COPENHAGUE – Sesión intercomunitaria: Hacia la mitigación eficaz del uso indebido del DNS: prevención, mitigación y respuesta
Lunes, 13 de marzo de 2017 – 13:45 a 15:00 CET
ICANN58 | Copenhague, Dinamarca

CATHRIN BAUER-BULST: Hola a todos. Vamos a empezar la sesión en breve. Les pido que por favor se acerquen porque esto no se trata de un panel sino que la idea es tener una conversación. Tenemos acá sitio, tenemos micrófonos. Les pido que por favor se acerquen al sector delantero de la sala. Gracias.

Bienvenidos a esta sesión para una mitigación del uso indebido de DNS más efectiva. Mi nombre es Cathrin. Estoy acá con el grupo de trabajo que habla sobre este tema.

BOBBY FLAIM: Yo soy Bobby Flaim, del FBI. Miembro del grupo de trabajo de seguridad pública, igual que Cathrin.

CATHRIN BAUER-BULST: ¿Por qué vinimos hoy acá? quienes estuvieron en Hyderabad recuerdan quizá que tuvimos un ejercicio que tenía que ver con la mitigación del uso indebido del DNS. Hoy vamos a dar

mayores detalles sobre qué es lo que podemos hacer como para hacer una mitigación de este uso indebido que sea más eficaz. Nosotros siempre hemos hablado, pero cada vez es más importante, sobre todo después de la transición de la IANA, de cuál es la función de las partes privadas dentro de este ecosistema. Nosotros sabemos entonces como norma general que no ejecutan ninguna ley estas partes privadas pero la ICANN tiene un rol cada vez mayor en esta comunidad. Hay un contrato entre dos partes. Nosotros, por ejemplo, tenemos un RAA de 2013, así como otros contratos donde están incluidos no solo el interés de las dos partes contratadas sino también terceros que son partes de ese contrato.

¿Cómo enfrentamos este desafío? ¿Qué es lo que hacemos por fuera del contrato? Una de las partes y una de las cláusulas del contrato habla de garantizar la rendición de cuentas y la transparencia de nuestro lado. Es por eso también que el GAC está interesado en este tema y por eso patrocina esta sesión. Bobby nos va a dar un poco más de antecedentes sobre cómo participa el GAC en este tema.

BOBBY FLAIM: Gracias, Cathrin. Este grupo, junto con el aval del GAC, se creó porque hubo un asesoramiento que brindó el GAC y que tenía que ver con la mitigación del uso indebido del DNS y la

seguridad, y sobre todo cómo el departamento de seguridad de la ICANN y cumplimiento contractual trabajan juntos. Ellos hicieron una investigación independiente sobre lo que se está llevando a cabo. Nos concentramos en tres áreas. La primera, después del asesoramiento del GAC, era el RAA del 2013 o el Acuerdo de Acreditación de Registradores. Si recuerdan, esto fue un asesoramiento del 2010 que tiene que ver con algunas de las disposiciones del RAA que tenía que ver con el WHOIS, la acreditación de la exactitud, etc.

Después, hicimos una validación cruzada de direcciones en las especificaciones el WHOIS. Algunas de las otras cosas que nosotros también queremos explorar en lo que tiene que ver con el asesoramiento del GAC es si las disposiciones del RAA del 2013 están haciendo lo que se pretendía conforme al contrato, para que el cumplimiento sea más eficaz en cuanto a los contratos, para que se mitigue el uso indebido, etc. Esta fue la primera parte entonces del asesoramiento del GAC que se llamó Anexo 1 en el comunicado de Hyderabad.

La segunda parte del Anexo 1 del comunicado de Hyderabad tenía que ver con las medidas de protección del GAC, sobre todo los nuevos gTLD. Lo que incluía esto era cómo los registros podían hablar de los temas de seguridad, sobre todo cómo los podían analizar, cómo los iban a informar a la ICANN. Queremos

hacer un seguimiento de este asesoramiento para ver cuál es la eficacia del asesoramiento, si hay algún informe que se ha realizado y si ha tenido el efecto deseado.

La última parte del Anexo 1 de la que esperamos hablar, y por eso vinieron Maguy y Dave acá, tiene que ver con la relación de ICANN y cómo ellos abordan el tema del uso indebido, cómo reciben los reclamos, cómo investigan los reclamos, qué es lo que están realizando y cuáles son los mensajes que se transportan en cuanto a cumplimiento contractual en cuanto a mitigar este uso indebido. Estas son algunas de las cosas, entonces, desde la perspectiva del GAC y desde la perspectiva del PSWG para hablar un poco más de esto en el día de hoy.

CATHRIN BAUER-BULST: Ahora vamos a pasar a las presentaciones. La primera la va a hacer Greg Aaron del grupo de antiphishing.

GREG AARON: Gracias, Cathrin. Mi nombre es Greg Aaron. Represento al grupo de trabajo de antiphishing. Yo soy uno de los principales investigadores. El APWG es una de las principales asociaciones dedicadas a realizar investigación, educación y a ayudar a las entidades públicas y privadas que están relacionadas con el delito informático sobre todo malware, phishing y el robo de

identidad. También soy un investigador. Yo trabajo con iThreat Cyber Group y también soy miembro del SSAC en la ICANN. A ver cómo funciona esto… No funciona. Les pido a ustedes, por favor, que pasen a la siguiente imagen.

Esta es la información que tenemos del grupo de trabajo de antiphishing que tiene que ver con el phishing que se ha registrado desde 2009. Pueden ver que la línea roja crece constantemente. En el 2016 fue la primera vez que el APWG registró más de un millón de ataques de phishing durante el año. Lo que vemos es que hay mucho phishing que se está realizando y también muchos nombres de dominio involucrados en esta actividad. Miremos el 2009, por ejemplo. Ahí hubo una duplicación del phishing, casi, desde lo que fue el año anterior. Estamos viendo esto. Ese año, mucho de este phishing tuvo que ver con una banda que se llama Avalanche. Establecieron un botnet muy grande. Hubo un ataque muy importante y al año siguiente hicieron malware. Desapareció su actividad de este gráfico. Este equipo hizo el trabajo desde el 2008 hasta el 2016. Fueron arrestados el 30 de noviembre de 2016.

Lo que quiero señalar es que es un grupo que pudo hacer su trabajo durante muchísimo tiempo. En los últimos años, por ejemplo, robaron seis millones de euros nada más que de un banco en línea alemán pero tienen distintos objetivos en toda

Europa, en América del Norte y en otras partes del mundo también. Las pérdidas totales creo que, en definitiva, estarían en cientos de millones de euros. Siguiente imagen, por favor.

Acá tenemos parte de la realidad que tenemos que abordar cuando hablamos del delito cibernético, sobre todo cuando estamos hablando del sistema de nombres de dominio. Con Avalanche, ustedes saben que muchos de estos delitos son profesionales. Por ejemplo, Avalanche tenía el botnet, que se lo alquilaron a otros delincuentes. Hay algunos servicios que utilizan los criminales, los delincuentes, y se los venden entre sí porque en realidad están orientados a obtener ganancias.

Otra de las cosas que vemos es que el uso indebido tiende a concentrarse en determinados lugares dentro del espacio de nombres de dominio con el tiempo y que también con el tiempo se mueven de un lugar a otro. Hay muchos dominios registrados con algunos registradores o ciertos TLD. Las actividades estaban alojadas en determinados proveedores de alojamiento. Una de las cosas obviamente tiene que ver con por qué sucede en estos lugares. Una de las respuestas es que a los delincuentes les gusta estar en lugares donde nadie los va a molestar, donde puedan continuar trabajando por la mayor parte del tiempo posible. Es decir, donde hay alguien que mira para otro lado o que no presta atención a lo que está pasando, que no le presta atención a sus

clientes y que tiene que ver con el espacio de dominio. A veces hay falta de atención, a veces los precios son bajos y obviamente ellos quieren mantener y no ser vistos en el radar.

Hay otras cosas que tienen que ver con la infraestructura. A veces son ellos mismos los dueños de esa infraestructura y todo tiene que ver con el delincuente. Esto pasa en algunos servicios y también pasa en el espacio de nombres de dominio. Hay muchos registradores que en realidad son comprados por los delincuentes. Son propiedad de delincuentes que después fueron arrestados por delitos cibernéticos y los registradores incluso también tenían contratos para matar a algunos de sus asociados. Esta gente existe.

Parte de la mitigación no se hace en el espacio a través de los organismos encargados de la ley ya que tiene ciertas limitaciones. Tienen limitaciones en términos de recursos. Cada organismo encargado de la aplicación de la ley puede trabajar en su propia jurisdicción. Por lo tanto, tiene que establecer cooperación en algunos casos con sus colegas en otra jurisdicción. Eso lleva tiempo. También los fiscales a veces no quieren tomar casos que saben que no van a ganar. El aspecto internacional del ciberdelito trabaja en contra de la aplicación de la ley en muchos sentidos. Lo que estamos analizando entonces es un entorno en que las partes privadas traten de

mantener las cosas en su lugar. Proteger a sus clientes, ellos mismos, y que utilicen contratos para hacerlo. La relación contractual se ve potenciado por esto.

¿Ustedes quieren utilizar el servicio? Google, Facebook… Bueno, vamos a hacer un acuerdo de términos de servicio. Hay que cumplir con esos términos de servicio. Esos contratos también cubren el alojamiento y demás. Ahí es donde se potencializan estos contratos para acabar con las actividades delictivas. Los delincuentes también entienden cómo funciona esto y realmente no juegan con nuestras normas en el espacio de nombres de dominio.

Acá vemos un ejemplo de ciertos datos de reputación de una empresa que se llama SURBL. La idea es proteger el navegador, proteger la casilla de correo. Esto es información que publican, porque hacen una lista de nombres de dominio que consideran que tienen esa reputación. La primera es .COM. Eso se supondría porque tiene 140 millones de nombres de dominio. Es muy grande. La segunda es .TOP. .TOP es un nombre de dominio mucho menor, porque son 4.6 millones. El tercero es .SCIENCE, que tiene 250.000 nombres de dominio en la actualidad, lo que significa que la mitad de esos TLD es un problema, al menos según lo considera este proveedor.

Podemos ver entonces acá, en estos datos, dónde están esos problemas. ¿Por qué se agrupan en lugares como estos? ¿Quién utiliza estos dominios? ¿Qué es lo que está pasando? ¿Quién los vende? Desde mi perspectiva y desde la perspectiva de la comunidad de seguridad, creo yo, nosotros vemos lo siguiente. La ICANN tiene una función que cumplir en lo que tiene que ver con la flexibilidad y la estabilidad. Existe un interés público. Existe una diferencia en hasta dónde llega ese interés público pero en definitiva todos queremos una Internet que sea utilizable y que sea segura para los usuarios.

La ICANN es quien acredita a los registros y registradores. Como parte de ese proceso, la comunidad ha realizado algunos aportes respecto de lo que dicen los contratos. Algunas de las herramientas que nosotros tenemos para abordar este tipo de problemas tienen que ver con las disposiciones de exactitud en el WHOIS. Son disposiciones en el contrato contra el uso de usos maliciosos de la registración. También existen ciertas responsabilidades de parte de los registradores para hacer una respuesta y un informe de estos usos maliciosos. Si existen los contratos, ¿por qué pueden ejecutarse? El tema es: ¿Cómo la ICANN puede utilizar estas herramientas y ejecutar esos contratos?

Como yo dije, nos tenemos que concentrar en utilizar estas herramientas para concentrarnos en los problemas peores porque esta gente se concentra en algunas áreas. Como profesional de la seguridad, a mí me preocupan los problemas repetidos en los mismos lugares, cosas que suceden vez tras vez y van subiendo en cuanto a magnitud. ¿Cómo los abordamos? ¿Cómo hacemos que las partes sean responsables o rindan cuentas si eso es lo que tienen que hacer? Gracias.

CATHRIN BAUER-BULST: Gracias, Greg. Después de esta presentación vamos a hacer una pausa. Ahora vamos a tener preguntas y respuestas con ustedes. Pueden participar desde el micrófono que está acá en el pasillo del centro. Les pedimos por favor que se identifiquen, que manifiesten la pregunta o el comentario que quieren hacer y vamos a esperar que algunos puedan participar. Después de escuchar la presentación veo algunas de las dificultades que podemos encontrar cuando hablamos de mitigación del uso indebido del DNS. ¿Hay alguna mejor práctica como para saber quiénes mitigan bien este uso indebido, quiénes han tenido éxito en esta mitigación?

GREG AARON: Quizá no sea visible para la comunidad porque estas actividades de mitigación se realizan día tras día. De hecho, es algo periódico. Los registradores, los registros, reciben información. A veces a través de los propios organismos de monitoreo o informes de otras personas y los nombres de dominio realmente se suspenden de a cientos y miles por día. En algunos aspectos, las cosas pueden funcionar muy bien. Sin embargo, esto exige que todas las partes reciban una comunicación y que estén dispuestas a hacer lo que les corresponde hacer. Muchos de los problemas no tienen que ver con las personas que forman parte de la reunión de ICANN sino aquellos que no vienen a las reuniones de la ICANN. Hay muchas historias de éxito.

La investigación nos llevó cuatro años. Sabíamos que había cosas que estaban sucediendo pero el grupo consumió un millón de nombres de dominio. Estoy hablando nada más que del grupo Avalanche. No lo sabíamos en ese momento pero pudieron consumir todos esos nombres de dominio, registrarlos y además obtener más. Entonces esto significa un problema repetido.

CATHRIN BAUER-BULST: Gracias, Greg. Ahora los que están frente al micrófono.

JIM PRENDERGAST: En realidad voy a decir algo fácil para empezar. Esto no está en la página de la reunión. ¿Podríamos tenerla?

CATHRIN BAUER-BULST: Sí.

JIM PRENDERGAST: ¿Vieron? Era fácil mi pregunta.

SHANE TEWS: Hola. Shane Tews, de [inaudible]. Esto era para Maguy porque yo estuve en la reunión anterior del día de hoy. Greg tiene buenos datos analíticos. Creo que cumplimiento contractual tiene que mantener la privacidad de la gente pero también nos tienen que dejar saber cuáles son los problemas. Como Greg mencionó, esta gente empezó con phishing. Después pasó a malware. La idea es ver que es el mismo grupo de gente para que los puedan seguir los que están encargados de aplicar la ley obviamente. ¿No pueden hacer que esta información esté disponible o darnos algún tipo de nombre? Porque estamos buscando tendencias. No estamos buscando datos específicos de los casos en particular sino para ver una tendencia que sigue la gente. Eso permitiría que los organismos encargados de la aplicación de la ley vieran que acá hay una queja, la gente se está quejando de

esto, está haciendo reclamos y saber entonces cuál puede ser la tendencia para que nos sea útil para todos.

MAGUY SERAD: David, no sé si lo viste. Yo voy a empezar desde el final hacia delante. Existe una forma que nosotros tenemos de seguir los reclamos. Los reclamos que se hacen a cumplimiento contractual de la ICANN. Si existe un problema, una preocupación que vio una parte contractual y que tiene que ver con un uso indebido, podemos revisarlo según el reclamo recibido. Desde la parte inicial de su pregunta, que tiene que ver con la capacidad de tener más profundidad, más detalles de los reclamos que se reciben, yo creo que es una de las recomendaciones que escuchamos del equipo CCTRT que es tener una granularidad mayor.

Estamos trabajando con el informe. Vamos a trabajar con el equipo de revisión de CCT, el equipo que se armó para poder entender mejor cuáles son los requisitos y ver cómo les podemos dar a ustedes ese nivel de granularidad. Muchas gracias.

CATHRIN BAUER-BULST: Gracias. Megan y después la persona que está delante.

MEGAN RICHARDS: Tengo mi propio micrófono así que no tengo que pararme. Yo soy la representante del GAC de la Comisión Europea. También estoy en el equipo de revisión del CCT. Era una de las preguntas que iba a hacer pero la voy a dejar de lado. Quiero decirles entonces lo que tiene que ver con la lista de phishing. Ustedes dieron los números de crecimiento y lo que resulta importante en ese contexto es la importancia relativa porque en .COM, como dijeron, había tantos millones y en .SCIENCE, 250.000. Los números sí tienen una gran importancia en .SCIENCE. ¿Ustedes pueden ver una diferencia entre los ccTLD, los nuevos gTLD y los gTLD legados? Drew también está analizando esto porque el equipo de revisión de CCT también está haciendo un estudio sobre uso indebido del DNS. También sería muy útil para el GAC la forma para ver cómo reacciona entonces, algunas acciones que se pueden tomar. No sé si los ccTLD nacionales son otro contexto también.

GREG AARON: Yo estoy trabajando en un documento que se va a publicar el próximo mes junto con uno de mis colegas, Rod Rasmussen. Habrá detalles sobre toda la información sobre phishing que se llevó a cabo en el 2015 y 2016. También habrá información sobre otras categorías. Son muchísimos datos. Esperamos que esta sea una publicación específica y abarcativa de los últimos dos años.

Vamos a ver exactamente lo que ha sucedido. Esto va a ser publicado el próximo mes y va a estar clasificado por tipos de TLD.

CATHRIN BAUER-BULST: Vamos a tomar primero algunas preguntas y después vamos a dar por finalizada la discusión de este debate. Luego vamos a seguir en la segunda parte de la sesión.

ORADOR DESCONOCIDO: Tenemos información que no es muy prometedora y también sobre el uso indebido del 2016. Esto implica que hay una cifra que realmente no nos pone muy contentos. Con respecto a la diapositiva número dos, supongo que la forma de mitigar otros usos indebidos va a depender del sector privado más que de las autoridades de cumplimiento de la ley o las autoridades legales. Esto no sucede con los amateurs sino que viene de sectores más profesionales. Nosotros quisiéramos saber las opiniones que tienen las autoridades al tener que liderar y ser los líderes para prevenir este tipo de usos indebidos.

GREG AARON: El uso indebido en algunos casos puede ser rápido y avanza rápidamente. En algunos casos, los delincuentes lo que hacen es

registrar nombres de dominio. Esto avanza muy rápido para las agencias de cumplimiento de la ley. Se tienen que centralizar en ciertos casos en un periodo de tiempo. Básicamente estos son los problemas. Las entidades privadas, los operadores de red y los proveedores de servicios de Internet han lidiado con este tema durante muchos años porque son los únicos que lo pueden hacer. Creo que un buen debate aquí dentro de la ICANN sería que cuando vemos que estos problemas suceden una y otra vez, pensemos qué podemos hacer. Es allí donde nos tenemos que focalizar. Esto, por supuesto, implica al departamento de cumplimiento contractual. La actividad delictiva se mueve con mucha rapidez. Esto no es algo que la legislación pueda abordar en forma diaria. No tan a ese nivel.

CATHRIN BAUER-BULST: Le voy a pedir a los oradores que se identifiquen para los traductores y la transcripción y también que sean breves en sus intervenciones. Adelante, por favor. Siguiente orador.

WERNER STAUB: Muchas gracias. Mi nombre es Werner Staub. Me gustaría referirme a la lista que ustedes han mostrado en relación a SURBL y los TLD. Dos de esos vienen de una parte que tienen un comportamiento independiente con respecto a la ICANN. Esto

muestra la diferencia de flujo entre la gente que trabaja dentro de la ICANN. Me parece que tiene que ser posible que las partes interactúen para poder abordar este tipo de uso indebido. Esa parte puede ganar un proceso en ese caso.

CATHRIN BAUER-BULST: Gracias.

DENISE MICHEL: Denise Miche, de Facebook. Greg, me gustaría volver al último punto que usted mencionó. Quisiera que explicase un poco más respecto de cómo las obligaciones contractuales actuales se utilizan efectivamente para poder abordar todo este tema de uso indebido que estamos viendo en los gTLD y si no, ¿qué sugerencia tendría usted para darnos?

GREG AARON: Probablemente, creo que esta sería una pregunta para Maguy. Lo que yo sí veo en mi trabajo es, por ejemplo, que los registratarios que tienen cientos y miles de dominios tienen que enfrentarse a este tipo de información y a la información del WHOIS. Yo sé que hay algo que está sucediendo allí. No es un indicador de mala fe por parte de los registradores. Podemos ver allí lo que sucede con esos nombres de dominio. A mí me

inquieta un poco cuando veo que estas cosas suceden una y otra vez en ciertos lugares.

DENISE MICHEL: Maguy, quizá usted podría responder eso en la presentación.

ORADOR DESCONOCIDO: Hola. Con respecto a lo que mostró Greg, quiero decir que lo que nosotros hacemos es ajustar el tamaño del TLD. Nosotros tenemos una serie de nombres de dominio y de TLD. También para responder la pregunta que se hizo por allí, sí, vemos muchas diferencias entre el uso indebido en el espacio de ccTLD, que generalmente son los gTLD tradicionales versus los nuevos gTLD. Creo que se puede explicar por qué sucede pero también esto es un signo de que hay mucho por hacer.

CATHRIN BAUER-BULST: Por favor, ¿nos puede decir cuál es la diferencia?

ORADOR DESCONOCIDO: La diferencia es que la mayoría de los ccTLD tienen políticas de registración más limitadas, más restrictas. Por ejemplo, es necesario pertenecer a un país o tener al menos un titular dentro de ese país y para algunos gTLD no existe esto. Están abiertos a

todos. Esto es una diferencia muy importante. Otra diferencia tiene que ver con el precio. Hay dominios que son más baratos y estos atraen a más personas porque las personas que hacen un uso indebido, les importa una sola cosa. Luego, una vez que hacen ese uso, lo abandonan, lo desechan. Si van a desechar un recurso, quieren que ese recurso sea lo más económico posible, obviamente.

DREW BAGLEY: Soy Drew, de la Asociación de Seguridad y CrowdStrike. Quiero hacer un comentario sobre nuestro estudio sobre el abuso o uso indebido del DNS. El grupo se va a reunir mañana a las 11:00. Habrá una sesión donde se abordará en detalle. Se llevó a cabo un estudio del DNS, del uso indebido del DNS. Lo llevó a cabo SDIN y Deflt. La idea es tratar de recabar la mayor cantidad de datos posible. Seguramente muchos de los que están aquí presentes puedan aportar información a ese estudio y también puedan comentar sobre la metodología y con gusto se lo vamos a agradecer. Gracias.

CATHRIN BAUER-BULST: Muchas gracias. Ahora vamos a dar por finalizada la lista de oradores. Vamos a pasar a la próxima presentación. Quiero recordarles a todos que en la sala de Adobe Connect tenemos

también la transcripción. Además de la traducción pueden leer la transcripción que está disponible en la sala de Adobe Connect.

BOBBY FLAIM: Lo que vamos a hacer es lo siguiente. Los presentadores van a dar su presentación durante cinco minutos y luego vamos a dedicar otros 5 o 10 minutos a las preguntas específicas de esa presentación. Al final de la sesión vamos a darles un momento para que hagan preguntas generales. Gracias, Greg, por su presentación. Me parece que ha sido muy buena porque explora las diferentes formas en las que vemos uso indebido y también cuáles podrían ser las formas efectivas de abordar esta situación desde la ICANN, de medir estas tendencias a nivel de las empresas y de qué manera podemos ser más efectivos.

Ahora les voy a presentar al siguiente orador, a Craig Schwartz. Él es el cofundador del consorcio de TLD verificado y también es el registro de .BANK. Craig, si está ahí, por favor, adelante.

CRAIG SCHWARTZ: Muchas gracias, Bobby.

BOBBY FLAIM: Lo escuchamos muy bien. Adelante, por favor.

CRAIG SCHWARTZ: En esta sesión voy a compartir nuestra experiencia con nuestro TLD. Nosotros operamos .BANK. Es el TLD comercialmente más restringido. Hay restricciones en materia de registración. Algunos de los temas con respecto al uso indebido que estamos discutiendo hoy son importantes. Yo voy a dar mi presentación. Estos temas coinciden seguramente con mi presentación.

BOBBY FLAIM: Por favor, Greg. Díganos cuándo podemos cambiar las diapositivas. Craig, parece que tenemos algunos inconvenientes en mostrar las diapositivas. Lo que puede hacer es seguir hablando y mientras tanto resolveremos ese tema.

CRAIG SCHWARTZ: Hay muchos detalles en la presentación del día de hoy. Yo en realidad quiero resaltar algunos datos específicos. Como operador de registros, nosotros tenemos una actividad importante y también hemos hecho un gasto significativo para poder desarrollar políticas y procedimientos y requerimientos para los nombres de dominio y para servir al sector bancario y de seguros a nivel global y a sus comunidades pertinentes. Estamos representados por representantes de la comunidad financiera global. También algunos registros, registradores y otros expertos

en áreas como por ejemplo la seguridad y las operaciones del DNS.

La integridad de .BANK y .INSURANCE está preservada por nuestras políticas. Estas definen estándares sumamente restrictos para poder utilizar .BANK y .INSURANCE. También garantizamos que estos TLD no tengan registratarios que puedan dañar. También tenemos políticas de anti-uso indebido que los operadores pueden utilizar. Ahora estamos avanzando en las cuestiones de antimalware y antispam. En segundo lugar, con respecto a la verificación de los registradores, podemos tener más información en la próxima diapositiva. Se ha realizado un grupo de trabajo, se ha creado un grupo de trabajo basado en la comunidad que ha desarrollado algunas de estas políticas para nuestros registratarios y registradores, para que ellos estén al tanto de esto. Nosotros tenemos también servicios de representación y privacidad para que los delincuentes no puedan acceder a .BANK y .INSURANCE.

En cuanto a la verificación de los registratarios, y esta ha sido una parte fundamental de nuestros TLD, cuando uno es un registratario, no siempre es un operador de registros. Aquí requerimos la verificación antes de otorgar el nombre de dominio, a fin de garantizar que el registro de nombres de dominio sea adecuado. Nosotros sabemos que esto se puede

hacer. También es uno de los gastos más importantes que encaramos al momento de operar los TLD. Con respecto a la selección de los proveedores de servicios de verificación, en 2014 nosotros emitimos una solicitud de propuesta y seleccionamos a un operador que era líder en seguridad para que fuera nuestro proveedor de servicio. Con Bobby estuvimos hablando de esta sesión en la semana y la idea era poder compartir ciertos costos en materia de verificación. Lo que les puedo decir es que las propuestas de servicio de verificación abarcan desde 140 dólares a miles de dólares para los registradores. A veces son menores para los nombres de dominio.

Además de la verificación de registratarios, también tenemos algunos requisitos de seguridad importantes como por ejemplo el DNSSEC. Estos son requisitos: encriptaciones específicas, verificación o autenticación de correo electrónico. Esto se da a diferentes niveles en relación a la información de nuestro sitio web. Como saben, trabajamos en relación a todos nuestros requisitos de seguridad y esto implica un gasto operativo para nosotros.

En cuanto a los puntos en materia de operativa, hay restricciones de registración y verificación que son esenciales para .BANK y .INSURANCE; para poder reducir los riesgos. También hay otros TLD que también están dentro de este grupo.

También quiero compartir que en casi dos años de operación no hemos tenido ningún caso de uso indebido con la utilización del .BANK o .INSURANCE. Tenemos un gasto considerable para desarrollar una serie de recursos para que los registratarios comprendan cómo operar los TLD y que también nos ayuden a activar sus nombres de dominio. Ellos venden muchos nombres de dominio. En .BANK y en .INSURANCE tenemos aproximadamente unas 6.000 registraciones pero no todos utilizan los nombres de dominio.

Antes de pasar al próximo tema, creo que mencioné que los gastos operativos son elevados para los servicios de registro pero los nombres de dominio generalmente van de 1.000 a 1.500 dólares por año. Hay muchos registros que compran estos nombres. También quisiera señalar, como dijo Bob al comienzo, que el fTLD también es un miembro del consorcio de nombres de dominio de alto nivel verificados. Esto incluye otros dominios como por ejemplo .PHARMACY, .MED, junto con otros nombres de dominio respetados. Participamos de las diferentes sesiones de otros grupos de trabajo como el grupo de trabajo de seguridad pública del GAC. También damos resúmenes con respecto a nuestra actividad. Además, hay una serie de recursos que brindamos aquí y que pueden ver en la pantalla. Con gusto voy a responder las preguntas que tengan en esta sesión o en

forma offline. Una vez más, muchas gracias por darme la posibilidad de participar en esta sesión.

BOBBY FLAIM: ¿Hay alguien en la audiencia que tenga alguna pregunta específica para Craig? Tenemos una pregunta.

JOHN LEVINE: Gracias. Creo que usted dijo que había 6.000 participantes pero yo vi que había 2.900 nombres en .BANK.

CRAIG SCHWARTZ: Es una buena pregunta. Debido a los requisitos de seguridad para nuestros nombres de dominio, debe haber una firma del DNSSEC y tiene que estar utilizando sus propios servidores para poder aparecer en la zona de .BANK. Para los registratarios que no tengan esto, tienen que cumplir con estos requisitos para poder entrar en la zona. Si es así, los van a poder encontrar allí en la búsqueda del WHOIS.

JOHN LEVINE: Tengo otra pregunta. .BANK e .INSURANCE siempre han estado regulados. Uno puede ir a un regulador y preguntar si es un banco real. Esto también se aplica a otros como por ejemplo

.PHARMACY o .MED. Me pregunto lo siguiente. ¿Este modelo se expande más allá de ustedes o sigue siendo una parte del modelo?

CRAIG SCHWARTZ: Creo que en general esto se aplica a .BANK y .INSURANCE. Uno de nuestros valores de nuestra proposición es que nosotros tenemos una naturaleza regulada y que podemos dar un aval dentro del espacio. Yo trabajo también en otros espacios pero no podría hablar al respecto.

MICHELE NEYLON: Hola, Craig. Lo obvio para mí es que esto tiene que ver con la escala y el precio. Con este tipo de política y proceso, los dominios solo van a estar disponibles para un subgrupo muy pequeño de registratarios, sean organizaciones o personas individuales. En muchos aspectos, como modelo, no veo cómo esto pueda escalarse para llegar a que los nombres de dominio sean accesibles a todo el público. ¿O hay algo que me estoy perdiendo?

CRAIG SCHWARTZ: No sé si entiendo el comentario, Michele.

MICHELE NEYLON: Voy a ser más preciso entonces. Para verificar y validar los registratarios, según ustedes lo hacen, cuesta una fortuna. El costo de registración de nombres de dominio en cualquier de esos TLD va a ser mucho más alto que en un TLD como .COM. Es por eso que, en términos lógicos, la gente solo puede registrar esos nombres de dominio y mantenerlos si quieren pagar un precio significativamente alto. Es por eso que estos nombres de dominio solo van a estar disponibles para quienes tengan una determinada cantidad de dinero. Básicamente estoy diciendo eso.

CRAIG SCHWARTZ: Sí, es así. Parte del atractivo de nuestro TLD tiene que ver con esa exclusividad y la confianza del consumidor. Es por eso que nuestros TLD son pequeños por diseño. A nosotros nos parece un buen modelo.

BOBBY FLAIM: Gracias. ¿Tenemos alguna otra pregunta para Craig? Entonces podemos pasar a la siguiente presentación. Una de las cosas de las que quería hablar y que tiene que ver con la última pregunta, nosotros ya le hemos preguntado esto a Craig, considerando la escalabilidad y cómo puede funcionar esto en todo el sistema de nombres de dominio. Escuchamos anteriormente que cuando se

escala, no es tan caro. Cuando tuvimos esta conversación, nos parece que existe una gran cantidad de fondos de las subastas que están disponibles. ¿Podrían utilizarse para estos esfuerzos? Sin ir a los detalles específicos, yo creo que para hacer una buena mitigación del uso indebido tenemos que utilizar fondos. ¿Cómo nos puede afectar esto? ¿Cómo puede verse esto dentro de las registraciones de nombres de dominio? No estamos asignando un costo a un registrador y a un registro sino que lo tiene que soportar toda la comunidad. Voy a volver a hablar de este tema. Nuestro siguiente presentador va a ser David Conrad, director técnico de la ICANN. Gracias.

DAVID CONRAD: Gracias, Bobby. Siguiente imagen, por favor. Yo tendría que decir que mi equipo de la dirección técnica ha realizado trabajos de investigación así como actividades de flexibilidad, seguridad y estabilidad. John Crain, que está acá en la sala, es el director de flexibilidad, seguridad y estabilidad. Es su equipo quien ha hecho esta investigación y de lo que voy a hablar yo en esta sesión. Voy a hablar de distintos puntos que incluyen cómo manejar el uso indebido y las interacciones con cumplimiento contractual, las partes con contrato y otros. También vamos a hablar del proyecto de investigación sobre la investigación pública del uso

indebido. La metodología de mitigación del ataque al sistema de identificadores y cómo mejorar la mitigación del uso indebido.

Vamos a hablar del equipo de SSR y cómo interactúa con el equipo de cumplimiento contractual. El equipo SSR y cumplimiento contractual en este momento están investigando cómo podemos mejorar la colaboración. Ustedes saben que tenemos ahora un nuevo departamento de contractual dentro de la ICANN. tanto el nuevo jefe, Jamie Hedlund, como yo, hemos estado hablando sobre la forma en que nuestros equipos pueden dar un mayor apoyo a cumplimiento contractual en lo que tiene que ver con los distintos aspectos de las actividades que tiene que llevar adelante el departamento de cumplimiento contractual. El equipo de SSR tiene que mandar problemas. Obviamente, nosotros no hacemos cumplimiento contractual pero cuando nosotros detectamos algo, lo transferimos a cumplimiento contractual para que ellos entonces lo analicen con mayor profundidad.

El equipo SSR en general habla con las partes contratadas y la comunidad de seguridad operativa para permitir entonces una colaboración informal en lo que es una mitigación voluntaria de las amenazas. Mi equipo, el equipo de John, es el que participa en distintos grupos de confianza del consumidor y estos equipos de confianza lo que hacen es brindar información confidencial

que va y viene y permite que nuestros equipos entonces puedan descubrir los distintos problemas que han estado surgiendo para utilizar nuestro conocimiento y para mitigar entonces en la medida de lo posible.

También tenemos un proyecto de investigación contra el uso indebido en el equipo SSR. Realmente tenemos un contratista que hace un análisis del uso indebido que está en la fase beta. Obtenemos distintos datos, distintas formas de uso indebido que son pertinentes dentro del contexto del comunicado del GAC porque en ese comunicado se habla del phishing, botnets, malware y algunos otros que hemos incorporado por fuera del comunicado del GAC, porque nos pareció que estos eran indicadores muy buenos, aunque no podemos abordarlos directamente. La idea es cómo poner estos resultados a disposición del público. Los datos que nosotros recibimos se consideran datos privados y además están protegidos por un acuerdo de no divulgación que está dentro del contrato.

Esta es una captura de pantalla de esta plataforma beta. Sé que es difícil de leer. La letra es muy pequeña. La idea es que acá encuentran un ranking de los TLD e incluye información como los dominios en la zona, el número de dominios que está en la lista, una calificación para el uso indebido, muestra del 1 al 10. Muestra entonces esta calificación con distintos gTLD que tienen

que ver con el uso indebido que en este caso son dominios incluidos en la lista en relación con la cantidad total de nombres de dominio.

Vamos a hablar un poco entonces de la metodología de mitigación del ataque al sistema de identificadores. Este documento se generó como respuesta a una de las recomendaciones del primer equipo de revisión de flexibilidad, seguridad y estabilidad. Fue obligatoria esta revisión y me parece que se hizo hace cuatro años, no recuerdo bien. La recomendación 12 decía que debía crearse una metodología de mitigación para el ataque del sistema de identificadores. El equipo de SSR entonces generó este documento y acá están los pasos de alto nivel incluidos en esa metodología. Identificar, asignar prioridades y actualizar periódicamente una lista de los ataques principales, desarrollar pautas sobre los ataques de alto impacto y la emergencia de las vulnerabilidades de alto riesgo, describir las prácticas de mitigación de ataques correspondientes y alentar una adopción más amplia de estas prácticas a través de los contratos, acuerdos e incentivos. Si quieren ver todo el informe, lo pueden encontrar en el sitio web de la ICANN y ahí tienen la URL a la a que dirigirse para extraer el PDF.

En lo que tiene que ver con mejorar el estado de mitigación del uso indebido del DNS, el equipo SSR tiene que producir entonces análisis y datos imparciales, por así decirlo, para permitir entonces que la comunidad informada pueda desarrollar políticas que aborden el tema del uso indebido del DNS. También nos confirmamos los aspectos internos, la organización interna, con distintas funciones que tienen que ver con el uso indebido del DNS. Tanto el equipo de SSR como el grupo de investigación del CTO se concentran en estas cosas.

Para mejorar la mitigación del uso indebido del DNS nosotros también damos capacitación y asesoramiento a la comunidad de seguridad pública para permitirles explicar cómo es el DNS, cómo funciona. Los procesos de desarrollo de políticas de la ICANN, cómo se desarrollan, y también cuáles son los procesos administrativos y los procedimientos dentro de la ICANN, dentro de la organización en sí misma. Ahora le voy a ceder la palabra a Maguy.

BOBBY FLAIM: ¿Podrían poner las transparencias de Maguy? ¿Son estas? Perfecto.

MAGUY SERAD: Buenas tardes a todos. Yo trabajo en cumplimiento contractual. Siguiente imagen, Fabien, por favor. Lo que fue el pedido específico del PSWG tuvo que ver con hablar de estos temas. Estos son los antecedentes. Es la respuesta al Anexo 1 del comunicado del GAC. Siguiente imagen, por favor. La primera pregunta fue cómo ICANN y el equipo de SSR de la ICANN y el departamento de cumplimiento trabajan juntos. Como lo dijo David, el equipo de cumplimiento contractual tiene distintas derivaciones internas de la organización de la ICANN. Acá hice una lista de algunas nada más pero quiero poner énfasis en lo que habló David recién. Nuestro equipo ha trabajado desde el comienzo con el equipo SSR en lo que tenía que ver con el uso indebido del DNS. La forma en la que operamos es que nos envían, nos derivan algún problema que han visto y obtenemos la mayor cantidad de información posible de ellos antes de analizar todas las herramientas contractuales y antes de ponernos en contacto con la parte contratada. Todas las derivaciones a cumplimiento tienen la misma metodología. Siguen la misma metodología.

La otra pregunta era qué acciones específicas se habían tomado contra los registradores. Nosotros en cumplimiento somos muy transparentes respecto de las acciones que tomamos y publicamos todos los informes. Lo que publicamos tiene que ver

con las acciones que se ejecutan contra las partes contractuales. Durante esa ejecución, ponemos a disposición del público, de la comunidad, cuál es la actividad de ejecución que se está realizando, para qué parte contratada y, además de un tema específico que se está analizando, lo que hacemos en cumplimiento contractual es antes de emitir un aviso de incumplimiento hacemos una verificación de cumplimiento. Es decir, cuál es el cumplimiento generalizado de esa parte contratada. Es decir, en qué otras áreas puede haber incumplimientos. Lo incluimos todo en el aviso de incumplimiento para que todo forme parte de un mismo tema y no abordar uno por vez.

En el 2016, y esto está en nuestra memoria anual, tuvimos cuatro registradores que recibieron esta nota de incumplimiento. El tema es cuáles son las acciones que tomamos para mejorar el cumplimiento de los registradores. Yo tengo muchas imágenes para mostrar pero para resumir, la mejor forma de mejorar el cumplimiento es hacer actividades proactivas que el equipo de cumplimiento contractual puede iniciar. Nosotros analizamos cuál es el estado del mundo contractual, dónde vemos tendencias, dónde vemos coherencia en temas y oportunidades como para hacer difusión externa, si se trata de difusión externa

al público, por región, al sector público o con una parte contratada específica.

Es una imagen más amplia de hacia dónde dirigimos nuestra difusión externa pero también para mejorar el cumplimiento. Cuando por ejemplo surge un problema que ya abordamos en el pasado y nos damos cuenta de que vuelve a surgir el mismo problema, inmediatamente vamos a un aviso de escalonamiento con la parte contratada porque significa que si no resolvió lo anterior, tiene que resolverlo ahora con este nuevo. También estamos mejorando y promoviendo el cumplimiento a través de las auditorías proactivas que realizamos. Es una forma proactiva de identificar problemas, de que sean abordados, de que sean aclarados, de que sean mitigados para evitar una repetición de estos mismos problemas.

Acá tenemos algunos datos. No voy a analizar una por una estas transparencias. Siguiente, por favor. Una más. Acá tenemos los detalles que respaldan la respuesta que dimos nosotros al Anexo 1 del comunicado del GAC. Tiene que ver con 32.000 reclamos entre noviembre de 2015 y noviembre de 2016 sobre la base de la conversación que tuvimos. Querían saber cómo se desglosaban, cuántos se habían recibido, cuántos se habían cerrado. Lo que quiero resaltar en esta tabla que tienen en pantalla es que nosotros recibimos el volumen que ustedes ven a la izquierda

pero también necesitan ver y prestar atención a que revisamos los reclamos antes de enviárselos a las partes contratadas y entonces ven que hay una columna que dice: “Cerrado antes de un primer aviso”. Pueden ver cuál es el volumen. ¿Por qué hacemos esto? Porque a veces nosotros recibimos reclamos que no están completos o que no están dentro del alcance de las alegaciones o un reclamo que nos hicieron pero que tiene que ver con un nombre de dominio que ya fue suspendido o que ya ha sido eliminado o que no es válido. Por eso tenemos muchas causas para el cierre y están publicadas en nuestro sitio web.

Lo que le damos a la audiencia es algo que quizá no revisan. También tenemos un procedimiento de resolución informal. Yo quiero llamar la atención a esta audiencia sobre qué es lo que sucede entre la primera, segunda y tercera notificación antes de esta notificación o aviso de incumplimiento. Miren lo que es el primer aviso. Después de dar el primer paso. Vamos a ver inexactitudes de WHOIS, casi 14.000 reclamos en la primera notificación. Lo que nos dice esto es que esta cifra, que es mucho menor en la segunda notificación, significa que cuando se plantearon, se resolvieron los problemas en la primera notificación. Cuando hablamos de una segunda notificación, hablamos de 1.340.

¿Qué sucede en este caso? Si una parte contratada no responde a un aviso de cumplimiento, entonces pasamos a la siguiente etapa. Si cumplimiento recibe una respuesta completa de esta parte contratada a último minuto, pasa a la segunda fase. El mensaje acá es de 14.000, pasamos a 1.300. Se aplica el mismo principio porque tenemos 160 en la tercera notificación. El objetivo que tenemos nosotros entonces es que los problemas que se plantean a cumplimiento contractual hayan sido revisados, hayan sido abordados y que hayan sido resueltos o cerrados. Eso es lo esperable. Podría hablar un poco más de esto porque en realidad, Bobby, ustedes nos pidieron más detalles sobre esto.

Estoy terminando. Fabien, por favor, una más. Esto es para que ustedes analicen. Una más, Fabien, por favor. Estas son las actividades de monitoreo que realicemos. Acá quiero mostrarles cuáles son las fuentes que nosotros utilizamos cuando hablamos de estos monitoreos. Acá resalté algunas actividades de difusión externa del 2016 pero estas también están disponibles en nuestro sitio web. Con esto concluyo mi presentación. Muchas gracias.

BOBBY FLAIM: Muchas gracias. Perdón que pedí que te apuraras pero teníamos nada más que 12 minutos. Veo que hay preguntas en la

audiencia. Quienes están aquí en la mesa también pueden pedir la palabra.

JOHN CARR: John Carr, de la Alianza de ONG Europea para la Seguridad Infantil en Internet. Realmente me llamó mucho la atención la primera presentación en la cual se muestra el alto nivel de seguridad y verificación para confirmar la identidad de ciertos registratarios, etc. Voy a dar un ejemplo concreto de por qué. Nosotros venimos siguiendo el tema de .KIDS, de ese gTLD, y el proceso correspondiente. Como saben, ha sido resuelto pero hace cinco meses descubrimos que de hecho .KIDS está en alfabeto cirílico. Hay un registro en Rusia que se llama .DYETI. Tengo estas dos preguntas. Cuando uno vende una registración a .DYETI, ¿qué hace? ¿Se verifica quién puede comprar ese dominio? Por ejemplo, ninguna persona que haya sido convicto por delitos de abuso infantil. ¿También se estipula quién puede trabajar por una organización comercial que opera un dominio .DYETI o .KIDS? ¿Se verifica si ese es el caso?

La respuesta a ambas preguntas fue no. no se estipula nada al respecto. Obviamente, tampoco tratan de verificar si se han cumplido esas condiciones o no. para mí, entonces, la ICANN ha fracasado en su deber de cuidado hacia los niños para garantizar que en el acuerdo de registro para .DYETI se hayan incluido estas

condiciones. Creo que esto entonces demuestra lo que tendría que hacer la ICANN. Si .KIDS es aceptado dentro de una cuestión de seguridad, entonces podría ser parte de otra cuestión para verificar cuestiones financieras de los TLD que sí se verifican. Esta es una pregunta general que guarda relación con un comentario general para ver hasta qué punto se podría lograr lo que yo estoy proponiendo. Gracias.

DAVID CONRAD: No estoy seguro de cómo responder esa pregunta. Lo que yo diría es que uno de los procesos que se están realizando actualmente tiene que ver con procedimientos relativos a la próxima ronda de nuevos gTLD. Quizá ahí entonces se podría prestar atención a este tema y requerir mayor información por parte de los registratarios. Con respecto a los gTLD existentes, obviamente no soy la persona indicada para hablar al respecto porque no tengo formación acerca de los contratos y las cuestiones legales respecto de quién puede registrar un dominio dentro de estos TLD. Tengo que dejar que eso lo responda el departamento de asuntos legales.

CATHRIN BAUER-BULST: Tenemos una pregunta de Steve Metalitz que dice: “Gracias por la presentación. Ustedes hablan de los contratos y del

cumplimiento efectivo y luego también algunos dicen que ese cumplimiento lo realizan algunas partes que operan en las sombras. ¿Ustedes tienen respuesta a esas críticas?"

GREG AARON: Creo que Steve se refiere al cumplimiento efectivo de marcas comerciales. Esta es un área muy específica que se distingue de los delitos cibernéticos o ciberdelitos. Creo que hace un tiempo se estableció que el phishing y el malware y otras cuestiones delictivas ameritan un rol de la comunidad. Hay muchas partes como registros y registradores que vienen tratando estas cuestiones. Steve se refiere a las marcas comerciales que son más bien una cuestión del derecho civil.

KEITH DRAZEK: Hola. Soy Keth Drazek, de VeriSign. Tengo una pregunta acerca de si ustedes se ocupan de la cuestión del hopping de dominios. Los funcionarios de coordinación de propiedad intelectual de la Casa Blanca se ocuparon de esta situación en la cual hay delincuentes que pasan de un TLD al otro, al otro, al otro y así sucesivamente. Es decir, saltar de un dominio a otro para poder continuar con el uso indebido. Esto no es específico de la propiedad intelectual sino que usted, Greg, en su informe mencionó instancias de miles de dominios que están siendo

registrados. En esas instancias, ya sea 1, 10 o 10.000, hay delincuentes que traspasan su comportamiento indebido de un TLD a otro.

Pregunto: ¿La ICANN podría ayudar a los actores de la industria, registros y registradores, a que colaboren y se comuniquen para identificar instancias en las cuales estos actores maliciosos están identificados en un TLD, ya sea gTLD o ccTLD, y luego identificar este comportamiento indebido y hacer las comunicaciones pertinentes para identificar su posible curso de acción? Es decir, ir detrás de estos ciberdelincuentes cuando pasan de un TLD a otro. Gracias.

GREG AARON: Ahora tenemos una gran cantidad de estos dominios registrados a nivel mundial y a veces estos dominios son utilizados inmediatamente después de su registración. A veces quedan ahí durante meses y luego se comienza a utilizarlos. Habría que hacer una iniciativa de coordinación para tratar de identificar a estas personas que también utilizan identidades falsas. Falsifican su información en WHOIS, por ejemplo. Tenemos que garantizar el acceso a la información y tener disponible siempre la información de WHOIS es un tema bastante candente en este momento en la ICANN. Tenemos que ver cómo lograr la

existencia de las normas aplicables y la disponibilidad de la información. La ICANN tiene que tratar con esta cuestión.

Por supuesto que es importante tener esta información porque sin ella es muy difícil ver qué es lo que está sucediendo y poder tomar decisiones. También es difícil que podamos rastrear a estas personas y ver qué están haciendo a diario. Es decir, tal o cual persona estuvo aquí y ahora está en este otro lugar. Es una tarea muy difícil. Requiere fondos y recursos específicos para lograr el objetivo.

CATHRIN BAUER-BULST: Antes de pasar a la próxima pregunta quiero decir que es muy interesante ver también qué pasa cuando se retiran contenidos y evitar que el contenido aparezca en otro sitio web. Ustedes estarán al tanto de las fotos en este sistema. Lo que hacemos es poder comparar imágenes que fueron modificadas con este ADN fotográfico para ver entonces la similitud. No estamos utilizando información personal identificable sino información que tiene determinado tipo de características que permite su identificación. Probablemente entonces podríamos hacer algo similar y utilizar los fondos provenientes de las subastas para estos temas. Son grandes desafíos que tenemos por delante. Vamos a tomar tres preguntas más y luego concluiremos la sesión.

JOYCE LIN: Soy Joyce Lin, de 007names.com. Creo que es muy importante tener los análisis de datos para los usos indebidos del DNS pero creo que lo más difícil es el cumplimiento efectivo. Me parece que actualmente el cumplimiento efectivo recae sobre los hombros de los registradores. Por ejemplo, hace poco recibimos un correo electrónico de quienes monitorean el tráfico ilegal de medicamentos en Internet. Nos enviaron un correo electrónico y nos dijeron: "Tienen 12 nombres de dominio que están vendiendo productos farmacéuticos ilegales". Nosotros tratamos de proceder bien, de colaborar. Identificamos a los registratarios y les enviamos los correos electrónicos. Les dijimos que habíamos recibido esa queja acerca de su nombre de dominio, que estaban incumpliendo el acuerdo de servicios de registración y según el RAA y las disposiciones contractuales, les teníamos que dar un plazo para que corrigiesen esta situación. En dos horas, tres dominios desaparecieron. Se trasladaron.

¿Qué hacemos? Nosotros, como registradores, perdimos la renovación de esos dominios y las ventas y no pudimos resolver nada. Yo me siento un poco tonta porque eché a un cliente pero tampoco pude ayudar a resolver el problema que se nos había planteado. Creo que la ICANN probablemente tendría que pensar en otra manera de abordar este tipo de uso indebido. Por

ejemplo, tenemos cuatro o cinco nombres de dominio que deberían ir al registro y no al registrador en cuanto a este tipo de cumplimiento efectivo. De repente, no sabemos qué pasó con esos dominios. El cliente no lo pudo modificar, renovar. Fuimos al registro y vimos que había una resolución judicial para suspender esos dominios. Sin embargo, nos dijeron que había que seguir pagando por esos dominios y nuestro cliente no lo quiso hacer. ¿Durante cuánto tiempo estará vigente la resolución judicial? Quizá por el resto de mi vida, entonces yo tengo que pagar todo esto.

Lo que quiero decir es que la ICANN o quien sea que tenga la autoridad legal, tiene que identificar los nombres y decirle al registro: "Usted tiene estos nombres bajo su patrocinio. Tiene que suspenderlos, retirarlos del archivo de zona". Esto sería más efectivo. De lo contrario, no hace falta saltar de un TLD a otro. Se puede pasar de un registrador a otro. Hay muchísimos a nivel mundial y eso se puede hacer. Gracias.

BOBBY FLAIM: En respuesta a esa pregunta, y a la pregunta de Keith, que tiene que ver con el hopping de dominios, quisiera saber si el equipo de cumplimiento contractual o de seguridad de la ICANN puede compilar una lista de actores maliciosos para evitar que accedan al DNS. ¿Es posible?

DAVID CONRAD: Bueno, en Internet nadie puede reconocer a un ciberdelincuente si no hay información externa que lo identifique. Muchas veces es muy difícil identificar soluciones a estos problemas. La organización ICANN se fundamenta en la comunidad de la ICANN para que nos ayude a identificar mecanismos que permitan abordar las cuestiones que nos afectan a todos. Con respecto al saltar de un dominio a otro, al hopping de dominios, quizá puede haber grandes datos asociados que sean de utilidad, algunas técnicas que sugieran cierta actividad potencial en la cual un conjunto de nombres de dominio se utilicen de esa manera, saltando de un TLD a otro. Eso se lo podemos enviar a los registros y registradores como una posible vía de identificar a los TLD que estarían en vulnerabilidad. Después hay que ver qué se hace con esa información. ¿Bloqueamos los dominios? ¿Evitamos que los adquiera alguien que tenga una razón totalmente válida para su adquisición?

Ahí empiezan a surgir preguntas complejas. Con respecto a los registros versus los registradores y la recepción de notificaciones, claramente hay algunas zonas en las cuales se podría mejorar la comunicación, la cadena de notificaciones. Eso es algo que un miembro de mi equipo está investigando: El ciclo de vida del uso indebido de los nombres de dominio y ver cómo

enviamos la información que recabamos en la organización a la comunidad y cómo ayudamos a la comunidad en sus debates acerca de políticas, lo cual básicamente significa que no vamos a tener una respuesta a corto plazo pero esperamos poder ayudar a la comunidad en sus deliberaciones.

KAVOUSS ARASTEH: Soy miembro del GAC. Quisiera presentar una perspectiva diferente a esta situación. Quizá estamos tratando esta cuestión de a poquito, paso a paso, y no mediante una estrategia a largo plazo. Las medidas adoptadas que incluyen la mitigación aparentemente no abarcan y no están a la par de la velocidad de estas cuestiones de uso indebido. Quizá hay personas que van más rápido que ustedes. Son más inteligentes que nosotros y utilizan esa inteligencia para actuar de mala manera. Tenemos que cambiar nuestra forma de actuar. Tenemos que actuar de manera más coordinada. Hasta tanto no veamos una reducción concreta en estas medidas contra el uso indebido, no creo que podamos sentirnos seguros de que lo que estamos haciendo responde proporcionalmente al problema.

Probablemente no lo solucionemos del todo pero según las estadísticas que ustedes nos han mostrado, esto crece de manera exponencial. Con lo cual, nuestras medidas tienen que ser revisadas. Por favor, no se tomen esto como una crítica sino

como una advertencia para considerar esta cuestión desde otro ángulo. Algunos han dicho que los reclamos no se procesaron porque no eran reclamos completos. Uno tiene que utilizar herramientas de validación para el reclamo y antes de enviar un reclamo a la ICANN hay que validarlo. Si no se valida el reclamo, entonces todavía no es tal, no es un reclamo. Es decir, eviten recibir algo y registrarlo como un reclamo que no recibió tratamiento. Además, existe la necesidad de ver si realmente existe la voluntad de todas las partes de actuar.

Yo dudo de que exista esa voluntad. Desde el 2007 he presenciado distintas deliberaciones que comenzaron como parte de la agenda de ciberseguridad que derivaron en dos años de estudios que luego fueron rechazados porque hubo quienes dijeron que no se los podía aplicar por cuestiones internas, por políticas internas, etc. Quizá deberíamos ver si todas las partes tienen esta voluntad y luego ver si tenemos una estrategia a largo plazo y ver si las medidas adoptadas se condicen con todo lo que está sucediendo. Si no vemos una reducción significativa, eso significa que nuestro proceso ha fracasado y que no es un problema de ustedes sino nuestro. Es un problema colectivo y lo tenemos que volver a considerar. Gracias.

CATHRIN BAUER-BULST: Gracias, Kavouss. No sé si alguien quiere responder.

MAGUY SERAD: Kavouss, quisiera referirme a lo que usted dijo respecto de los reclamos incompletos. Básicamente, lo que estaba tratando de decir anteriormente es lo siguiente. Cuando recibimos reclamos los analizamos para garantizar que tengan la información correspondiente. A veces no nos dan pruebas, no nos dan información correspondiente entonces volvemos a quienes presentaron los reclamos y les pedimos más información. Los casos realmente son muy diversos. Quiero que usted sepa que nosotros hacemos un seguimiento con quienes han presentado los reclamos de manera tal que cuando le enviamos la cuestión a las partes contratadas, tienen la información necesaria para ocuparse del tema. Gracias.

ALAN WOODS: Quiero decir algo con respecto al programa en versión beta que usted mencionó y que tiene una lista de los usos indebidos en distintos TLD. Tengo tres dudas o preguntas o comentarios. En primer lugar, quisiera saber quiénes son los terceros sobre los cuales usted basa su información. Desde el punto de vista de un registro, muchos de nosotros estamos en esa situación. Tenemos requisitos y cada uno de nosotros quizá tenga una perspectiva distinta acerca de esta lista. Una de las preguntas que siempre formulamos es si quizá hay algunos integrantes que haya que

considerar, que sean mejores que nosotros. Nos han dicho que esta lista nos permite pensar en lo siguiente. Sí, deberíamos tener cierta idea de que es lo que está sucediendo, cuántos casos existen, etc. pero al mismo tiempo debemos tener bien claro que tener una lista negra de proveedores no equivale a algo sobre lo cual los registradores puedan actuar porque nosotros necesitamos evidencia de esos informes o denuncias y podemos decir: "Esto está en la lista negra. Yo puedo actuar al respecto". No, no. tenemos que investigar un poquito.

Yo diría: ¿Cuál es el propósito de este programa beta? ¿Hay una idea equitativa de que hay ciertas listas negras que tienen una mejor calidad? Luego preguntaría cómo va a relacionarse todo esto con los registros y con la manera en la cual nosotros actualmente cumplimos con nuestras obligaciones.

CATHRIN BAUER-BULST: Muchas gracias. Yo sugeriría lo siguiente. Vamos a tomar una última pregunta y luego vamos a escuchar las respuestas. Si puede hacer su pregunta en 30 minutos… Podrían ser 30 minutos, pero no, quise decir 30 segundos.

VOLKER GREIMANN: Yo soy un registrador en Key-Systems. Nosotros, como parte contratada, a veces es difícil ver el reclamo porque nosotros

somos expertos en la gestión de nombres de dominio y no de uso indebido. No sabemos si es algo legal o es algo ilegal en algún país. No podemos ver toda la imagen. A veces nos piden que bajemos un sitio web y lo hacemos, y luego nos llama un mecanismo encargado de aplicación de la ley y nos dicen: "No. ¿Qué están haciendo? Están investigando esto. Dejen de investigarlo". Realmente no sabemos qué es lo que pasa con ese sitio web. Nosotros tenemos una indicación de lo que puede suceder pero también cuando tenemos que tomar una decisión respecto de un reclamo por un uso indebido, a veces no sabemos qué hacer porque nadie nos identifica como aquellos que tenemos que tomar la acción o que tenemos que dejar de tomar la acción. Entonces la tenemos que tomar a nuestro propio riesgo social, nuestro propio riesgo jurídico y nuestro propio riesgo económico.

DAVID CONRAD: Para responderle a Alan, la génesis de todo este proyecto de investigación fue un informe publicado me parece por Blue Coat que documentó y dio estadísticas sobre el uso indebido del DNS, algo que fue cuestionable. La metodología que utilizaron se consideró que no era eficaz, que dio una estimación razonable del uso indebido que podía sufrir un registro. La idea de nuestro proyecto entonces fue recopilar los datos de la mayor cantidad

de fuentes posibles. Nosotros no tenemos una limitación en cuanto a la cantidad de fuentes que podemos incluir en el sistema y documentar una metodología públicamente para que la comunidad pueda verla, pueda estar de acuerdo con esa metodología y ver cómo se establecen las métricas.

La intención es nada más que informar. Tenemos un conjunto de datos que muestran ciertas conductas en el tiempo. Mi equipo, como dije anteriormente, nosotros no tenemos responsabilidades de cumplimiento contractual. No es nuestra tarea pero la idea es darle información a la comunidad para que la comunidad entonces pueda confiar respecto de qué nivel de uso indebido está afectando a determinados registros con la intención, con la esperanza de que los registros puedan utilizar esa información para trabajar con la comunidad y con los procesos de generación de políticas para mejorar la mitigación del uso indebido del DNS en el futuro. No sé si Maguy puede responder a la segunda pregunta.

CATHRIN BAUER-BULST: Me parece que vamos a tener que cerrar la sesión porque lamentablemente nos hemos pasado del tiempo. Pueden darse cuenta de que esta conversación va a seguir adelante de una forma o la otra. Creo que hay algunos aspectos clave antes de cederle la palabra a Bobby para que concluya la sesión. Creo que

no existe suficiente información. A veces existe información que se contradice y no hay acuerdo sobre cuál es la información que debemos recopilar. Creo que tiene que haber una cooperación entre el equipo de SSR y cumplimiento contractual. Vemos también que algunos de los registros también hablaron de un 48% para .SCIENCE y otros registros. Yo, como abogada, digo que esto tendría que disparar directamente la actuación de un organismo encargado de la aplicación de la ley pero quizá esto no siempre es posible. Tenemos que ver cuál es la información viable y cuáles son los pasos que puede tomar cumplimiento contractual de la ICANN sobre la base de esta información. Creo que también la comunidad tiene un rol que cumplir. Tenemos que mirar cómo mejorar la cooperación y también, como somos diferentes partes de la comunidad las que tienen sobrecargadas por el rol que tienen que cumplir en este proceso, nosotros como unidad tenemos que ver cómo poder mitigar esa responsabilidad, siendo la mitigación obviamente el término clave de hoy. Ahora le voy a ceder la palabra a Bobby para las palabras finales.

BOBBY FLAIM: Gracias, Cathrin. En primer lugar, quiero agradecerle a Maguy, a David, a Craig, que participó remotamente, y a Greg. Muchísimas gracias a todos los miembros del panel porque realmente fueron

presentaciones que arrojaron mucha luz sobre este tema. Como dijo Cathrin, nosotros tenemos algunas cosas que tienen que ver con la mitigación del uso indebido del DNS. El PSWG del GAC tiene algunas otras preguntas vinculadas con el Anexo 1. Esperamos obtener más información. También quiero resaltar el CCRT y también el informe de mitigación del uso indebido del DNS.

Contar con este informe también va a ser muy útil y también, como dijo Kavouss o también Keith y Joyce, tiene que haber algún enfoque sistémico a todo lo que tiene que ver con el uso indebido, los registratarios y ver también cómo podemos trabajar con los registradores para que no hagan un uso indebido del DNS. Obviamente también podemos utilizar parte de los fondos que tiene la ICANN, que resultaron de las subastas, para ver si podemos promover esto y que no sea un peso para ninguno de los miembros de la comunidad. Muchísimas gracias a todos. Les agradecemos el tiempo, la participación y haber asistido a esta reunión. Muchísimas gracias.

[FIN DE LA TRANSCRIPCIÓN]