. En general son los dominios más grandes pero esta es una banda relativamente acotada.

También empezamos a ver que salen del reino de la estadística normal. Nuestra intención en el futuro es publicar los nombres para darle a la gente una idea de cuáles son los registros y los registradores que sufren más abuso que otros. Siguiente, por favor.

Claramente el spam es algo muy interesante, sobre todo varía con el tiempo. Ustedes pueden ver estas burbujas, cómo suben y bajan, y van de izquierda a derecha. Es muy interesante ver esto porque nos da información importante sobre lo que nosotros llamamos el flocking, aunar y pasar en manada de un registrador a otro. Esto es lo que pasa con la resolución de nombres entre los legados y los nuevos gTLD. Vemos que los legados tienen unos números conocidos. También pasa lo mismo en el caso de los nuevos gTLD en lo que es registraciones totales y abuso. Aquí

están los abusos de dominios que figuran en DAAR. Aquí vemos un aumento en el caso de los legados con el tiempo y una disminución en los nuevos gTLD.

Una de las cosas que tiene DAAR para alguien que está interesado en el uso indebido, les da una gran cantidad de datos para decir: ¿Qué es lo que está pasando aquí? ¿Qué es lo que entretiene realmente a mi equipo? No queremos que esta gente salga por la calle y haga cosas por las noches. Por eso nos concentramos en ver cómo prevenirlo.

Aquí tenemos estas estadísticas que nos muestran que hay una cantidad relativamente pequeña de dominios que son los que generan la mayor cantidad de abuso. Es algo que lo conocemos desde hace un tiempo pero DAAR nos está dando datos concretos de esto.

El estado del proyecto. Como mencioné, nosotros nos estamos concentrando en hacer algo bueno y no en hacerlo rápido. Como dije, tenemos también informes de los revisores, que son los que van a salir esta semana. Estamos ajustando los sistemas de recopilación de datos para generar unas actualizaciones que sean flexibles y oportunas. La idea es poder automatizar gran parte del informe para no tener mano de obra manual, hacerlo todo oportunamente. También estamos viendo cómo hacemos esta distribución granular de los datos que obtenemos. Estamos

experimentando con algunas medidas adicionales. Siguiente imagen, por favor.

Con esto termino. Hay un área que es la más desafiante en relación con el DAAR. Tiene que ver con la recopilación de la información sobre los registradores, que esa es una función del WHOIS. Ahora no estamos muy seguros o no confiamos demasiado con los datos vinculados con los registradores como para publicarlo en las primeras versiones. Posteriormente, quizá podamos hacerlo pero en realidad necesitamos pensar un poco exactamente sobre cómo podemos recopilar los datos de los registradores y que sean eficaces. Con esto termino. No sé si le doy la palabra a Fabien o si hay alguna pregunta, por favor.

CATHRIN BAUER-BULST: Muchas gracias por esta presentación, David. Realmente agradecemos cómo la ICANN está realizando este esfuerzo. Esta información para nosotros va a ser crucial, sobre todo lo que tiene que ver con el desarrollo de políticas porque pone bajo el microscopio cuáles son los problemas, la tensión que le tenemos que prestar en el desarrollo de políticas y tenemos que cambiar los procedimientos y tenemos que mejorarlos para poder tener una forma de combatir este tipo de abusos sistémico que se da. Nos gustaría escuchar qué es lo que habría que hacer antes de que esta iniciativa esté en posición de dar información pública

para decirnos dónde está el abuso, dónde está ese uso indebido respecto de determinados dominios, registros, registradores, etc.

DAVID CONRAD: Como mencioné, nuestro foco ahora antes de publicar los nombres vinculados con los datos que vemos es tener una revisión independiente por parte de un tercero para verificar que no estamos haciendo nada tonto con los datos para minimizas las posibilidades entonces de que existan informes falsos y que haya entonces una mala atribución de datos en lo que tiene que ver con el abuso del DNS y tratar de dar un nivel de confianza a la comunidad de que los datos que nosotros estamos brindando pueden utilizarse para tener información concreta basada en datos concretos para hacer un desarrollo de políticas.

Cuando los revisores independientes terminen su trabajo, como dije, uno ya va a terminar y el otro creo que en un par de semanas o un par de días, vamos a poder entonces presentar esos informes y vamos a comenzar con el proceso que está vinculado con la generación de los informes para publicarlos a la comunidad e indicar así cuáles son las estadísticas reales, dónde están los actores dentro de estas estadísticas.

LAUREEN KAPIN: Hablaron del rate limiting o limitación de la velocidad. No sé si entendí exactamente qué significa esto.

DAVID CONRAD: En los servicios de las redes puede haber una denegación de servicios para iniciar una recopilación de datos más rápido de lo que puede hacer ese sistema. Los operadores de las redes y los de servicio imponen una limitación para reducir la cantidad de conexiones que pueden ocurrir para evitar el uso indebido. En el contexto de los registros y los registradores, hay en realidad creo que todos tienen esta limitación a la velocidad porque entonces la gente no puede ir y buscar en todas las base de datos para buscar los contactos y generar entonces el spam u otro tipo de ataques. El efecto colateral es que los investigadores que están tratando de recopilar información para atribuir los nombres de dominio a los registradores significa que tenemos que enfrentarnos con estos límites en la cantidad de conexiones. A veces se pueden hacer nada más que cinco consultas por hora o algo así. Estos son los límites que se imponen.

Los fundamentos para estas limitaciones obviamente tienen que ver con algo razonable, con algo prudente para las operaciones de la red. Sería bueno que encontráramos la forma de que los investigadores reconocidos o acreditados estuvieran en una lista

sin estos impedimentos, sin estas limitaciones, pero estamos luchando con ellos por el momento.

CATHRIN BAUER-BULST: Muchísimas gracias, David. Quiero enfatizar el tema de la responsabilidad de los actores individuales porque creo que hubo un reclamo específico sobre un registrador específico que en términos diplomáticos estaba sujeto a una gran cantidad de abusos y entonces en el reclamo se decía que estaba basado en el informe DAAR y estábamos hablando de enero de 2017. Es decir, no se basaba en los datos más recientes. Ese es uno de los puntos donde los informes DAAR realmente van a tener valor porque van a dar información sobre un análisis continuo del abuso que además va a estar vinculado con actores específicos y va a permitir transparencia que esperamos pueda también suplementar los esfuerzos de cumplimiento contractual. Me parece que nos estamos quedando sin tiempo pero no sé si alguien tiene alguna otra pregunta antes de cerrar esta sesión.

LAUREEN KAPIN: Yo tengo una última pregunta. Supongo que ustedes saben que puede haber cambios en el sistema de WHOIS y lo que quiero saber es cómo estos cambios pueden afectar a la iniciativa DAAR.

DAVID CONRAD: El sistema DAAR en sí mismo no utiliza información de identificación personal. La única identificación y la única información que utiliza DAAR dentro de la ICANN o que es pertinente al informe del que estamos hablando es la del registrador y el nombre de dominio asociado. El resto de la información es útil cuando uno está tratando de profundizar y entender un ataque en particular, un vector en particular. Para los fines de generar el informe, la información del registrador es la única que nos preocupa en realidad. En la teoría, al menos, esa información debería estar disponible en el WHOIS público, sin ninguna limitación a su acceso. Nosotros sabemos que hay debates en este momento que tienen que ver con la decisión final sobre qué información va a estar disponible al público y cuál no pero esto todavía está ahí pendiente.

LAUREEN KAPIN: Muchísimas gracias. Gracias por todos los esfuerzos de la iniciativa. Sé además que va a ser beneficiosa para la comunidad y también sé que es mucho trabajo. Queremos agradecer todo esto. Vamos a cerrar la parte uno de este debate del PSWG que habló de nuestro plan de trabajo. Hicimos un foco en particular en una de las iniciativas que tiene la ICANN y que nos va a ayudar a darle más luz a todo este tema del abuso del DNS, ver también cuáles son las tendencias para que la comunidad incorpore estos

datos en el desarrollo de políticas. Estamos cerrando este tema entonces.

**[FIN DE LA TRANSCRIPCIÓN]**