HYDERABAD – Sesión de temas de alto interés: mitigación del uso indebido de los gTLD
Sábado, 5 de noviembre de 2016 – 13:45 a 15:00 IST
ICANN57 | Hyderabad, India

ORADOR DESCONOCIDO: Sala 3. 5 de noviembre de 2016, de 13:45 a 15:00. Es la sesión de temas de alto interés, mitigación del uso indebido en los gTLD.

ALICE MUNYUA: Buenas tardes a todos. Les agradezco estar presentes en esta reunión de temas de alto interés, que va a ser liderada por el PSWG. Vamos a empezar con una breve introducción de los panelistas, que les pido que digan de donde vienen y a qué lugar pertenece.

MICHELE NEYLON: Yo soy Michele Neylon, registrador.

BRIAN CIMBOLIC: Brian Cimbolic, registros.

STATTON HAMMOCK: Statton Hammock, registros.

CARLOS ALVAREZ: Carlos Álvarez, equipo SSR, personal de la ICANN.

GIOVANNI SEPPIA: Giovanni Seppia.

DENISE MICHEL: Denise Michel, unidad de negocios.

ALLEN GROGAN: Allen Grogan, de cumplimiento.

DREW BAGLEY: Drew Bagley. Yo vengo de la fundación de dominio.

BOBBY FLAIM: Bobby Flaim, del FBI, PSWG.

FABIEN BETREMIEUX: Fabien Betremieux, soporte de la ICANN, personal de la ICANN.

RICHARD ROBERTO: Richard Robert, de registros.

ALICE MUNYUA: Muchas gracias. Les damos la bienvenida a todos.

Brevemente, el PSWG fue creado en el 2015 durante la reunión de Singapur y el principal término de referencia se concentra en los procedimientos de la ICANN que tienen relación con la seguridad del público. Entonces sé que no tenemos mucho tiempo. Entonces quiero que sea un debate interactivo.

En esta sesión nos vamos a concentrar en como mitigar el mal uso de los gltd. Y el objetivo y resultado que se espera obtener de esta sesión es darles una actualización a la comunidad de la ICANN y a las organizaciones de apoyo y a los comités asesores. También de cuáles son las mejores prácticas de la industria en mitigar el mal uso del DNS.

Vamos a tener una actualización de la comunidad de la ICANN, de las SO, de los AC, de la situación actual de las actividades, incluso lo que es la información actual, y también todos los compromisos que tienen que ver con mitigar el mal uso. Después vamos a darle una oportunidad a nosotros como comunidad de la ICANN para plantear preocupaciones, presentar cuáles son las opiniones para ver cómo es el camino que tenemos que seguir, sobre todo con lo que tiene que ver con las actividades de revisión que se están realizando.

Ustedes pueden ver el temario que tenemos. Vamos a empezar con una definición con Bobby Flaim, del PSWG. Así que, Bobby Flaim, le doy la palabra.

BOBBY FLAIM: Gracias, Alice. Creo que cuando hablamos de abuso estamos hablando… Nosotros tenemos un juez en EEUU que trata de definir la pornografía que es que uno la reconoce cuando la ve. Y creo que esto se puede aplicar cuando hablamos del mal uso o uso indebido del DNS. En realidad la definición proviene del PSWG o de las medidas de protección del GAC. Pueden hablar de pharming, phishing, malware, pero no es una lista exhaustiva, sino que es una lista técnica.

El mal uso y la delincuencia varían de país a país. Hay que considerar cuales son las leyes vigentes porque lo que es un delito en un país puede no ser un delito en otro país. El tema de la explotación de los niños del DNS se utiliza también sitios web para el terrorismo. Lo vemos en la televisión. Hay muchos malos usos diferentes de lo que puede ser el abuso del DNS. No hay una sola definición sólida. Creo que es lo más importante que tenemos que tener en cuenta cuando hablamos del DNS, cuando hablamos de la seguridad pública del DNS.

Sé que tenemos un buen panel. Y uno de los propósitos del grupo de trabajo de seguridad pública es hablar con los operadores, que tiene que ver con los registradores, los registros, la seguridad, el cumplimiento, para ver qué es lo que se ha hecho, cuáles son algunas de las mejores prácticas para

garantizar que estamos previniendo y evitando el uso indebido en el DNS, sobre todo en la ecosfera de la ICANN.

Confiamos en que esta sesión va a ser productiva y esperamos tener un dialogo. Parte del debate que vamos a tener hoy, no solo con los oradores, sino con ustedes, con la audiencia, porque esperamos que participen. Entonces sin más voy a presentarles a mi colega, Drew, que va a hablar o mostrar algunos de los ejemplos claves, si quieren llamarlo ustedes, del uso indebido.

Drew.

DREW BAGLEY: Gracias, Bobby. Bueno yo voy a hablar entonces desde la perspectiva de algunas de las tendencias de un uso indebido que hemos visto en la Secure Domain Foundation, que es una organización sin fines de lucro, que se especializa en la investigación del uso indebido proactiva.

El uso indebido del DNS es algo que resulta importante, no solo en el mundo en el que vivimos en la ICANN sino que es algo que afecta a tantas personas en todo el mundo porque son víctimas de las últimas tendencias del ciberdelito que muchos de los titulares que escuchamos hoy empiezan con algo simple, que es la registración de un nombre de dominio.

Entonces, como mencionó Bobby, las definiciones técnicas del abuso son en general más estrechas y presentamos en phishing, pharming, un alojamiento de software malicioso, botnet. Pero incluso el uso indebido del DNS puede afectar a muchas otras cosas. Hay algo que es una tendencia y supongo que todos los conocen en los últimos años es que el uso indebido del DNS ahora tiene ramificaciones financieras a gran escala, como nunca lo tuvo en el pasado. No es aislado y se trata de una sola víctima, sino que no tiene una importancia micro, como nosotros pensábamos. El uso indebido ahora está hablando de la estabilidad y está interrumpiendo la estabilidad del DNS.

Algunas de las tendencias más nuevas, sobre todo en lo que vimos el último año y algunos de los títulos que algunos de ustedes vieron en los últimos meses, tienen que ver con el ransomware, que tiene diferentes formas, Cryptolocker y Locky por ejemplo. También hemos visto el compromiso de correo electrónico de las empresas y los botnets, sobre todo en las últimas 2 semanas lo hemos visto en todos los titulares.

Entonces el ransomware o este software que pide un rescate para seguir adelante, cuando uno va a un sitio web o hace clic en un enlace y dice que está todo encriptado y que se puede solo desencriptar si uno paga el rescate. Ahora este ransomware ha afectado no solo a grandes empresas, sino hospitales también. Entonces lo que vemos en el resto del mundo es que

algo que se transformó en un problema donde una empresa puede perder, realmente toda su propiedad intelectual en forma instantánea y su posibilidad de seguir adelante con el negocio, una vez que las computadoras están encriptadas, a menos que paguen ese rescate.

Como consecuencia, las victimas en general pagan este rescate. Realmente se ha vuelto un negocio lucrativo para los ciberdelincuente. Las estadísticas muestran que las infecciones están aumentando rápidamente. En marzo del 2016 hubo nada más que 56.000 infecciones, solo en ese mes. Es dos veces más de lo que habíamos visto el año anterior, donde teníamos 23.000 infecciones por mes. La cantidad de dinero que se ha pagado ha superado los 200 millones de dólares.

Hay otra tendencia dentro del ransomware y es que ahora se ofrece como servicio. Uno no tiene que saber exactamente cómo codificase, sino que uno puede pagar para utilizar el ransomware como servicio y así obtener víctimas. Otra tendencia que mencioné es el compromiso de correo electrónico de empresas porque hay phising en los correos electrónicos y entonces parecen legítimos porque están escritos en el mismo estilo que el empleado del que se supone provienen. Y en última instancia generan una operación financiera donde el ejecutivo de esa empresa piensa que es un pedido real del departamento de contabilidad y entonces hay

un robo. Según el FBI ha habido más de mil millones de dólares en pérdidas por este tipo de ataques.

En los botnets y la internet de las cosas lo hemos visto en ciberataques. Me estoy quedando sin tiempo así que voy a cerrar diciendo que estas tendencias se dan de dos formas, donde los perpetradores toman un sitio web legitimo o registran su propio nombre de dominio. Una de las últimas tendencias no es registrar el nombre de dominio si no era un revendedor que utiliza bitcoin y también utiliza servicios de privacidad y representación. Entonces si bien los revendedores dentro de las responsabilidades de los registradores y los registros, los revendedores no tienen una relación contractual directa con la ICANN, lo que estamos viendo es una tendencia interesante en la periferia que está afectando a algunas de las tendencias de ciberdelitos más importantes que vemos.

Ahora sí que termino mi tiempo. Le doy la palabra al siguiente orador.

BOBBY FLAIM: Antes de pasar, cuando estamos hablando de las amenazas del DNS y el uso del bitcoin, ¿cuál cree que puede ser la solución a algunas de estas tendencias?

DREW BAGLEY: Bueno, creo que una de las principales soluciones seria la mitigación de este uso indebido. No tengo tiempo, pero incluso cuando no tenemos buenos datos para trabajar y puede haber credenciales falsas y seguimos hablando de privacidad y representación, estas pueden escalar igual que otros y a veces se puede utilizar la misma dirección de correo electrónico una vez tras otra. Entonces tenemos que darles a los proveedores de servicios de representación y proxy datos para que ellos puedan ver y desenmascarar qué es lo que pasa. También ver cuáles son los datos maliciosos como para no utilizar estas credenciales maliciosas vez tras vez con estos mismos proveedores de servicios de representación.

BOBBY FLAIM: Ahora va a hablar Allen Grogan y también Carlos Álvarez. Me parece que ustedes lo van a hacer en forma consecutiva. Así que, Allen, te doy la palabra.

ALLEN GROGAN: Gracias. Bueno, el departamento de cumplimiento de ICANN de alto nivel que trabaja con los registradores y los registros realmente tiene distintas formas de abuso, como es la primera reunión de la ICANN. Después de la transición voy a delinear el marco de referencia porque esto tiene que ver con el uso indebido y en realidad voy después a responder las preguntas.

Según el nuevo estatuto existe una prohibición de la ICANN para actuar fuera de su misión. Ustedes pueden revisar la misión, pero en términos simples dice que tiene una naturaleza técnica y que se relaciona con la asignación de los nombres y facilitar el DNS y el sistema del servidor raíz del DNS. Utilizar los identificadores únicos de internet o el contenido de esos proveedores de servicio y un reconocimiento de que no existe una regulación, pero yo digo que cuando hacemos valer los contratos existentes y cuando hablamos de los derechos adquiridos, es decir, estamos hablando de anteriores a 2016 o los contratos que tienen la misma forma que fueron celebrados después de esa fecha. Estamos hablando de la renovación de esos contratos.

En las próximas imágenes muestro varias disposiciones que están en los contratos con las partes con contrato que tienen que ver con el uso indebido y al pensar en esto y cuál es la función de la ICANN para combatir el uso indebido hay que recordar que sean cual sean las acciones dentro del alcance del estatuto todo tiene que estar dentro de estas disposiciones con controles.

Ahora le voy a ceder la palabra a Carlos para que siga hablando.

CARLOS ALVAREZ: Gracias. Como miembro del equipo de SSR (seguridad, estabilidad y flexibilidad de internet), hablamos con la comunidad operativa y no estamos concentrados en las partes contractuales, sino que hablamos de una cooperación voluntaria. Y nos concentramos específicamente en las actividades maliciosas que tienen que ver con botnets, el control de comando y phising.

Lo que no está en esta categoría esta fuera de nuestro alcance. No hacemos nada que tenga que ver con marcas comerciales ni con cosas corporativas. Quiero que esto quede claro.

Me voy a concentrar rápidamente en algunas de las cosas que hacemos. Son algunas de las cosas que hacemos y me parece que vale la pena mencionarlas acá. Actualmente le damos capacitación a las unidades de ciberdelito de todas las entidades encargadas de aplicación de la ley porque a través de todo el mundo todas las semanas hay alguien que capacita a los policías de los aspectos fundamentales del DNS a una investigación un poco más profunda sobre temas que tienen que ver con las amenazas al sistema del DNS o nombres de dominio como tal.

Tenemos por ejemplo el DOJ, que es el departamento de justicia en los EEUU, también el Medio Oriente, tenemos asociaciones también con la OEA. Dentro de los estados americanos también

hemos celebrado reuniones en Perú, varias veces en Costa Rica, y también tenemos algunos ejemplos para dar operación sobre el trabajo que hacemos en la aplicación de la ley en diferentes formas.

Les brindamos asesoramiento para llegar respecto de las investigaciones en las que están trabajando y además respondemos preguntas sobre cómo funciona el DNS. A veces ellos no saben cómo seguir con el DNS y entonces les explicamos de qué se trata el DNS y cómo tienen que seguir adelante con las investigaciones. Tienen que entender cuál es el marco contractual de la ICANN, actualmente es el RAA, para sacar las dudas sobre las expectativas, qué cosas pueden utilizar para presentar informes de uso indebido a los registradores. También los ayudamos y también a OpSec, como lo llamamos nosotros, cuando presentan pedidos de IRS. Y eso tiene que ver con el proceso de la ICANN, que es el que se llama un pedido de seguridad de registro acelerado. Entonces le damos ejemplos para lo que se llaman Cryptolocker y take-down. Y también les damos asesoramiento al personal y a la comunidad. Actualmente tenemos como ejemplo la especificación 11 y el marco de seguridad de registro.

Si alguno de ustedes tiene preguntas respecto de los temas del SSR, acá estamos para responderlas. Algunos de los desafíos que tenemos… Y me queda 1 solo minuto, que la verdad no es

mucho tiempo. Vemos que los registradores y registros tienen diferentes sistemas, diferentes implementaciones de procesos, diferentes disponibilidad de recursos y diferentes niveles de conocimientos específicos. También vemos la gente en el área de seguridad a veces reportan un uso indebido que no puede ser claro, que no brinda demasiada información. A veces también sabemos que no existe una normalización para informar el uso indebido, lo que hace que todo sea más difícil para los registradores y también para quienes están encargados de aplicar la ley. También vemos que hay una falta de comprensión en las disposiciones contrarias al uso indebido tanto en quienes presentan las quejas como en los registradores. Esto lo hemos visto y ha sucedido en la práctica.

También hay otras cosas que podemos mencionar y que no tenemos términos de servicios o políticas aceptables entre todos los registradores que sean uniformes. Algunas son más exigentes y algunas son más livianas con sus registros o registradores y con los registratarios. No tenemos una uniformidad en el caso de los términos de servicios. Y también existe la complicación para incluir datos la investigación.

En cuanto a las aspiraciones, esperamos tener una definición más clara de qué constituye un uso indebido del DNS. Quizás el PSWG y otras partes de las comunidades nos podrían ayudar a definirlo mejor, de forma que tenga que guardar coherencia con

el modelo de la ICANN. La investigación de la normalización de los procesos para informar usos indebidos haría que la vida fuera más fácil para quienes presentan la queja como para los organismos encargados de aplicar la ley. Muchas gracias.

BOBBY FLAIM: Gracias, Carlos. Quería que Drew volviera a hablar porque Drew se va a ir. Usted quería compartir también algo con nosotros con respecto a las soluciones de mitigación de uso indebido del DNS.

ALLEN GROGAN: Gracias, Bobby. Quería enfatizar que más allá de las función que puede desempeñar la ICANN y de las funciones de las autoridades de aplicación de la ley y de otras partes, es importante que los registros y los registradores compartan datos entre sí, ya sea de forma directa o a través de otras organizaciones de confianza, organizaciones sin fines de lucro, los nombres de dominio suspendidos, y esos datos a los que yo me refería. Es importante que toda esa información se comparta en toda la comunidad porque solo compartiendo esos datos será posible realmente hacer que los malos puedan hacer menos daño e identificar su patrón y usarlos en contra de ellos.

Entonces el mensaje en cuanto a la función que pueden desempeñar las diferentes partes, creo que es importante que la

comunidad se mire a sí misma y vea qué puede hacer con los datos con los que cuenta para actuar por el bien y para ayudarse entre todos y hacer que el internet sea un poco más segura a través de la cooperación.

BOBBY FLAIM: Gracias. Un par de preguntas para Allen y Carlos. Ahora que estamos entrando en el mundo posIANA, ¿piensan que va a haber más presión en términos de autocorrección, aplicación, medidas de seguridad proactivas?

ALLEN GROGAN: ¿Podría explicar un poco mejor su pregunta? No estoy seguro de a que se refiere.

BOBBY FLAIM: Ahora que estamos en el mundo post IANA, en el mundo de ICANN independiente, ¿piensan que la comunidad va a mirar más a lo que hacen ustedes? ¿Va a pedir que ustedes hagan más, más autocorrección, más autorregulación, más aplicación de los contratos, dado que no hay, entre comillas, supervisión?

ALLEN GROGAN: Lo que yo creo que va a pasar en el nuevo mundo post IANA es que habrá mucho debate en la comunidad acerca de cuál es la

función de la ICANN en cuanto a combatir el uso indebido. No sé muy bien hacia donde nos va a llevar ese debate en la comunidad de diferentes unidades constitutivas dentro de la organización de la ICANN, que tienen diferentes puntos de vista con respecto a qué es lo que está dentro del ámbito de la ICANN y que es lo que esta fuera del ámbito de la ICANN. El mundo de la post IANA habrá debates acerca de la misión, los estatutos y en la diapositiva que les mostré hacemos referencia a esto. Supongo que habrá mucho debate. Algunos harán presión para que hagamos más, otros harán presión para que hagamos menos.

BOBBY FLAIM: Carlos.

CARLOS ALVAREZ: Nuestros colegas en la comunidad de seguridad de aplicación de la ley nos dicen que esperan que la ICANN sea más activa con respecto a las actividades contra el uso indebido. Esperan que la comunidad de la ICANN enfrente este problema y actúe contra el uso indebido. Eso es lo que diría yo.

BOBBY FLAIM: Gracias. Ahora está Statton y Brian, quienes van a hablar acerca de las mejores prácticas de los registros y estrategia de mitigación de DNS. Statton, ¿usted es el primero?

Brian. Pido disculpas.

BRIAN CIMBOLIC: Del programa antiabuso. Nuestro programa comienza y finaliza con una política antiuso indebido, que cubre el abuso técnico del DNS, junto con explotación infantil y junto con nuestro proveedor de back-end (Afilias). Tenemos medidas proactivas y reactivas para tratar de mitigar el uso indebido.

En cuanto a las medidas reactivas, la primera línea de defensa es nuestro alias de abuso o uso indebido que opera 365 días por año, ya sea yo o nuestro asesor legal general manejamos directamente los casos y consultas de uso indebido. En general si ocurre algo, si nos derivan un caso en horas hábiles, iniciamos la investigación a la hora o dentro de las 2 horas o respondemos diciendo estamos llevando a cabo la política. Si es fuera del horario hábil podemos llegar a tardar de 8 a 12 horas.

En general las consultas llegan a través de usuarios finales, autoridades de aplicación de la ley o derivaciones de organizaciones. La mayoría de las de usuarios finales en general no constituye un uso indebido. Piensa estado de registro o

registradores nos piden que actuemos, pero nuestro aspecto no está dentro de nuestras políticas de uso indebido. Ahora cuando la gente sí nos deriva un caso de uso indebido, en general spaming o phising, también recibimos de fuentes de la industria notificaciones acerca del malware.

Cuando recibimos un caso real de uso indebido, en general lo que hacemos es en primer lugar contar con los registradores. Y lo hacemos porque por un lado somos sensibles a la relación que tiene el registrador con su cliente. Y en segundo lugar porque así el registrador tiene la oportunidad de conectarse directamente con el registratario y hay una explicación quizás legítima con respecto a por qué ocurre algo. Entonces los registradores con frecuencia actúan con las deliberaciones y los casos que les enviamos. Ahora cuando llevamos un caso al registrador, decimos: en caso de que usted no actúe en forma satisfactoria, vamos a tomar alguna medida de acuerdo con nuestra política en contra del uso indebido. Si lo hacemos suspendemos el dominio en general. Suspendemos el dominio porque las medidas tomadas no son efectivas. Una vez que se elimina el nombre de dominio, al día siguiente es registrado por la misma persona para el mismo propósito de uso indebido.

Cuando recibimos casos de aplicación de la ley, siempre reciben la máxima atención de PIR. Trabajamos en estrecho contacto con las a autoridades de aplicación de la ley y tratamos de

desarrollar juntos un lenguaje para una orden para que el tribunal pueda emitir una orden de acuerdo con el caso. También implementamos algunas medidas proactivas para mitigar los casos de uso indebido del DNS. Esta es un área en la que trabajamos en estrecho contacto con nuestro proveedor de back-end, Afilias.

Implementamos sistemas para detectar patrones de registración inusual. Por ejemplo si un registrador tiene un pico significativo en la registraciones, eso hace que le prestemos un poco más de atención. No significa que las registraciones necesariamente sean de uso indebido, quizás simplemente fue un día de gran actividad. Pero eso nos da un motivo para prestar más atención y realizar una investigación para ver si los dominios están recibiendo spam u otro tipo de uso indebido.

También recibimos informes todos los días con respecto a las registraciones del día anterior y hacemos referencias cruzadas de la información. Esto una vez más no significa, en caso de que haya una coincidencia, que sea un caso de uso indebido necesariamente, pero sí nos da un motivo para analizar en mayor detalle las registraciones y ver si está pasando algo extraño. En caso de que encontremos un uso indebido posible o probable, en general seguimos los mismos pasos que seguimos en el caso de las medidas reactivas. Contactamos con los registrados, le damos la oportunidad de resolver o contactarse

con el registratario. Y si no actúa, en ese caso nosotros suspendemos el nombre de dominio.

Habiendo dicho esto, le voy a dar la palabra a Statton.

STATTON HAMMOCK: Namasté a todos. Gracias por estar acá. Soy Statton Hammock de Rightside. Para aquellos que no saben que es Rightside es una empresa de servicios de dominio con integración vertical. Somos registro y registrador. El registro opera con 4 nombres de dominio de alto nivel y somos unos registradores más grandes también y vendemos nombres de dominio de todo tipo.

Como vicepresidente de políticas y asuntos legales y comerciales, vemos muchos casos diferentes de uso abusivo del lado de registros y registradores. Y es un placer para mí conocer con ustedes algunos de los datos para que tengan una idea de lo que nosotros vemos diariamente, especialmente con respecto a los nuevos gTLD.

En primer lugar cuando hablamos de uso indebido, quiero dejar en claro que estoy hablando que cuando hablo de antiuso indebido hablo de diferentes cosas. Algunas, que se exigen a los registros, de acuerdo con estos contratos con la ICANN, y son los mecanismos de protección de derechos e implementación, que fueron diseñados y desarrollados durante la génesis del

programa de nuevos gTLD y que incluye el periodo de reclamos URS y UDRP, proceso de resolución de conflictos por delegación. Además como registro también tenemos que incluir algunos compromisos de interés público que eran exigidos. Algunos provenían de la comunidad de múltiples partes interesadas. Otros provenían de asesoramiento del GAC y otros lugares. Y eso también se implementaron en nuestro contrato de registros. Y luego tenemos lo que yo denomino los esfuerzos más voluntarios liderados por la industria, que no son exigidos por contratos y que los registros y registradores emprendieron por su cuenta para combatir ciertas actividades en internet.

Algunos registros, incluyendo a Rightside, ofrecen listas de bloqueo de protección para proteger a los titulares de dominios y dueños de marcas comerciales para que no tengan que gastar dinero en todos los diferentes TLD. Procesos de reclamos donde extendemos el periodo de notificaciones para que los dueños de marcas comerciales puedan realizar registraciones y también otros proyectos que incluyen trabajar para crear un marco de seguridad. Y los miembros de partes interesadas de registros ahora están definiendo distintos procesos y distintas identificaciones de uso indebido. Es más, fuera de estos proyectos de esfuerzos voluntarios de la comunidad de la ICANN hay registros y registradores individuales que llevan adelante procesos para combatir distintas formas de uso indebido.

Trabajamos para alguno de estos grupos para luchar contra el abuso infantil a nivel internacional, contenido, protegido, iniciativas a través de la asociación de dominios, de la asociación profesional que representa en la industria de nombres de dominios y que trabaja con las mejores prácticas y principios para luchar contra cosas o actividades ilegales, ataques a la seguridad y otras formas de uso indebido.

Este es el panorama general de los esfuerzos antiuso indebido. Desde el punto de vista de Rightside, tenemos más de medio millón de nombres de dominios registrados en nuestros 4 gTLD. Tenemos 4 fuentes de informes que usamos para mostrar diariamente. Tenemos 3 nombres de dominios de alto nivel muy regulados. Cuando digo muy regulados, me refiero a que son nombres que el GAC considera muy sensibles, como .lawyer, .attorney, .dentist. Tuvimos cero procedimientos de resolución de disputas para el compromiso de interés público. Cero procedimientos para asociación de conflictos sunrise. 52 procedimientos de URS iniciados.

Los datos de Rightside no son necesariamente indicativos de la actividad de todos los registros, pero vemos que coincide con lo que se está diciendo el departamento de cumplimiento de la ICANN en términos de uso indebido. En general el phising, malware y spam, y muy poco del lado de contenido o de los otros tipos de reclamos que pensamos que serían el caso en los

dominios de alto nivel. En respuesta a estos reclamos, los registros toman algunas medidas, los registradores también. Y finalmente una vez más para repetir esto, considerando los nombres de dominios registrados, vemos un bajo nivel de uso indebido.

En esta última diapositiva vemos los casos de Rightside y los TLD de mi colega Brian y decidimos compartir esta información con ustedes. Muchas gracias por su atención.

BOBBY FLAIM: Gracias, Statton y Brian. Quería hacerles una pregunta colectiva. ¿Ustedes comparten en forma colectiva información sobre uso indebido? Cuando ven actores o tendencias en particular, ¿comparten esa información?

STATTON HAMMOCK: Sí, en forma informal. En genera a nivel de registrador, mi equipo de cumplimiento está dispuesto a compartir con otros registradores la información que detectan de malos actores y vemos un actor que está tratando de secuestrar nombres o actividades maliciosas, compartirnos esa información con distintos registradores para que ellos también estén al tanto de lo que está haciendo este actor. No hay nada formal. Lo hacemos simplemente como buena práctica.

BOBBY FLAIM: Gracias, Statton. Ahora tenemos a Giovanni Seppia. Perdón. Por cómo estamos sentados no veo a todos. Hay una pregunta del público.

ORADOR DESCONOCIDO: [Nabil]. Soy becario de ICANN. Tengo una pregunta con respecto a listas negras. Una pregunta de PIR. Usted dice que escanean los informes a través de distintas listas de bloqueo y listas negras. ¿Cómo recopilan esas fuentes?

BRIAN CIMBOLIC: Gracias por la pregunta. Hay varias listas que están disponibles para todo el mundo. Muchas son listas por suscripción. Con frecuencia hay cierta sensibilidad y confidencialidad con respecto a estas listas. En general al derivar la información a un registrador, este se contacta con el registratario. Si el registratario considera que fue incluido de forma adecuada en la lista, tiene la oportunidad de decir por qué nuestra conclusión de que fue uso indebido está equivocada.

ORADOR DESCONOCIDO: Voy a suponer que estas listas, estas fuentes en general, son verificadas y no son listas que simplemente circulan por internet.

BRIAN CIMBOLIC: Sí, por supuesto.

BOBBY FLAIM: Vamos a recibir una pregunta más, pero si hay más preguntas las vamos a dejar para el final hasta que hayan terminado todas las presentaciones, así nos aseguramos de que alcance el tiempo para todas las presentaciones. Creo que tenemos 30 o 45 minutos designados para preguntas y respuestas al final.

KIRAN MALANCHARUVIL: Kiran Malancharuvil de MarkMonitor. No me gusta mucho esta diapositiva que muestra y les voy a explicar por qué. Creo que no es necesariamente justo decir que es debido a que no denunciamos los casos de uso indebido que esto no esté ocurriendo debido a que tenemos políticas de uso indebido muy estrechas. Y ustedes esperan que la forma que interpretamos el uso indebido sea la misma. El hecho de que no les derivemos los casos a ustedes no significa que no los haya. Ustedes deberían ayudarnos a entender cuántos nombres de dominios se denuncian en todo tipo de canales, cumplimiento contractual

de la ICANN, registradores, ISP, asociados con sus registros. Creo que serían datos mucho mejor para nosotros, que nos permitirían entender qué clase de uso indebido se está denunciando, y no solamente lo que se les denuncia a ustedes como registro.

STATTON HAMMOCK: Los datos que les mostré muestran informes de uso indebido de todo tipo de fuentes incluyendo la ICANN, en nuestro caso. Por lo tanto, provienen de todas partes. Todo lo que recibimos directamente de los registros, de nuestro sitio web de sitio indebido o el departamento de cumplimiento de la ICANN. Todo esto está reflejado ahí.

BOBBY FLAIM: Pasamos a Giovanni.

GIOVANNI SEPPIA: Gracias, Bobby, por esta oportunidad. Pertenezco a EURid, que es el operador de .eu.

En esta primera imagen lo que quiero resaltar es, desde la perspectiva administrativa y técnica, el .eu es un cTLD. Es por eso que pertenecemos a la familia de los sTLD y realmente estamos muy regulados. Somos altamente regulados. Tenemos

mucha regulación. La primera se hizo en el 2002 y la segunda, que tiene que ver con las normas de políticas públicas, del 2004. Estas dos regulaciones de la comunidad europea tiene una disposición básica donde dice que el .eu es un nombre de dominio que solo puede ser registrado por residentes de la Unión Europea o algún país dentro del área económica europea. Entonces nosotros atendemos a un mercado de 31 países y somos un poco más de 3,8 millones de registradores de uso de dominio bajo .eu y el primero de junio de este año del .eu en cirílico, que es muy importante para nosotros destacar este aspecto multilingüe de nuestro servicio.

Hemos implementado distintas medidas entonces para proteger nuestros nombres de dominio. desde la perspectiva publica tenemos entonces DNSSEC, registry lock, un paquete de homoglyph, que es algo que surgió hace unos años para que entonces los IDN están empaquetados por así decirlo. Entonces no es posible registrar nombres de dominio que sean parecidos para evitar probables problemas de nombres de dominios que pueden parecer muy similares entre registradores. También como tenemos una política de macheos de script para que los nombres latinos y los nombres en cirílico puedan tener una coincidencia o macheo dentro de todo lo que es el entorno de .eu.

Lo que estamos implementando desde hace unos años es lo que llamamos el plan de calidad del whois. La autoridad de EURid que es quien gestiona el .eu está limitada por estas dos reglamentaciones que mencioné anteriormente. Pensamos qué es lo que podíamos hacer en el marco de estas dos reglamentaciones. En general tomamos una acción cuando recibimos una queja sobre un posible abuso que tiene que ver con un nombre con .eu y tenemos cooperación con nuestros registradores acreditados. De hecho, este plan de calidad de whois fue desarrollado junto con los registradores y le da a EURid mucho asesoramiento sobre cómo seguir adelante con este plan, como implementar este plan de calidad.

Verificamos los datos de registración y verificamos estos datos de registración diariamente. Los datos de registración se verifican directamente a través de EURid o cuando hay un pedido de un tercero. Algunos de ellos son organismos encargados de la aplicación de la ley. En lo que tiene que ver con la verificación de la dirección, solo operamos con los residentes de los 31 países. Entonces lo hacemos verificando las bases de datos de terceros o utilizando Google Maps.

Les voy a dar algunas estadísticas. A fines de 2015 habíamos eliminado más de 30.000 nombres de dominio porque no cumplían con los criterios de residencia establecidos en las dos reglamentaciones que mencioné. Acá tenemos una lista de las

distintas autoridades que están basadas en Bélgica. Ustedes saben que en la Unión Europea tenemos un memorando de entendimiento con CERT y algunos de mis colegas en este panel señalaron que necesitábamos mucha educación para decirles qué es lo que podemos hacer basándonos en nuestra reglamentación de políticas de seguridad pública y tenemos que actuar en cooperación con ellos o la red de registradores acreditados.

En el siguiente límite tenemos un sistema de alerta temprano para prevención del uso indebido. Es muy interesante porque es un análisis que estamos realizando en la actualidad en cooperación con la universidad de [incomprensible] para evitar el uso indebido, así como demorar la delegación de las solicitudes de registración de algunos nombres de dominio que pueden llegar a un uso indebido. También tenemos un foco especial en los niños para utilizar el principio de prevención y no tener que solucionar las cosas después de la registración.

Voy a responder a las preguntas que tengan que hacer. Muchas gracias.

BOBBY FLAIM: Tengo una pregunta. Parece que ustedes están haciendo mucha mitigación del uso indebido y antiuso indebido. ¿Cómo es

posible cuantificar los recursos que utilizan para hacer lo que hacen?

GIOVANNI SEPPIA: Es una buena pregunta porque de hecho lo que hemos hecho durante estos años es que hemos decidido hace unos años tener el punto .eu y promoverlo como un nombre de dominio de calidad. Entonces invertimos mucha calidad para que sea un dominio de calidad e incluye todo lo que nosotros estamos haciendo para mitigar el uso indebido y prevenirlo. En cuanto a recursos, en departamento jurídico tiene 3 personas. dos de ellas se dedican totalmente a la verificación del whois, a este plan de calidad del whois. Y mi equipo… Yo soy también gerente de asuntos externos. Mi equipo cubre todo los países de la Unión Europea y junto con el equipo jurídico analizan, tanto los registros como la excelente cooperación que tenemos con los registradores.

En el último año tuvimos ejemplos de acciones que realizaron los registradores acreditados. Algunos de los revendedores estaban haciendo un uso indebido en nuestro caso. Entonces hubo acciones que llevaron a cabo a la rescisión del contrato porque el revendedor estaba haciendo un uso indebido de todo el sistema de registración. Es uno de los elementos clave que tenemos en esta lucha contra el uso indebido y la prevención.

BOBBY FLAIM: Tengo otra pregunta. Dijeron que trabajaban con los registradores. ¿Cómo hacen ese trabajo? ¿Ven cosas o utilizan disparadores para remitirse a los registradores? ¿Cómo hacen?

GIOVANNI SEPPIA: Nosotros, cuando hay un ataque a un nombre de dominio, utilizamos los datos de registración con la dirección de correo electrónico o el nombre del registratario o algún otro dato del registratario. Cuando nos parece sospechoso le enviamos un correo electrónico al registratario para la dirección de correo electrónico que suministró y copiamos al registrador. La mayor parte de las veces, antes de eliminar ese nombre de dominio, hacemos una coordinación con el registrador para ver que el registrador también tiene la posibilidad de hacer un coordinador con el registratario porque ellos son el canal realmente para la registración del .eu. Como dije en el pasado, muchos de ellos se negaban porque significaba una carga extra. Necesitaban recursos extra. Pero ahora puedo decir que tenemos una gran cooperación con todos los registradores. No pudo hablar de ningún registrador que no nos haya ayudado en este tipo de plan de calidad de whois.

BOBBY FLAIM: Muchas gracias. Vamos a pasar ahora a Michele.

MICHELE NEYLON: Soy Michele Neylon. Soy de registradores. Proveemos servicios de alojamiento.

Voy a hablar brevemente de algunos de los desafíos que enfrentan los registradores y otros proveedores de servicios de internet porque se ha hablado de los datos que tienen algunos de los desafíos que enfrentan desde nuestro extremo, como registradores. También proveemos alojamiento, ISP y además uno de los problemas que tenemos tiene que ver con la presentación de informes en sí mismos, con las denuncias. En los últimos años han existido distintas iniciativas en distintas partes de las comunidades de seguridad para tratar de mejorar la calidad de las denuncias, pero realmente no hemos llegado bien. Es decir, no hay normas en este momento que hayan sido implementadas. Y hay gente que se queja de que no hay normas en cuanto tienen que ver con las respuestas también.

Entonces vamos a dar algunas pautas de cómo hacer las denuncias. Cuál es el tipo de uso indebido que ven. Nos tienen que dar ejemplos claros de cuál es el uso indebido. Cuando yo miré hoy lo que eran los abusos indebidos en los informes solo dicen que el dominio X hace un uso indebido. Es muy útil realmente porque voy a tratar de tener que averiguar cuál es el uso indebido exactamente. El resto es cuando estamos

hablando del uso indebido en esta sección, lo estamos mirando en términos de tratar de estrechar el alcance porque, como proveedor de alojamiento, no vamos a terminar en una situación donde alguien nos pide que seamos juez, parte y ejecutor. Tenemos que tener una guía clara de qué es lo que tenemos que hacer, cuál es nuestro mandato, qué se espera que hagamos.

En el caso de un software malicioso, botnet, todo ese tipo de cosas en términos generales la mayor parte de nosotros no queremos tener ese tipo de contenido dentro del servidor de nombres de dominios que tiene que ver con nosotros. Los nombres de dominio, si nosotros estamos actuando como registradores no queremos una herramienta donde yo diga "bueno, puedo sacar directamente el nombre de dominio o puedo sacar parte del nombre de dominio". "no quiero matarlo totalmente o sí quiero hacerlo con todos los servicios asociados". Tiene que estar en claro lo que podemos hacer nosotros y qué piden que hagamos nosotros. Entender cuáles son nuestras limitaciones.

Acá en esta reunión se ha hablado mucho de las revisiones que se están realizando y veo que hay miembros del equipo de revisión del CCT acá. Están haciendo una revisión que incluye el uso indebido. Espero que nos puedan dar entonces datos concretos porque son los datos que nos ayudan a nosotros.

Ahora ¿existe una relación entre los nombres de dominios en determinadas extensiones y su uso y lo que tiene que ver con las estrategias de fijación de precios? Porque los datos reales nos van a ayudar y no las teorías.

También puedo mencionar que en última instancia, como registradores, queremos trabajar con el resto de la comunidad, pero tenemos que entender que estamos limitados en lo que podemos hacer. Entonces les pedimos a ustedes que nos den más detalles. No porque queremos ser difíciles, sino porque queremos entender de qué se quieren quejar y cuáles son los problemas.

No tengo mucho más que decir. En última instancia, creo que desde nuestra perspectiva tiene que ver con la calidad de la denuncia en sí misma. Si la comunidad puede mejorar estas denuncias nos va a ayudar entonces a avanzar con aspectos más positivos. Gracias.

BOBBY FLAIM: Tengo una pregunta. Has hablado de la especificidad para actuar. ¿Hay algún ejemplo que nos puedas dar sobre seguridad operativa, alguna compañía o alguna unidad constitutiva especifica que pueda proveer esos datos específicos que pueda proveer esos datos específicos que les ayude a actuar?

MICHELE NEYLON: Claro que sí, Bobby. Porque por ejemplo con un organismo encargado de aplicar la ley quizás quieren que quien alberga ese nombre de dominio pueda tomar alguna acción o algún registrador puede tomar otra acción más allá de suspender o eliminar el nombre en el DNS. Entonces creo que tiene que ver con cada caso en particular, pero todo se relaciona con que en lugar de decirnos hay un problema y queremos que hagan esto, esto y esto. Por ejemplo, un tema común, quizás alguno otro lo mencionó, tiene que ver con la jurisdicción. Mi compañía es irlandesa y ustedes están en EEUU. Entonces si ustedes me envían algo conforme a la ley de EEUU, yo les voy a decir amablemente "no tengo nada que ver". Porque si es algo con lo que yo puedo actuar, está bien.

Pero por ejemplo me dicen DMCA. Como empresa irlandesa, no tengo nada que ver con el DMCA, sino que además no puedo actuar al respecto, lo que no significa que voy a ignorar la denuncia. Pero si esperan que tome una acción directa, no va a suceder eso. Entonces también sé que han estado hablando. Bertrand De La Chapelle habló de jurisdicción. Y creo que es un tema muy importante porque hay que ver cuál es la legislación real. Además, cuál es la acción que se espera porque cuanto más específica sea la denuncia, más fácil va a ser para nosotros tomar una determinación para saber. Tenemos suficiente

información para tomar una acción o necesitamos decir: "Bueno, está bien. Está perfecto, pero la verdad es que no es parte de nuestra jurisdicción. No está dentro de nuestra competencia. No tenemos suficientes detalles para hacer algo al respecto".

BOBBY FLAIM: Sí, sé que es un tema muy grande cuando estamos hablando de un uso indebido del DNS porque no estamos en tratados internacionales, en convenciones de delitos internacionales. Cuando hablamos del DNS sí que hablamos de conflictos de leyes y sé que también en EEUU podemos hablar de utilizar un tratamiento mutuo, pero sé que esto lleva tiempo y no se aplica en todas partes.

Quiero que Denise hable porque es la última en presentar. Después sí podemos tomar todas las preguntas si no le molesta, caballero.

DENISE MICHEL: Voy a señalar los desafíos que enfrentan las empresas en todo el mundo, así como los consumidores. Hay algunas empresas que tienen la misma dimensión de Facebook. No son muchos. Y nosotros hacemos mucho para proteger la seguridad de la internet. Los nombres de dominio son la fuente del uso indebido

y también son claves para intentar y prevenir estos ataques a la seguridad en la plataforma internacional.

Es un punto que a veces no se toma en cuenta. En la comunidad de la ICANN no están conscientes de ello, pero un dominio altamente cualificado es un número de dominio que tiene un nombre de dominio y un nombre de host. Entonces esto puede crecer en forma exponencial en la cantidad de URL que se puedan ver afectados. Cuando hablamos de esto que llamamos un FQDN. Esto puede causar un gran daño a los usuarios. No es lo mismo que tener nada más que un uso indebido de un único nombre de dominio. Entonces acá voy a mostrar en distintas imágenes una referencia con elementos clave que tienen que ver con el RAA, cosas que se pueden utilizar en las obligaciones contractuales y qué es lo que se puede utilizar para mitigar este uso indebido. Ustedes pueden ver acá en la transparencia de qué estoy hablando.

Ahora también proteger al usuario final es bueno para proteger el ecosistema del DNS, así como el negocio del registro de nombres de dominio. Quiero señalar algo que pasó en el mundo real. Hay dos dominios que se registraron comvideo.net y loginaccount.net. Realmente tenían todos los nombres de contacto y nombres de Facebook y acá pueden leer lo que paso. Fue registrado, se tomó toda esta información y se utilizó para registrar estos dos nombres de dominio. Esta toda esa

información de Facebook, incluso nuestra dirección de correo electrónico, excepto los nombres de los servidores.

Estos dos nombres de dominio tenían phising, software malicioso, y afectaron a 30.000 usuarios finales. Fue detectado rápidamente por Facebook. Lo bloqueamos y además lo informamos al registrador, así como al equipo de cumplimiento de la ICANN. El registrador onlineNIC no verificó la registración de estos dos nombres de registros con nosotros. Entonces hicimos una queja, tratamos de hablar con el registratario varias veces, también hablamos con el departamento de cumplimiento de la ICANN y tratamos de hablar con el registrador, y dentro de 24 horas no hubo un cambio ni en los registros del whois ni en los nombres de dominio. Nos llevó dos meses para cancelar estos dos nombres de dominio. Esto es a pesar del reconocimiento que había hecho el registrador de que el whois era fraudulento.

Entonces lo que aprendimos de esto nada más que este único ejemplo que tuvimos en la vida real es que el sistema falla si el registrador no hace en el momento de la registración la verificación correcta. Falla y fracasa si no se presta atención a los informes de uso indebido. Y si el sistema fallase, los registradores no pueden tomar las acciones necesarias según el RAA. Y en esta instancia también insistimos que era el mismo aprobador de la cuenta quien la había usado con objetivos

fraudulentos. El sistema fracasa si el departamento de cumplimiento de la ICANN no puede dar los resultado y toma lo que llama un esfuerzo de cooperación con un registración no cumple. Esto entre comillas.

Entonces entendemos que no todo puede captarse y que estos procedimientos para evitar el uso indebido no son perfectos, pero nuestra comunidad debe exigir esto. Todas las partes que participan tienen que pedir estas políticas y procedimientos para evitar el uso indebido. Se detectaron fallas, pero por ejemplo no debería llevar dos meses para sacar de circulación a quien intenta realizar una registración fraudulenta de un nombre de dominio. La ICANN necesita evitar esto y tener procedimientos habituales y más rápidos. No queremos crear la rueda nuevamente, pero tenemos la disposiciones contractuales y deben ser utilizadas por la mayor parte de los registros y registradores, muchos de los que están sentados en esta mesa. Y creo que debemos implementarlos a todos.

BOBBY FLAIM: Gracias, Denise. Tenemos 12 minutos para preguntas. Les pido disculpas. Peter, es el primero. Sé que tiene una pregunta. Si alguien más tiene una pregunta, por favor háganla. Tenemos hasta las 3 de la tarde.

PETER VAN ROSTE: Gracias, Bobby. Buenas tardes a todos. Soy Peter, gerente general de CENTR, que es la organización de los ccTLD europeos.

Quería responder a un punto que plantó Michele en cuanto a que aparentemente no se entienden cuáles son los factores diferentes que aumentan o disminuyen el uso indebido de determinados dominios. Hicimos un estudio en CENTR hace un año aproximadamente. El resumen general disponible se lo vamos a enviar por twitter. Pueden compartirlo. Además sé que algunos miembros de CENTR hicieron investigaciones de algunos factores específicos. No sé si esa información ya es pública, pero sé que tienen la intención de ponerla a disposición del público en general. Ese es un punto. Espero que esto les sirva.

En segundo lugar, crucial para este debate, al menos para los europeos, es el hecho de que el debate haya tenido lugar en el marco del mercado digital. Hay una propuesta para ayudar a proteger a los consumidores europeos cerrando dominios, deshabilitando temporalmente el acceso. El problema en ese caso, y esto es algo que a mí me pareció muy confuso en este panel también, es la falta de un vocabulario común para definir de qué estamos hablando, especialmente con respecto de los gobiernos, aplicación de la ley. En Europa sentimos la necesidad de empezar a armonizar y estandarizar eso. Yo les sugiero este

panel que vea así como comunidad más amplia, no solamente nosotros los ccTLD europeos, sino la comunidad más amplia quizás podría enfrentar este problema. No es fácil pero es algo que vamos a tener que enfrentar y resolver tarde o temprano. Gracias.

BOBBY FLAIM: Gracias. ¿Alguien tiene algún comentario al respecto?

MICHELE NEYLON: Peter, esos datos estadísticos son muy útiles. El problema por supuesto es que yo hablaba principalmente en relación con los gTLD, no con los ccTLD, pero gracias. Estoy 100% de acuerdo, antes de que nadie lo diga, en cuanto a que son los CC y los G. son todos los dominios.

BOBBY FLAIM: Gracias.

MICHAEL PALAGE: ¿Hay alguien que tiene informes proporcionados por terceras organizaciones? Informes de uso indebido y de cumplimiento de los registradores.

ALLEN GROGAN: ¿Se refiere a informes comerciales?

MICHAEL PALAGE: Hice una solicitud recientemente tratando de identificar qué fuentes está utilizando la ICANN y simplemente quiero ver si el equipo de cumplimiento recibe algunos informes, la ICANN abduce confidencialidad y ese tipo de cosas. Simplemente quiero saber qué recursos tiene el equipo de seguridad, el personal del staff, para hacer su trabajo.

ALLEN GROGAN: No sé si puedo decir esto. El equipo contractual de la ICANN utiliza fuentes de terceras empresas. Quizás hay otro equipo que sí lo haga.

CARLOS ALVAREZ: ¿Se refiere a qué ocurre cuando alguien envía un informe de uso indebido? En ese caso hablan con el equipo contractual de la ICANN.

MICHAEL PALAGE: Quiero saber lo siguiente. Ayer Margie, en el grupo de CC, hablaba acerca de cómo van a tratar de llevar a cabo un análisis de uso indebido de los gTLD heredados y cómo van a llevar eso al mercado actual. Entonces si están llevando a cabo este análisis histórico versus lo que había antes y lo que había hoy.

Donde se están recopilando esos datos. Para poder hacer eso alguien tiene que haber recopilado esos datos.

CARLOS ALVAREZ: Creo que la pregunta es qué metodología están utilizando y qué fuentes de información están usando.

MICHAEL PALAGE: Como equipo SSR, ¿ustedes qué están haciendo? ¿Pueden compartir con nosotros qué informes usan o qué hacen ustedes para hacer su trabajo y qué comparten con el equipo de cumplimiento? ¿Ustedes simplemente operan en silos? Quizás la pregunta debería ser si hay algún tipo de comunicación.

CARLOS ALVAREZ: Nosotros no producimos informes de uso indebido. Esa no es nuestra función.

MICHAEL PALAGE: De acuerdo.

CARLOS ALVAREZ: Analizamos los datos, identificamos a los registradores que podrían estar registrando grandes cantidades de dominios que podrían considerarse maliciosos y compartimos la información

con el equipo de cumplimiento para que ellos lo incluyan en su proceso.

BOBBY FLAIM: Mike, quizás usted podría responder. Nos quedan pocos minutos, así que vamos a terminar aquí la fila de personas.

KIRAN MALANCHARUVIL: Kiran Malancharuvil de MarkMonitor. En primer lugar, fue una muy buena sesión. Gracias a todos.

Quisiera saber cuál fue la respuesta del señor Grogan con respecto a los puntos planteados por Denise de Facebook. Los registros de whois fraudulento son todo un tema. MarkMonitor y un grupo de dueños y titulares de marcas recientemente presentaron a la ICANN un informe que contenía miles de nombres de dominios registrados en punto feedback. Son casos en los que se usaron en forma maliciosa registros de whois y es similar al ejemplo que mencionó Facebook en su presentación hoy.

Entonces quisiera saber qué nos puede decir el señor Grogan al respecto. Me refiero a lo que planteó Denise con respecto a cómo, qué hace el departamento de cumplimiento con estos informes.

ALLEN GROGAN: Voy a decir dos cosas. En general no discutimos en los foros públicos los casos individuales. Y en segundo lugar, no estaba preparado sobre este tema. Por tanto no hice ninguna revisión de este caso o de los reclamos de MarkMonitor. No me preparé y por tanto no puedo responder a esta pregunta ahora.

KIRAN MALANCHARUVIL: Entonces ¿ustedes nunca vieron un registro de whois fraudulento?

ALLEN GROGAN: Esa no fue mi respuesta. Usted me preguntó sobre el reclamo que hizo Denise y yo no estoy preparado para responder esto porque no me preparé para hablar de este caso en esta sesión.

KIRAN MALANCHARUVIL: Gracias.

ORADOR DESCONOCIDO: Gracias al panel por la sesión informativa. Usted habló acerca de dos nombres de dominio que publicaron información fraudulenta. Y dijo usted, Denise, que llevó dos meses resolver esto. Quisiera decir que tenemos más de 100 registradores en .in. Hay un límite para tomar medidas. En caso de que no se

tomen medidas en 48 horas, esto se deriva a registro. Y en registro tienen que tomar una medida también en 48 horas. Entonces quisiera saber por qué ustedes no se comunicaron con el registro directamente y por qué esperaron dos meses.

DENISE MICHEL: Nosotros contactamos al registrador directamente, al registrador responsable de registrar ese dominio para tratar de que ese registrador cumpliera sus obligaciones en virtud del RAA y para que el dominio era el dominio que tenía toda la información. Y luego involucramos al equipo de cumplimiento de la ICANN ya que era su responsabilidad ocuparse de estos reclamos, en términos de que ese registrador debía cumplir con su obligación en virtud del RAA.

Este es el proceso y las obligaciones contractuales de los registradores. Para nosotros era importante seguir los procedimientos y las obligaciones establecidas por la ICANN y sus contratos con los registradores. Entendemos por supuesto que los registros, y esto lo subrayé en mi diapositiva, también tienen responsabilidades. Esto es algo tan prevalente en algunos registradores, este tipo de comportamiento, que nos parecía que era importante tener un registro y una responsabilidad completa para ver cuánto tiempo iba a llevar en este proceso dar de baja a estos dos dominios.

ORADOR DESCONOCIDO: Estoy levemente en desacuerdo con usted, Denise, en cuanto a que tuvieron que ir al equipo de cumplimiento de la ICANN. El registro, registrador o registratario, si el registrador no toma ninguna medida, ustedes deberían ir al registro. Esto obviamente hubiera resuelto el problema mucho más rápidamente.

MICHELE NEYLON: Quiero responder muy brevemente. Creo que Denise habla específicamente de los nombres de dominio .com. Y si como tal el registro no tiene los datos de whois para los dominios, quizás habría que reclamar. Si el registrador sigue recibiendo reclamos seguramente se va a enojar con el registrador y se los va a derivar. Pero en el caso de .com y .net, el registrador es el que controla los datos de whois y el registrador es el que puede hacer cambios también en datos del whois. No estoy tratando de defender a ningún registrador. Simplemente estoy estableciendo esta relación. Como el caso de .org o de los TLD de Rightside, en ese caso la relación seria levemente diferente, pero cuando hablamos de .com y .net los datos de whois residen a nivel de registrador solamente y no de registro.

ORADOR DESCONOCIDO: Solo quería decir que hay un acuerdo entre registro y registrador en caso de que el registrador no actúe y no tome ninguna medida.

BOBBY FLAIM: Si quieren pueden continuar esta conversación después. Sí, porque hay un par de preguntas más.

PAUL McGRADY: Durante 15 años tuve algo parecido a lo que mencionó Denise. Siempre pensé: bueno, le voy a ignorar una vez cada 15 años, y quizás tenga otro caso más. Pero nos pasó algo similar. Fue un problema con un par de nombres de dominio que contenían información perfecta del cliente y básicamente la misma información. Nosotros le escribimos al registrador, que no estaba en EEUU. Suspendieron el nombre de dominio, en lugar de eliminarlo. Y la ICANN nos dijo que una vez que un nombre de dominio es suspendido ya no se considera que sea un nombre de dominio real y esta era la política y la practica vigente.

Por supuesto, después de conservarlo, asegurarnos de que no se nos suspenda todos los días y seguimos agregando una situación que empeora en el sistema. Si esa es la práctica, creo que no es muy buena. Antes en las mejoras épocas de internet, esto podía existir pero es una brecha que quizás ICANN tendría

que llenar para ver que esto cambie porque cuando hay gente que está en los registros de whois que dice “no somos nosotros”, creo que es una situación muy clara. Gracias.

BOBBY FLAIM: La última pregunta. Nick.

NICK SHOREY: Nick Shorey del gobierno de Reino Unido. Quisiera decir simplemente que este fue muy buen debate, así que muchas gracias a todos por haber organizado esto. Gracias a todos los miembros del panel. Creo que surgieron algunas ideas muy interesantes, que quizás podríamos considerar de aquí en adelante en los próximos meses, en cuanto a la colaboración, cómo podemos mejorar la seguridad pública, los pedidos de seguridad pública. Michele habló de esto. Y me parece que en este debate sí tenemos que trabajar en cuanto a definir a qué nos referimos de uso indebido. Definitivamente esto es algo que tiene que pasar. Hay una diferencia entre proactivo y reactivo, en cuanto a respuesta frente al uso indebido. Hablamos en cuanto a mejorar la validación de whois. También hay medidas proactivas. Después tenemos la parte reactiva.

Quisiera saber si un registro… Como una persona que no sabe mucho dela parte técnica, quisiera saber si un registro ve un URL

completo por ejemplo en un caso en donde se hace un pedido de meses y ven que hay información que no es completa, ¿toman una medida? Quizás la próxima vez porque creo que eso habría que volver a hacerlo. Quizás sería bueno que la próxima vez hubiera un operador de red acá también, como una empresa de hosting por ejemplo. La ICANN siempre participa en estos debates difíciles. Siempre dice que no somos un regulador de contenido, etc. Entiendo ese punto de vista. Por tanto creo que sería bueno entender esta colaboración y quizás que viniera alguien que se dedicara solamente al hosting o un operador de red para tener un debate un poco más amplio, así que muchísimas gracias.

BOBBY FLAIM: Gracias. Creo que es muy buena idea. Tener un proveedor de hosting y operador de red en este panel. Michele.

MICHELE NEYLON: Nick, yo soy operador de red, proveedor de hosting y registrador. Por lo tanto, en cuanto a los URL y las consultas de URL creo que tenemos que darles un poco más cómo funciona el servicio de DNS. el registro no ve eso. El registro va a saber qué servidores de nombre está utilizando un nombre de dominio, pero no ve ningún pedido de DNS para un nombre de dominio en su registro básicamente. Lo que ve es el otro nivel que tiene

que ver con distintos niveles, pero con todo gusto puedo ayudarlos si necesitan ayuda.

CARLOS ALVAREZ: Quiero agregar un último punto, pues ya nos pasamos de nuestro horario. Hay aproximadamente 2.000 registradores que tenemos. Y aquellos que decidimos analizar son muy pocos. Los miramos con respecto a malware, control de botnet o phising. Eso dentro del ámbito de la ICANN. Hay muchos comentarios en el comité de seguridad de operaciones con respecto a los registradores. Spam no está dentro del ámbito de la ICANN. No se menciona el asesoramiento del GAC de 2013.

Por lo tanto, no podemos ocuparnos de eso. No podemos analizar esos registradores. Decidimos hacer la revisión de registrador por algún motivo en particular y se lo pasamos al departamento de cumplimiento. Y si el departamento de cumplimiento hace su trabajo y encuentra que no hubo ninguna falla, que no hubo ningún problema, no podemos hacer nada más. Si la comunidad piensa que vale la pena resolver el sistema de otra forma habría que plantearlo. Nosotros recibimos los tomates, pero es algo que la comunidad tiene que resolver y hablar desde el punto de vista de la seguridad. Gracias.

ALLEN GROGAN: Como dije antes, no estoy planteado para hablar de casos específicos. Pero mientras tanto mi equipo me envió un mensaje. Los nombres de dominio que son suspendidos frente a un primer caso de abuso o uso indebido quedan suspendidos durante todos esos dos meses.

BOBBY FLAIM: Un último comentario y después Alice va a hacer un resumen.

GIOVANNI SEPPIA: Simplemente quería decir que el debate de hoy fue muy importante y muy breve. Es muy importante el dialogo entre todas las partes interesadas. Cuando hablamos de uso indebido no se trata de culpar a ninguna de las partes involucrada. Es cuestión de comunicarnos y asegurarnos que todos entendamos qué podemos hacer todos juntos. Gracias.

DENISE MICHEL: Es importante entender que un whois fraudulento, un nombre utilizado para atacar a sus seres en internet, que tiene la información de mi compañía, no debería seguir estando en el dominio público en suspensión. No tengo duda de que si Rightside hubiera sido el registrador, o la empresa de Michele (Blacknight), esas registraciones se habrían verificado con el email. Si eso se les hubiera escapado, habrían pasado 24 horas

hasta que los desactivaran completamente. La suspensión no es una resolución en este caso. Nosotros planteamos esto como un problema. Esto no es un caso único. Tenemos muchos desafíos en este sentido y quisiera subrayar el hecho de que estoy muy contenta con el hecho de que el departamento de cumplimiento reciba prioridad por parte del nuevo CEO, ya que es un tema crítico para nosotros con respecto al uso indebido.

ALICE MUNYUA: Muchas gracias. En primer lugar quiero agradecerle a los panelistas porque ha sido realmente presentaciones muy importantes. Gracias por mantenerse a horario porque tuvimos poco horario. Gracias a todos por las preguntas. Supongo que va a haber muchas más preguntas, así que los panelistas tienen presentaciones mucho más detalladas. Quienes estén interesados en entender mucho más de los temas que se presentaron hoy en día tenemos las presentaciones disponibles en línea.

Muchas gracias, Bobby, por moderar la sesión. Y a Fabien por organizarla.

Ahora pasamos entonces a la siguiente. En 5 minutos vamos a pasar a la siguiente sesión que también tiene que ver con el whois y que también va a estar a cargo del PSWG. Gracias.

[FIN DE LA TRANSCRIPCIÓN]