ABU DABI – Sesión intercomunitaria: informe de uso indebido para la mitigación y creación de políticas
Lunes, 30 de octubre de 2017 – 13:30 a 15:00 GST
ICANN60 | Abu Dabi, Emiratos Árabes Unidos

IRANGA KAHANGAMA: Por favor tomen asiento. Vamos a comenzar con la sesión en breve.

Quiero agradecer a todos por su participación en esta sesión intercomunitaria qué es el informe de uso indebido para la mitigación efectiva y también para la creación de políticas sobre la base de hechos. mi nombre es Iranga. Yo soy miembro del grupo de trabajo de Seguridad Pública y estoy aquí con diferentes miembros.

CATHRIN BAUER-BULST: Mi nombre es Cathrin Bauer-Bulst. También soy miembro del grupo de trabajo.

IRANGA KAHANGAMA: Muchas gracias Catherine. lo que vamos a hacer es darle una breve presentación sobre la historia sobre este tema, y después Catherine hablará más sobre la logística y los detalles. Para grupo de trabajo de Seguridad Pública y su perspectiva es la evolución natural del uso indebido del DNS y la mitigación de

este uso indebido que tratamos de mitigar para la comunidad de la ICANN.

Esto incluye asesoramiento sobre cuestiones de uso indebido y también otros debates que hemos tenido. Cuándo se hizo la convocatoria esta sesión intercomunitaria nos pareció muy interesante y pensamos que sería muy interesante para la comunidad hablar sobre este tema y seguir avanzando sobre cómo abordar estas cuestiones. Para darles una breve introducción al tema tenemos tres llamadas del grupo de trabajo, convocatorias, al grupo de trabajo de diferentes unidades constitutivas, representantes que ven aquí en esta mesa. El grupo de trabajo de Seguridad Pública establece una serie de principios relacionados con la mitigación del uso indebido del DNS.

Y luego de proponer algunos resultó obvio que había diferentes perspectivas sobre el tema. Entonces el resultado natural de esto derivo en tener que debatir el tema y dividirlo en una subsección, y además lo que hicimos fue compilar esta información y dividir el uso indebido del DNS y su mitigación en tres categorías diferentes. Esta es la mitigación del uso indebido del DNS, el informe del uso indebido del DNS y las estadísticas sobre cómo se debe utilizar esta información. Hay diferentes temas y vamos a tener un enfoque basado en los principios, y la

idea es seguir participando en el grupo de trabajo de Seguridad Pública.

CATHRIN BAUER-BULST: Vamos a pasar entonces a la próxima de a positiva. En primer lugar, vamos a tener dos presentaciones breves por parte de David Conrad y Drew. Estos son representantes de los diferentes grupos participantes, de los diferentes grupos que también han contribuido la organización de esta sesión y a la preparación del material. Tenemos a Iranga; tenemos a Tania Tropina de la unidad constitutiva no comercial; tenemos a Denise Michel de la unidad constitutiva comercial; Jonathan Matkowsky de la unidad constitutiva de propiedad intelectual; a Rod Rasmussen del SSAC; Jamie Hedlund, quien es el VP para protecciones del consumidor y cumplimiento de la ICANN; y también a [incomprensible].

Como decía anteriormente, decidimos estructura este debate. y vamos a comenzar con dos presentaciones breves, y luego vamos a pasar a debatir estas tres categorías que ya hemos identificado. Lo que surgió en las llamadas y en el debate de los principios fue que no podíamos estar de acuerdo sobre qué principios se tendrían que aplicar en el informe del uso indebido del DNS y de qué manera se van a utilizar con posterioridad. Quedó claro que los principios que se aplicarían a este proceso

tendrían que responder a 3 preguntas clave. Y estas son las preguntas clave que ustedes ven en la diapositiva y que vamos a abordar luego, vez que finalicemos con las presentaciones.

Las preguntas son: En primer lugar, cómo identificamos el uso indebido del DNS de una manera confiable. y sobre esta base, cómo creamos un informe del uso indebido que sea transparente y efectivo y que permite tener datos disponibles. Y, en tercer lugar, cómo vamos a utilizar toda esta información. Estas son las tres secciones que esperamos tener y debatir con ustedes el día de hoy.

Tenemos un panel muy amplio con muchos expertos renombrados en la cuestión, así que queremos incluirlos a ustedes, y queremos que estás en una sesión participativa. Así que nosotros vamos a hacer lo siguiente. Vamos a dar las presentaciones que sean breves y luego vamos a abrir la sesión de preguntas y respuestas con una pregunta para los panelistas. Mientras respondemos esa pregunta los queremos invitar a ustedes aquí se expresen sobre las preguntas en general que se han planteado para estas categorías o que hagan comentarios sobre las preguntas específicas. Les quiero pedir que se presenten. El personal de la ICANN está dando vueltas con micrófonos así que si quieren tomar la palabra levanten la mano y el asistente de sala se acercará y les entregara el micrófono. A

fin de dar la mayor cantidad de oportunidades para que tomen la palabra, vamos a limitar el tiempo a 2 minutos para cada intervención. Así que en el panel queremos ser lo más equitativos posible, por lo tanto, hagan sus intervenciones de manera breve.

Ahora sin más vamos a pasar a la presentación. Nos vamos a focalizar en sistema de informe de actividad de uso indebido de los nombres de dominio.

DAVID CONRAD: Soy David Conrad. Soy el CTO de la ICANN. Lo importante para este debate es que hemos desarrollado un sistema de informe de actividad de uso indebido de los nombres de dominio con mi equipo.

Para contarles un poco de contexto, que es este sistema de informe de actividad de uso indebido de nombres de dominio o DAAR, como preferimos llamarlo porque es mucho más corto. Es un sistema que nos permite informar las registraciones de los nombres de dominio y el uso indebido en los registros y registradores. Ahora se focaliza en los gTLD porque es allí donde conectamos los datos y dónde estamos realizando los análisis, pero también los ccTLD si quisieran participar los podemos debatir con ellos también.

Cómo funciona o cuál es la diferencia de este DAAR con respecto a otros sistemas de reporte o de informe. Como ustedes saben hay muchos mecanismos de informe que están dando vueltas. Muchos de ellos están asociados con productos comerciales o servicios comerciales. Lo que estamos haciendo es estudiar todos los registros gTLD y registradores de los cuales podemos recolectar información y hemos hecho muchos análisis. Tenemos varias fuentes de datos. Estos son feeds de reputación, también listas de bloqueo, entre otras cosas. También recabamos información durante un tiempo a fin de mantener suficiente información que permita realizar estudios históricos. En realidad, se nos pide analizar una serie de amenazas. Las amenazas en las que nos focalizamos están identificadas en el comunicado del GAC, y esto incluye el pishing, botnet y la distribución de malware. También de forma controvertida hemos incluido el spam en nuestro estudio. Lo hemos incluido porque es un vector altamente efectivo para otras formas de uso indebido y también hemos brindado un índice en relaciones de información porque cuando un TLD resulta impactado o afectado por el malware de una forma u otra también va a ser impactado por el spam o correo indeseado.

Estos son los puntos principales. Lo que intentamos hacer es darle un enfoque científico, ser transparentes y poder reproducir

esta información tanto como sea posible. La génesis del proceso DAAR en realidad se llevó a cabo por un proveedor de hardware de seguridad para una serie de gTLD y algunos de estos informes eran numerosos y graciosos porque están relacionados en un 100% al spam y en realidad tenían que ver con un solo nombre de dominio. Porque aparentemente este nombre de dominio parecía reunir una gran cantidad de cuestiones de seguridad. Esto dio como resultado que otros nombres de dominio dentro de este dominio de alto nivel fueran clasificados con maliciosos. Cuando esto salió a la luz se generaron una serie de preguntas, y la ICANN y la comunidad en general, y algunas personas dentro de la comunidad, se dirigieron a mí, a la ICANN, y nos dijeron que alguien tenía que tener una lista que fuera autoritativa, tendría que hacer una lista y tener una metodología bien documentada con la que todos estuviesen de acuerdo para no crear un informe que estuviese sesgado o que estuviese plagado de intereses comerciales. Entonces estás fueron las ideas iniciales que dieron origen al DAAR.

Siguiente diapositiva. Otra vez tengo que tomar la palabra yo.

Imaginen que el DAAR es un conjunto de datos. Nosotros recabamos la misma información sobre uso indebido que se le reporta la industria de los usuarios de Internet. Uno de los requisitos clave es que todo lo que se haga dentro del proyecto

se tiene que hacer de manera reproducible. Nosotros no confiamos en ningún dato confidente. No generamos datos per se nosotros mismos, sino que básicamente lo que hacemos es tomar datos que están públicamente disponibles y generamos grandes hojas de cálculo con toda esta información para documentar el uso indebido en diferentes formas y en varias categorías.

Los datos en materia de uso indebido que recabamos es utilizado por los sistemas de seguridad que protegen millones de usuarios y miles de millones de casillas de correo electrónicos en forma de área por la industria y por la academia. Ellos están haciendo utilización de esta información y de estos conjuntos de datos los estudios académicos y la industria en validado estos conjuntos de datos porque son exactos, tiene una cobertura global, son confiables y tienen una baja tasa de falsos positivos.

Tenemos un marco de trabajo que es extensible. Estamos experimentando con una serie de análisis para poder entender mejor que es lo que está realmente sucediendo. El punto principal aquí es que el DAAR es una herramienta que permite a la comunidad de la ICANN determinar de qué manera el sistema de nombres de dominio se percibe fuera de nuestra comunidad.

Diría próxima diapositiva, pero nadie me va a escuchar y lo voy a tener que hacer yo mismo. Bien, acabamos.

Surgió la pregunta sobre los criterios para estos conjuntos de datos. en esta diapositiva se me los criterios que estamos utilizando en la versión actual del sistema DAAR. Una de las actividades que se están llevando a cabo es requerir del SSAC sus aportes sobre los criterios, mediante los cuales se va a seleccionar el feed para crear el DAAR. También actualmente nos encontramos desarrollando un RFP para la comunidad. Perdón, para los expertos independientes. Para que brinden aportes sobre nuestra metodología. Una vez que recibamos esta información, lo que haremos es redactar un documento que reescriba la metodología propuesta para ustedes. Lo vamos a someter a comentario público, y luego lo enviaremos al proceso normal de la ICANN y modificaremos los feeds de datos según los criterios y según los aportes recibidos. Por el momento los conjuntos de datos que utilizamos y los requisitos son las comunidades operativas y de seguridad confían en estos conjuntos de datos en relación a la exactitud y a la claridad del proceso. Los conjuntos de datos en este caso tienen un proceso muy claro con respecto a qué nombre se agrega o se elimina. Las listas de bloqueo que se eligen brindar una clasificación de las amenazas. Por ejemplo, si son botnets, si se trata de

distribución de malware, de phising, de spam. los principales. Estos son en realidad probablemente adoptados por la comunidad de seguridad operativa, y estos feeds también son incorporados en la seguridad comercial, en los sistemas de seguridad comercial, porque son utilizados por los operadores de red para proteger a los usuarios. También son utilizados por los proveedores de servicio electrónico para proteger sus casillas de correo electrónico.

En cuanto estas listas de bloqueo de reputación, están en todos lados. Están en los buscadores, en las nubes, en los sistemas de servidores, en las herramientas para redes sociales. Son muy frecuentes dentro del DNS. En Copenhague tuvimos una presentación con el exequipo de expertos técnicos. Ellos desarrollaron un software que utiliza algo que se denomina un software de desarrollo, dónde tienen zonas de política de respuesta, y esto permite a ciertos proveedores de servicios que están bloqueando los nombres de dominio porque estos nombres de dominios están representando o duplicando a nombres de dominios maliciosos. Además, los operadores de redes privadas tienen firewalls comerciales, también tienen sistemas de mensajería y proveedores de correo electrónico.

Perdón, pero me estoy excediendo. Dentro del sistema DAAR, básicamente tenemos siete RBL y hay algunos que tienen otros.

¿Por qué comenzamos a informar los nombres de dominio con spam? Esa pregunta ya surgió previamente. El comunicado de Hyderabad el GAC expresó su interés en el spam o correo indeseado. Básicamente el spam es un medio principal para otro tipo de amenazas. Se midieron los nombres de dominios que tenían spam y no los nombres de dominios que eran spam.

Ahora le voy a dar la palabra a Cathrin o alguien.

CATHRIN BAUER-BULST: Drew, usted.

DREW BAGLEY: Gracias, Cathrin. Soy Drew Bagley. Soy miembro de CrowdStrike, el departamento de Secure Domain Foundation.

Ya hablaron de la confiabilidad de este tipo de datos y yo voy a contar de qué manera podemos utilizar estos datos básicamente a nivel operativo para bloquear los TLD, en lugar de informar de políticas que puedan mejorar estos esfuerzos y que no vayan en contra de la aceptación universal, que es lo que sucede cuando aparece el uso indebido. Como Dave mencionó, no hay consenso en la comunidad con respecto al uso indebido. Básicamente hay dos: el phising y el malware. Y también hay consenso con respecto a los mecanismos que se utilizan para

llevarlo adelante. Es importante que la comunidad entienda que cuando se habla del uso indebido en relación a la política, no siempre se pueden tener en cuenta todas las diferentes interpretaciones sobre el tema. Es importante que la comunidad comencé a trabajar en cuestiones de política donde si existe el consenso y donde haya métricas que sean medibles. Como Dave describió, existen muchas métricas medibles en relación al malware, al pishing, al spam y también al control de los botnets.

Como parte de la tarea del equipo de revisión de confianza, competencia y elección de los consumidores, analizamos este problema y la idea es evitar el uso indebido en los nuevos GTLD. Para medir esto, lo que hicimos fue tener en cuenta el pishing, el malware y el spam, y encomendamos la realización de un estudio para analizar estos datos y existen listas de bloqueo para poder llevar adelante las recomendaciones de políticas. Yo utilizo esto como un ejemplo ilustrativo para mostrar de qué manera los datos se pueden utilizar y aplicar en la creación de políticas dentro de la comunidad. Lo que hallamos como resultado de un análisis que duró un año fue que en realidad el uso indebido es algo que no era completamente universal en todos los TLD y tampoco era el azar. Pudimos identificar factores que tenían más probabilidad de estar relacionados con un incremento del uso indebido en una zona o con un

registrador particular o un uso indebido bajo en relación a ciertos operadores de registro o registradores. Por lo tanto, no es sorprendente que haya un incremento en las restricciones para la registración y que haya una baja tasa de uso indebido. De igual manera, los registradores o los operadores de registro tienden a tener una mayor correlación con el alto nivel de uso indebido y también se encontró que tienen ofertas a muy bajo precio y registro acciones u opciones de registración a granel, de las cuales voy a hablar en breve.

También hicimos un análisis a un nivel micro y vimos que había una fuerte correlación entre los términos relacionados con marcas que se utilizaban en las campañas del pishing, lo cual no nos sorprende, y en este informe señalamos particularmente 76 nombres de dominios que utilizaban marcas relacionadas con Apple, como por ejemplo iPhone, y que trataban de hacer una campaña de pishing para captar usuarios. Estos 76 nombres de dominio comprendían unas 83 instancias de uso indebido. Lo que los datos nos mostraron es que hay una brecha en la política. Esto es importante a tener en cuenta y es lo que está haciendo el proyecto DAAR y otras personas a la comunidad de tratar de compilar todos estos conjuntos de datos para poder confiar en esta información porque allí se puede ver dónde existen los mecanismos y si estos mecanismos pueden no

resolver todas las situaciones que se presentan y que pueden afectar la estabilidad y la flexibilidad del DNS.

Quiero destacar dos registradores en particular que son muy problemáticos con el conjunto de herramientas y que deberían ser informados en la política que se está realizando. El primero es un registrador qué fue suspendido pero que pudo operar durante la mayor parte del año 2016 con un alto nivel de uso indebido. En realidad, no era el nivel de uso indebido por lo cual se le suspendió finalmente. Ellos dejaron de pagar las cuentas, y por lo tanto si uno cómete ciberdelito, en realidad tiene que seguir pagando las obligaciones, de esta manera puede seguir operando. Entonces lo importante aquí es que en un modelo de reclamo, donde tenemos un enfoque reactivo hacia el enfoque del uso indebido del DNS, surgían muchos reclamos y no era posible hacer nada para defender a la comunidad. Lo que hicimos entonces fue tomar en cuenta estos conjuntos de datos amplios y tener esta iniciativa del sistema DAAR para poder hacer algo al respecto, en lugar de siempre que darlos a esperar a que surjan estas violaciones específicas y que sean realmente afectadas. tiene la palabra ahora.

Este es el segundo registrador, AlpNames, que sigue operando del mismo modo con altos niveles de uso indebido. y también para cuándo se hizo la investigación del CCT este registrador

ofrecía registraciones a granel en las cuales un registro atar yo podía tomar nombres y registrar dos mil nombres a la vez, y esos nombres convenientemente creaban un algoritmo de registración de dominios a disposición de los usuarios. O sea que se podía aleatoriamente generar muchísimos nombres, 2000 nombres de dominio, para usuarios legítimos que tenían usos legítimos. No es de sorprender que aquí hubo alto nivel de uso indebido, pero sin existir reclamos jurídicos accionables no se lo sometió a un proceso de suspensión. con estos datos a granel se presenta una brecha de política potencial para la comunidad. Me sigo equivocando de botón o quizás inconscientemente quiero que quede claro que son solamente estos dos registradores.

Como ejemplo, el equipo del CCT utilizamos estos datos para elaborar recomendaciones específicas de política para la comunidad y redactar el capítulo de uso indebido del DNS que se desarrollará la semana próxima aproximadamente. En el equipo de revisión, a diferencia de la comunidad, tenemos más datos disponibles que ponemos a disposición de la comunidad a través del DAAR o bien a través de los miembros de las comunidades de ciberseguridad como APWG, la fundación de dominios seguros y otros miembros que presentan los datos. Nosotros como comunidad no debemos utilizar solo las

operaciones para bloquear las cosas, sino para implementar decisiones de política que aborden estas brechas y asegurarnos de que podemos dejar atrás el modelo reactivo y pasar a ser proactivos en el modelo en el cual los operaciones de registros y los registradores las dificulten la situación a los delincuentes para seguir haciendo uso indebido de los servicios, y también usar los datos para medir el progreso y ver si efectivamente estamos mitigando el uso indebido de manera holística.

Espero que el panel de hoy permite a discutir el tema desde distintos puntos de porque no cabe duda de que esto afecta a varias áreas de la comunidad y queremos hacerlo bien desde el comienzo. y también usar datos realistas y accionables, un esfuerzo que debemos abrazar para generar políticas para tener un mejor DNS para todos. Con esto le devuelvo la palabra a Cathrin.

IRANGA KAHANGAMA: Gracias. Quiero recordarles que hay un límite máximo de 2 minutos. estamos un ratito atrasados, pero quiero garantizar que haya plena participación. Vamos a comenzar la discusión con los panelistas, así que si alguien en el público quiere tomar el micrófono vamos a comenzar. Voy a comenzar con Alan, si no le importa comenzar. Vamos a empezar, por así decir, con el primer eslabón de la cadena.

Cuando hay un abusador claro, obvio, ¿qué herramientas tiene el registro para que estas tendencias observadas no se repitan?

ALAN WOODS: Alan Woods, de Donuts registry. Para ir directo a la pregunta, usted dice abusador obvio. Eso me preocupa de entrada. Yo veo los datos y veo datos que vienen de fuentes como DAAR y otras que nos dan listas fantásticas de cosas que pueden ser abusivas potencialmente. No obstante, no estamos en una posición de decir que es un abusador obvio porque lamentablemente no tenemos la prueba subyacente que nos permita escalar esto a una acción o a la parte que corresponda o al registro. Entonces la primera pregunta que tenemos que hacernos es de qué manera podemos determinar qué es una situación de uso indebido obvia. Obviamente cuando recibimos información, cuando tengamos la prueba, la utilizaremos para realizar una revisión objetiva y lo escalaremos a la parte que corresponda, que probablemente sea el registro del registrador. Ahora si el Registrador no toma una acción con el registro directamente, nosotros vamos a considerar intervenir.

En este momento las herramientas disponibles son los indicadores que recibimos de terceros. Además, nosotros mismos debemos identificar información por nuestra cuenta para cerrar esta brecha.

IRANGA KAHANGAMA: Gracias, Alan. Entonces ¿usted diría que como mínimo las estadísticas alcanzan para apuntar a algo que requiere por lo menos una investigación adicional de parte del registro?

ALAN WOODS: Sí. Y para añadir a la controversia, que sí que eso nos apuntaría esa dirección, pero muchas veces la única prueba que podemos encontrar es el hecho de que esté listado en la lista negra. A nosotros nos gustaría tener más detalles o tener estos puntos adicionales para saber por qué se les puso en la lista negra, más allá de tener solo una declaración de que está en la lista negra. Para nosotros es difícil, lo hacemos lo mejor que podemos en estos casos. Si vemos un indicador de alerta intentamos identificar la razón de esa indicación, pero no siempre es claro. Es difícil obtener esa información, en especial de los proveedores de listas negras que no dan esa información, o bien porque no pueden o porque no la tienen no porque son secretas de la industria.

CATHRIN BAUER-BULST: ¿Algún comentario?

DAVID CONRAD: Uno de los motivos por el cual el DAAR incluye información histórica es para ayudar a identificar tendencias a lo largo de largos periodos de tiempo, incluyendo información de uso indebido a través de largos periodos de tiempo. Estoy de acuerdo de que el concepto de uso indebido obvio depende de cada uno y su objetivo, pero sí tenemos que identificar qué es un uso indebido cierto, genuino, versus tener versiones aleatorias. en nuestro trabajo queremos facilitar a la comunidad información sobre periodos prolongados para permitir el debate sobre políticas que ayuden a identificar con claridad tendencias de uso indebido en espacios de nombres particulares.

IRANGA KAHANGAMA: Ahora tenemos a Rod [incomprensible].

ROD RASMUSSEN: Voy a hablar a título personal, no representando al SSAC. Voy a responder directamente a esta pregunta. Creo que la respuesta que oímos es la respuesta de qué manera una entidad particular identifica el uso indebido de manera confiable. Eso requiere confianza en la política. Esta industria existe desde hace 10 o 15 años y ha elaborado un método extremadamente confiable para identificar usos indebidos de manera sistémica. Eso tiene que ver con dos cosas: Internet Explorer, el browsing de Google,

Google Safe Browsing. Estas son herramientas que son automáticas hoy día y funcionan de manera automatizada en segundos. La parte de identificación de tecnología es muy confiable. Hay muchas maneras de determinar los falsos positivos en las listas. O sea, la tecnología existe. La clave es cómo transformar esa información en acción, y eso requiere contratos, confianza y otras cosas que hay que configurar en torno a un marco para que la gente pueda accionar ya sea a través del registro del registrador del proveedor de email o del proveedor de software web. Es un problema que debe resolverse desde el lado de la tecnología, no necesariamente del lado de la política. Gracias.

IRANGA KAHANGAMA: Abrimos ahora el micrófono.

DAVE PISCITELLO: No me gusta la frase de abusador obvio. No es algo que nosotros medimos en DAAR. Lo que medimos en DAAR son las amenazas en la seguridad basándonos en las listas de reputación, estás de bloqueo de lo que nosotros percibimos como uso indebido, y creo que eso es claramente distinto de la obligación que el registro o el registrador o la compañía de hosting del DNS o el ISP tendrá que evaluar la información, lo que se le presenta,

hacer una investigación y corroborar el reclamo. Si yo estuviera en esa posición, activamente iría a buscar el mail que contiene la URL y el adjunto que contiene el URL, ir al sitio, haría una acción benigna, un WebGet o curl. Hay muchos procedimientos que se esperan como parte de la diligencia debida del registro o registrador. No quiero decir que esto tiene costo cero, pero el DAAR no se presume como el lugar donde uno puede encontrar todas las respuestas. El DAAR se presume como una herramienta, un mecanismo para todo el espacio de nombres de dominio, para todo el paisaje de usos indebidos y amenazas al uso indebido y ver casos dónde hay buenas políticas, donde faltan políticas y ver cómo crear una síntesis.

CATHRIN BAUER-BULST: Gracias, Dave. Graeme, pasemos a los registradores.

Hemos hablado de los distintos indicadores. Tenemos el dar que constituye una base de evaluación. Nos han dicho que hay más cosas que hacer del lado del registro y el Registrador para que esta información se convierta en una herramienta accionable que permite iniciar acciones contra quienes no cumplen con nuestros términos y condiciones. Eso nos lleva a pensar en esos términos y condiciones, y qué es lo que ustedes tienen que hacer para que sean accionables, para poder tomar medidas de

cumplimiento de la política. Le pediría entonces que se refiriera esto brevemente.

GRAEME BUNTON: Graeme Bunton, de Tucows. Gracias, Cathrin.

Hay un par de conceptos interesantes aquí. Alan plantea un punto interesante. Como ustedes dicen, vincular las listas de bloqueo con una prueba concreta que sea accionable no es algo trivial. Lo que decía Dave, entiendo que los métodos que se pueden usar para combatir el uso indebido en la plataforma presuponen cierto nivel de sofisticación del personal de monitoreo de uso indebido de primera línea, que la verdad no está disponible en todos los registradores del planeta, en especial cuando uno quiere optimizar la producción y reducir el uso indebido. No es algo que necesariamente algo que uno tenga demasiado tiempo para investigar.

Quería referirme a otra cosa. Hemos visto nombres de dominio generados algorítmica mente varias veces, pero no son siempre los malos. Ha habido varios casos que existen y que operan empresas válidas. Es excepcionalmente difícil hacer un rastreo de los malos actores repetitivos basándonos en las colas de acciones de abuso de un uso indebido y como se monitorea. Es algo que somos conscientes y que nos interesa porque reduciría

el uso indebido de nuestra plataforma y nos interesaría hacer, requiere una visión muy amplia, que significa ir a las colas de uso indebido, entrar a las colas de uso indebido, y eso no es fácil de hacer.

CATHRIN BAUER-BULST: Gracias, Graeme.

ALAN WOODS: En relación con lo que decía Dave Piscitello, algo muy importante es que DAAR es un proyecto que muestra estadística, pero hago que hay que hacer entre DAAR y la acción es que es lo que tienen que hacer los registradores y los registros. gracias, Dave, por ese comentario, por recurrir a la otra parte correspondiente.

IRANGA KAHANGAMA: Gracias, Alan. Para entrar a un área más específica, ya vimos que queda mucho por hacer. ¿Qué son los datos que se necesitan para impulsar estas secciones?

ROD RASMUSSEN: Hay muchas metodologías que dependen del tipo de uso indebido. Hay cosas que son fáciles de detectar como las que son generadas por los algoritmos de generación de dominio. Un ejemplo es algo que se usa en malware para crear series de nombres de dominio que podrían potencialmente registrarse en el futuro. Esa ingeniería reversa del malware se puede ver la registración de los dominios y actuar en consecuencia. Esa es una vía de trabajo.

El spam es un camino obvio que ya se trabaja hace 10 o 20 años o 15 años. Es un análisis rudimentario. Hay distintas plataformas, Facebook, las redes sociales. Todas ellas usan los programas de email, utilizan los límites de contenidos que utilizan los usuarios, primero a nivel general y después se individualizan los dominios. A partir de ahí se puede hacer algo con esa información para correlacionar con metadatos que vienen a través de consultas del whois, del DNS o de la propia base de datos de objetos conocidos o desconocidos. Hay varias distintas formas de hacerlo o fórmulas. Hay herramientas adjuntas a los browsers, hay dispositivos de seguridad de red que analizan los flujos de datos entrantes y salientes, las redes, y correlacionan. Hay algoritmos sofisticados que permiten encontrar cosas como tunneling y otras actividades que monitorean la red. Son muchas las tecnologías que pueden

unirse para formar listas de las distintas áreas de uso indebido posible.

IRANGA KAHANGAMA: Gracias. Buena sincronización. Entiendo que la diversidad de los datos disponibles es un aspecto clave aquí. ¿Tenemos una pregunta remota? Vamos a tomar las preguntas remotas más adelante. Cathrin, la siguiente pregunta.

CATHRIN BAUER-BULST: Quisiera volver a los distintos tipos de datos que necesitamos para informar de la elaboración de políticas. Cómo escuchamos en la presentación elocuente de nuestro colega sobre las tendencias y los desarrollos que informan en la elaboración de políticas, por un lado, y de ahí los datos más específicos que los registros y registradores necesitan para tomar acciones específicas en casos específicos. Eso requiere pruebas, no solo investigación criminal sino también algo que se ve influenciado por los términos y referencias de cada proveedor individual. Quizás Denise por su experiencia específica en la definición de estándares para la comunidad y los clientes puede contarnos si hay lecciones que aprender sobre la reacción de condiciones para tener una reacción, una acción eficiente a las amenazas o el uso indebido.

DENISE MICHEL: Tenemos un amplio sistema global de seguridad y mitigación del uso indebido en todas plataformas, que es monitoreado de manera continua y es actualizado. Coordinamos de manera global a través de las industrias y los sectores para compartir mejores prácticas, términos de servicio, tendencias, y también compartimos datos de seguridad.

Si analizamos el contraste entre lo que hicieron los registradores y los registros, un elemento que todavía no se ha estudiado son los incentivos y la voluntad para hacerlo. La unidad constitutiva comercial público muchos comentarios sobre el estudio de uso indebido que hizo el equipo de revisión de la CCT y ofreció maneras muy específicas por las cuales puede usarse este estudio como punto de partida para incrementar la capacidad de mitigar el uso indebido de manera colectiva y mejorar las cosas en general, tales como vincular los incentivos con las buenas prácticas para el manejo del uso indebido, analizar los feeds o las cargas que tienen que pagar los registros y lo registratarios, las mejores prácticas y los resultados. Este es el primer estudio de uso indebido. Nosotros lo hacemos de manera constante y nos permite tener datos rigurosos de tendencias que son accionables en lo que hace al escrutinio de cumplimiento de los registros y las tasas de uso indebido de

cada uno. son muchas cosas que pueden hacerse para tomar medidas accionables. y cuanto antes podamos hacer funcionar la iniciativa de open data y lo antes que podamos tener la herramienta de reporte DAAR, mejor.

CATHRIN BAUER-BULST: Vamos a darle la palabra a la primera oradora.

REG LEVY: Gracias. Soy representante de Tucows. Quisiera mencionar algo que se dijo recientemente sobre las condiciones. Es real que muchos de nosotros a veces somos sacados sin ninguna razón y sin hacer ningún tipo de monitoreo. Quizás esto sea porque no hemos decidido algo antes o porque necesariamente eso es algo necesario en el momento. Quizás haya que hacer algo, pero esto no siempre se puede hacer cumplir dentro de nuestro ámbito.

CATHRIN BAUER-BULST: Vamos a pasar a esa pregunta en un momento, pero antes quiero hacer una pregunta de Jonathan sobre los indicadores. Rod dijo que había ciertos tipos de uso indebido que se analizaron y que había varios vehículos. Se identificó al spam. Y otro vehículo fue que a veces había infracciones de la propiedad intelectual que podrían interferir o ser indicadores del uso

indebido. ¿Podría por favor hablar sobre estos indicadores para poder identificar el uso indebido?

JONATHAN MATKOWSKY: Soy miembro del IPC, pero voy a hablar en mi propia representación.

En primer lugar, en cuanto a los registradores y sus obligaciones, según el acuerdo de acreditación de registradores para responder a un reclamo de uso indebido y hacer la investigación adecuada este es un beneficio para la comunidad, así que yo estaría todos a que tomen el beneficio y que utilicen esta oportunidad para garantizar o asegurarse de que la comunidad esté protegida del uso indebido, y esto incluye todas las actividades ilegales. Podemos estar de acuerdo en que el pishing, qué es la toma de información personal, tiene correlación con el contenido. El informe habla de por ejemplo el [incomprensible] y de los dominios utilizados maliciosamente o de diferentes formas en que el contenido una propiedad intelectual pueden ser sujetos de amenazas de uso indebido, especial donde hay amenazas complejas, quizás donde existe más de una ubicación o una localidad. A veces cuando se descargan cierto software, se puede descargar malware en las computadoras. Entonces los operadores de registros no siempre tienen visibilidad con estos registradores que no responden a

los reclamos, así que es necesario que se les notifique cuando un registrador no cumple con sus obligaciones. Esta información será incluida en el análisis técnico y estadístico del conjunto de datos que se informa en la ICANN. y la ICANN puede pedirlo en cualquier momento, así que yo diría que el estudio de DAAR o el proyecto DAAR debería utilizarse de manera interna.

Yo instaría al equipo de cumplimiento de la ICANN que la utilice en forma interna. Si se analizan algunos de los conjuntos de datos que yo vi en el informe podrán ver que incluso aunque hay pocos informes de reclamos planteados, se habla del volumen de los reclamos por uso indebido. Así que se puede ver qué es lo que sucedió. Por ejemplo, ver el informe y saber que sucedió en el 2013 en la ICANN.

IRANGA KAHANGAMA: Muchas gracias, Jonathan. Vamos a pasar a la siguiente diapositiva. Es como crear un sistema de informe para el uso indebido que sea transparente y efectivo. Para esto le voy a dar la palabra a Tatiana. David en su presentación mencionó diferentes instancias en las cuales las listas de bloqueo se pueden utilizar en los diferentes buscadores y en los correos electrónicos. Mi pregunta es: ¿cuál es el interés de los usuarios finales con respecto a estas herramientas de análisis? Y si el uso estadístico del análisis del DNS puede ser efectivo y se puede

utilizar para evitar que esto afecte a los intereses potenciales de los usuarios.

TATIANA TROPINA: Quiero aclarar una confusión. No estamos representando a los usuarios finales sino los usuarios no comerciales. Esto es una importante diferencia porque los usuarios finales pueden ser tantos comerciales como no comerciales. pero lo que yo quiero decir es lo siguiente. Tenemos una posición sobre el informe de uso indebido y sus herramientas y el sistema de informe de uso indebido. Quiero fastidiar que somos la NCUC. No estamos recabando estadística, no estamos suspendiendo sitios web. Lo que nosotros hacemos es, independientemente de la herramienta que se utiliza, desde mi punto de vista personal puedo decir que yo me focalizo en la estadística. Estoy a favor de compartir la información entre las industrias. Pero aquí en la ICANN nosotros tenemos una línea clara entra en el lado técnico del uso indebido del DNS en relación a la misión de la ICANN.

El uso indebido solo se refiere al contenido porque no todo lo que es ilegal según la ley aplicable sería considerado un uso indebido del DNS desde el punto de vista técnico. la ICANN y las herramientas que utiliza la ICANN tienen que estar relacionadas con la misión de la ICANN. Sé que alguien puede por ejemplo presentar el RAA, pero el RAA data del 2013 y nosotros tenemos

una misión de la ICANN que fue establecida durante el periodo de transición.

En segundo lugar, tenemos que ser cuidadosos con respecto a los enfoques preventivos. Tenemos que actuar y redactar y también prevenir golpes aquí. ¿qué es lo que significa prevenir? Cuando los actores en la industria tienen que accionar qué significa prevenir. Y en eso también tenemos que ser claros. Dije que tenemos que tener una definición acotada de lo que es el uso indebido del DNS. Y en representación de los usuarios no comerciales, no tenemos que olvidar que primero qué tiene que ver con el uso indebido no es suspender el dominio sino atrapar a aquellos que están violando la ley y que realmente comete en el uso indebido. Esto es cuestión de cumplimiento de la ley. No queremos intermediarios o que la industria actúe como una policía de contenido o que tenga poder de policía en algún sentido porque a veces nos asusta esta cuestión de que la industria debe ser la policía. La industria no debe ser la policía. gracias.

CATHRIN BAUER-BULST: Gracias, Tatiana. Le voy a dar la palabra ahora a Drew. Desde el punto vista de investigador en relación al uso indebido, ¿de qué manera estos conjuntos de datos se pueden publicar para ser

útiles? ¿cuál sería la frecuencia necesaria para que fueran útiles para la comunidad?

DREW BAGLEY: En el estudio al que me refería anteriormente del CCT, creo que es importante que sepamos que esto no es algo que aparece cada 5 años o que hay un equipo de revisión que lo analiza cada 5 años. Creo que si el DAAR produce datos estadísticos transparentes, esto lo podemos tener como conjunto de datos continuos, de manera que sea muy útil y con esto se puede hacer análisis periódicos con respecto a qué significan estos datos. Esa información puede estar disponible para la comunidad y quizás hay análisis más abarcativo, como por ejemplo los que hizo el equipo del CCT porque fue muy importante para nosotros comprender dónde están las cuestiones, las campañas de phishing y otras campañas maliciosas pueden esconderse en ciertos lugares. Entonces es importante tener una evaluación continua para que esté información llegue a la comunidad.

A mí me gustaría responder un poco a lo que dijo Tatiana. Porque Tatiana hizo comentarios muy importantes y que reflejan la diversidad de la comunidad y la diversidad de puntos de vista en este tema, así que creo que es muy importante. Yo enfaticé una de mis primeras diapositivas que en lugar de pasar

años debatiendo el tema algo puede ser considerado indebido en un país y en otro no. Creo que es importante que como unidad comencemos a enfocarnos en lo que ya tenemos consensuado y ver cuáles son las conductas que van a ser prohibitivas y los acuerdos. Son cosas muy tácticas. en lugar de perdernos en el bosque, creo que es importante que trabajemos en este sentido. Tatiana lo mencionó. También pienso que Alan mencionó algo muy importante sobre cuán importante es esto de ser reactivos. Esto requiere evidencia y como mencionó Tatiana también esto tiene que ver con el cumplimiento de la ley. Hay una diferencia entre suspender a alguien e identificar quién es el abusador o el delincuente.

Si hay algo que es suspicaz o que despierta sospecha cuando un nombre de dominio pasa estar en línea quizás hay algo para hacer ahí y eso se tenga que tener en cuenta con los diferentes proveedores.

DAVID CONRAD: Quiero hablar sobre la publicación de los datos en el sistema DAAR. Esto genera un informe mensual. Las estadísticas que vemos están divididas o clasificadas en registros y registradores. El plan es que esta información esté disponible para la iniciativa de datos abiertos a lo largo del tiempo para que la gente pueda hacer un análisis de tendencia histórico sobre la base de la

información que estamos recabando. Es un plan tentativo. En realidad, estamos interesados en todos los aportes que puedan tener la comunidad sobre la frecuencia en la cual se enlazaran estos datos o la metodología mediante la cual estos datos se pueden publicar.

IRANGA KAHANGAMA: ¿Tienda una fecha potencial?

DAVID CONRAD: Ahora estamos en una etapa de evaluación. Vamos evaluando los requisitos. No me sentiría cómodo en mencionar una fecha específica. Porque, bueno, ustedes saben, somos abogados.

IRANGA KAHANGAMA: Pasamos al micrófono número 3.

MILTON MUELLER: Parece que hay dos enfoques distintos cuando hablamos de DAAR. David habló de uno. habló de recabar una cantidad de datos y cómo utilizar los informes para las políticas. también escuché a los registradores y a los registros que hablan del trabajo que hay por hacer y la intervención al momento de tomar acción. Se habló también de medidas preventivas.

Y tengo una pregunta con respecto a cómo será a DAAR. ¿Cuán extensible sería? Uno está ahora confianza en terceros, en las RBL. La ICANN no puede recabar todos estos datos, pero la cadena delictiva o de amenazas, ¿cómo ustedes responden a todo esto? ¿Están desarrollando algo? Sé que confía en identidades en terceros para hacerlo.

DAVID CONRAD: La respuesta simple es que esperamos que la comunidad nos diga que hacer. Dentro del contexto de DAAR, las amenazas que se identificaron olas que hemos rastreado están plasmadas en el comunicado de Beijing y la comunidad puede sugerir que arrastra y hemos otro tipo de uso indebido. Por supuesto veremos qué podemos hacer para incorporarlo dentro del marco del DAAR. Es extensible.

Con respecto a las fuentes de datos, el requisito primario para las fuentes de datos que utilizamos es que estén públicamente disponibles. Si por ejemplo hay una fuente de datos que la ICANN genera o hay algún otro mecanismo, entonces podríamos incorporar esto dentro del sistema DAAR. Pero una vez más esto va a depender de la demanda que nos haga la comunidad. Creo que mi colega, el señor Piscitello, querer acotar algo al respecto.

DAVE PISCITELLO: Sí. Me complace saber que hizo esta pregunta porque hay ciertas cosas que creo que tenemos que hacer y que no hemos hecho antes. Tenemos un año y medio de historia. En este año y medio de historia uno puede simplemente mirar la conducta de migración y cómo se utilizan los nombres. Yo podría mostrar un gráfico que muestra que hubo un pico en diferentes registradores y sus registraciones, y estas registraciones fueron abandonadas a lo largo del tiempo durante un periodo curativo. Entonces estas son algunas de las mediciones que surgen del análisis en relación a la registración de nombres de dominio maliciosos.

Con respecto a la evolución de las amenazas, yo ya he debatido esto con algunos otros colegas, qué tiene que ver con agregar listas negras o listas de bloqueos, y hacerlo como una delegación distribuida de servicio y ver si un nombre de dominio es confiable, creíble, exacto, público. Estos son los criterios que tenemos. Como dijo David, creamos una plataforma, es una plataforma extensible muchas dimensiones. Y en tanto y en cuanto entendamos que amenazas queremos medir y de qué manera las vamos a medir, creo que podemos hacer mucho de lo que se acaba de sugerir.

IRANGA KAHANGAMA: Hay dos preguntas de la participación remota. Creo que las vamos a leer y después vamos a pasar a la última parte, último punto de debate.

Tenemos una pregunta de Maxim Alzoba. La pregunta dice: El CTO, ¿la fuente podría ser útil para los registradores y los registros? La segunda parte dice: ¿cuál es la razón de utilizar una compañía como Spamhaus como fuente de datos que sacan a los registros y registradores sin responsabilidad o sin procesos de responsabilidad y transparencia en sus sistemas?

DAVID CONRAD: Muchas gracias por la pregunta. Voy a tomar la última pregunta primero.

El uso de Spamhaus se debe a que dentro de la comunidad antiuso indebido, Spamhaus se considera una fuente confiable y que cumple con todos los criterios que hemos especificado inicialmente. Es una especie de construcción para eliminar en la selección de las vistas de bloqueo. También tenemos que tener en cuenta que independientemente de lo que nosotros podamos pensar sobre una lista de bloqueo en particular, la realidad es que estas listas de bloqueo son utilizadas por la academia, por la industria, por los proveedores comerciales y no comerciales para impactar en los flujos de tráfico en Internet y

no podemos decir que una lista de bloqueo no es importante porque no estamos de acuerdo con esa lista porque hay otros colegas que sí confían en esa lista de bloqueo y controlar el tráfico teniéndola en cuenta. Los criterios cambian. Si Spamhaus no es considerado una alternativa confiable, obviamente haremos los cambios necesarios. Y si hay alguna evidencia o alguna demanda de que no está funcionando correctamente o hay alguna especificación de cómo están manejando las solicitudes, eso es otra área que podemos abordar.

Nuestra experiencia ha sido que cada vez que hay algún bloqueo en particular ellos colocan esto en la lista de bloqueo. Tenemos evidencias si hay alguna razón por la cual hay una lista de bloqueo que no funciona tal como dice que funciona, nosotros podemos reconsiderarla. En cuanto a brindar los datos a la comunidad, el plan actual es brindar esta información a la comunidad mediante el proyecto de datos abiertos, pero obviamente esto es a pedido de la comunidad. Nosotros lo podemos adaptar teniendo en cuenta cuáles eran las necesidades.

IRANGA KAHANGAMA: Gracias, David. Creo que hay otra pregunta remota que pasamos por alto. rápidamente.

JAMES COLE: Una pregunta de Kristina Rosette, del registrador Amazon. ¿qué mecanismos y procesos pretende implementar ICANN para evitar los falsos positivos y potenciales responsabilidades en relación con la disponibilidad general del DAAR?

DAVID CONRAD: Como decía, nosotros no estamos generando los datos. Recurrimos a partes externas, a quienes cualquiera puede suscribirse, ya sea pagando una licencia o datos que están disponibles públicamente. Si se considera que un informe es un falso positivo, esto afecta a la manera en que millones de usuarios de estos RBL van a interactuar con el recurso, qué puede ser un nombre de dominio o una dirección IP.

Es cierto que han existido los falsos positivos. Son descripciones infrecuentes y anecdóticas que se llaman falsos positivos, pero la realidad que nosotros consideraremos y los criterios a través de los cuales seleccionaremos las listas de bloqueo es que son los usados por la industria y la academia, que tienen procesos conocidos, que existe un mecanismo claro de operación de la lista de bloqueo.

Respecto de la responsabilidad, no tengo conocimiento de que exista alguna porque yo no soy abogado.

CATHRIN BAUER-BULST: Los últimos 15 minutos veamos de qué manera el DAAR puede dar apoyo a los registros y registradores para prevenir y mitigar y también como puede usarse para ejecutar el cumplimiento y también para la elaboración de políticas. Internamente de la ICANN primero Jamie nos puede contar las necesidades del proceso y cómo piensa usted que esto puede usarlo el área de cumplimiento en el futuro.

JAMIE HEDLUND: Nunca me dieron la oportunidad de expresar cuáles eran mis necesidades, pero bueno, hemos trabajado estrechamente con el departamento de cumplimiento y OCTO. Y es interesante por varios motivos. En primer lugar, brinda evidencia impulsada en datos que da un foco de trabajo. Y segundo, si bien es cierto que las listas que usan DAAR las usan empresas y comunidades corporativas para servicios de email y acceso a la web y otras cosas, eso facilita nuestro trabajo porque ya hay un incentivo incorporado para los registros y registradores que están en un nivel superior en la jerarquía. Para ser claro, el producto del DAAR, como David explicaba, es un nivel acumulado, agregado. Y eso es lo que nosotros no podemos utilizar en cumplimiento. Necesitamos pruebas concretas y accionables que permitan limpiar las zonas de registros y registradores.

Lo último que quería decir es que los outputs que he visto muestran un puñado muy mínimo de partes contrastadas que son responsables de una vasta mayoría de los niveles de uso indebido que existen. Entonces a menudo no son entidades, por lo menos que yo haya visto, de gran participación en la ICANN. Si podemos usar estos datos para progresar, no será solo bueno para los usuarios en general de Internet, que también será bueno para la legitimidad y credibilidad de la ICANN en el modelo de múltiples partes interesadas, que después de la transición es un aspecto importante.

IRANGA KAHANGAMA: Gracias, Jamie. Alan.

ALAN WOODS: Rápidamente quería agradecer a Jamie por su comentario. Es bueno oír tal afirmación, pero quería agregar algo. Hay gente que se porta mal ahí afuera y hay muchos registros que están haciendo realmente lo más que pueden y lo mejor para actuar proactivamente y aparecen en las reuniones de la ICANN y en las discusiones. Nosotros en Donuts estamos siempre a favor de la aplicación. primero suspendemos y testeamos la evidencia. Por supuesto, un enfoque de este tipo nos parece lo mejor.

IRANGA KAHANGAMA: Graeme, ¿quería hablar?

GRAEME BUNTON: Los registros y registradores están a favor de eliminar los malos del planeta. Hay muchos de nosotros que trabajamos duro para mantener nuestras plataformas limpias. En lo que hace a implicancias para política, queremos soluciones de políticas que se apliquen a todas las partes contratadas y registradores. En realidad, la solución debiera ser focalizada a un actor específico. Eso resolvería muchos problemas y nos facilitaría las cosas muchísimo.

IRANGA KAHANGAMA: Micrófono número 1.

GREG MOUNIER: Soy Greg Mounier, de Europol. Tengo una pregunta para Graeme y Alan. A mí me parece que las industrias de nombres de dominio tienen un costo adicional con esto, que requeriría dar vuelta a la lógica y garantizar que en la industria existan medidas proactivas que sean una ventaja competitiva. Por ejemplo, en los registros como Tucows. Si vamos a Tucows y hay una tasa de uso indebido elevado, ¿qué pasaría si actúan

proactivamente desde el marketing y los precios y eso es un beneficio que además les haría ganar más dinero?

GRAEME BUNTON: Ser proactivo también incorpora una responsabilidad que hay que tener en cuenta en el resultado de nuestro balance. Entonces las tecnologías nos permiten ser proactivos en las registraciones, pero todavía yo no lo he visto en un nivel demostrado rentablemente.

ALAN WOODS: En Donuts todavía estamos de acuerdo. Intentamos en el DNS hacer que la iniciativa del DNS y las iniciativas voluntarias que nos diferencian como los buenos actores. Hacemos cosas así. Y también cada vez que cancelamos un dominio le enseña al abusador que puede irse a otra parte. Nosotros podemos sacar los de nuestra plataforma, pero esta gente encuentra otra. Entonces tenemos que dar cómo eliminarlos directamente.

IRANGA KAHANGAMA: Quiero darle la oportunidad a [incomprensible] de hablar.

ROD RASMUSSEN: Cuando vine a mi primera reunión de la ICANN, representaba a una industria, intentaba hablar con los registradores. En esa reunión pasaron otras cosas. La reunión de Vancouver. Entonces no pudimos llegar... Bueno, es historia. Lo que quería decir es que ya pasaron 10 años y muchas cosas se hicieron con éxito. Numerosos ejemplos. Uno de ellos es que grupo de trabajo antiphishing hemos elaborado un informe sobre tendencias en registraciones de dominios usados para pishing. Y estos informes fueron usados por los registradores y registros junto con ellos para identificar problemas. Tras ello, sus políticas se reflejan mejor y mejoraron el espacio de la ICANN y de los ccTLD a través de la evaluación de patrones. Además, muchos registros y registradores han establecido mecanismos automatizados de reporte a través de los cuales varios marcos de backend, algunos contratos.

En mi vida previa yo tenía una compañía que tenía que celebrar un contrato con estas entidades para ser su agente para saber si algo era abusivo o no, y hacer una determinación en su nombre y luego cerrar el sitio. Ahora hay un programa de confianza de intervención confiada que permite acreditar y determinar si alguien tiene el expertise. Entonces se van automatizando las cosas. Ahora es una cuestión de conseguir la información para que la gente la pueda usar. Gracias.

CATHRIN BAUER-BULST: Micrófono 1.

DAVID TAYLOR: David Taylor, de Hogan Lovells. Soy abogado, pero también estoy en el equipo de revisión de CCT. Estoy con ese señor de barba.

La pregunta de sobre el reporte de uso indebido. Es un tema clave. Hay muchísimos registradores buenos y hay muchos malos. Lo mismo con los registros. Cuando vamos por la gente lleva mucho tiempo para que un registrador individual vea que su sitio es cerrado por una actividad ilegal. Podemos estar semanas en la justicia que demoran las cosas. Pero cuando un registrador, como usted nos mostró, se le cancela el sitio, y Jamie lo mencionó, ese uso indebido de alto nivel como .science, donde el 51% de la zona es abusivo y el Registrador sigue acreditado después de meses y años, este representante, esta persona que no es especialista, ¿cómo lo maneja? Yo no logro entender esta dicotomía, esta diferencia.

JAMIE HEDLUND: Esto tiene que ver con dos cosas. El informe agregado, la evidencia, la parte contratada, que tiene altos niveles de uso

indebido no alcanza si no se tiene evidencia. Hay limitaciones además en el contrato propiamente dicho, así que por nuestra cuenta podemos ordenar la suspensión del dominio o la cancelación del sitio. Y algo que yo espero surja del informe del DAAR es que nos va a mostrar donde hemos logrado bien las cosas, donde hemos fracasado, y sigue habiendo malos actores a pesar de nuestros esfuerzos con las herramientas que tenemos. Es la información que llevaremos a la comunidad para que la comunidad lo maneje a través del desarrollo de una política. Incluso aunque no tengamos éxito en limpiar o ayudar a limpiar la base de Registradores y registros, la comunidad y personas como usted tendrán al menos prueba de donde las cosas no han funcionado y quizás sea el origen de una modificación o una enmienda de las políticas y los contratos.

IRANGA KAHANGAMA: Gracias, Jamie. Un último comentario antes de cerrar. Te voy a dar la palabra a Denis que es otra parte afectada del reporte y que nos cuente como todo esto podría usarse a la hora de tomar decisiones.

DENISE MICHEL: El informe SADAG, el informe sobre uso indebido de CCT, muestra que la experiencia de uso indebido con los nuevos gTLD

fue al menos 10 veces mayor que con los legados. La información relacionada y los datos sobre el uso indebido de ese informe ha sido muy útil. Por ejemplo, para el PDP sobre mecanismos de protección de derechos que en este momento está en curso, el PDF sobre procedimientos posteriores que está analizando la creación de políticas para la próxima ronda de nuevos gTLD. Ese es un ejemplo, pero hay muchos otros que se aplican por ejemplo a la implementación de privacidad y proxy y otras áreas de trabajo de la ICANN, pero todo esto tiene que ver con contar con datos de uso indebido con tendencias que luego van a informar a las otras áreas de la ICANN. Queremos que la comunidad tenga datos reales que puedan entender como fundamento para la elaboración de políticas. Es crítico. Si hay algo que podemos ayudar, David, para que los abogados se incorporen. Si podemos diseminar el informe DAAR a la esfera pública y que la iniciativa de open data se lance finalmente, que ha estado estancada durante meses, no me cabe duda de que va a ser muy útil a futuro. Gracias.

DAVID CONRAD: Obviamente yo no estaba bloqueando la acción de los abogados. Solo quería que quedara claro que conseguir la licencia para accionar contra el bloqueo lleva tiempo. Tenemos la confianza de que vamos a avanzar en el futuro. con la

confianza de la información disponible pronto vamos a tener algo en la forma, no sé, de un spreadsheet.

CATHRIN BAUER-BULST: No vamos a poder tomar más preguntas porque no tenemos más tiempo. Pido disculpas. Esto muestra claramente que tenemos que seguir debatiendo. Vimos distintas perspectivas sobre la mitigación del uso indebido y hemos resaltado las distintas necesidades de la comunidad desde la elaboración de políticas hasta las acciones individuales, tanto preventivas como reactivas. Nos ayudó a identificar de qué manera pueden identificarse los datos a través del DAAR. Y una perspectiva interesante que surgió de las intervenciones de David y Jamie en especial es que hay un puñado muy pequeño de partes contratadas donde se concentran los individuos y ahí es donde, en mi opinión, lo general se encuentra con lo específico. Porque los ejemplos que dieron de los 76 dominios es eso dónde tenemos que tomar acción. quizás a futuro de vamos ver cómo cerrar esta brecha entre lo general y lo accionable.

Aquí quizás debamos volver a la idea de los principios que menciono Iranga en la introducción. Y para ello le voy a dar la palabra para que continúe.

IRANGA KAHANGAMA: Decir a los panelistas por participar creo que es importante continuar con esta discusión y creo que la comunidad merece un mecanismo intercomunitario para organizar y generalizar estos temas. Sin duda vamos a reflexionar sobre cómo mejor progresar en el análisis de los temas para darle a la comunidad un mecanismo de trabajo sobre el uso indebido y su mitigación, pero voy a mantener a la comunidad informada para que la comunidad sea transparente y avance en el mejor sentido. Gracias a todos por venir y espero que sigan participando en eventos futuros. Gracias.

[FIN DE LA TRANSCRIPCIÓN]