ICANN69 | Reunión general anual virtual – Uso indebido del DNS
Martes, 20 de octubre de 2020 – 10:30 a 12:00 CEST

OZAN SAHIN: Vamos a comenzar con la sesión. Por favor, comiencen con la grabación. Hola y bienvenidos a la reunión sobre uso indebido del DNS. Mi nombre es Ozan Sahin. Soy el gerente de participación remota para esta sesión. Por favor, tengan en cuenta que esta sesión será grabada y cumple con las reglas de comportamiento esperado de esta sesión. Durante la sesión, los comentarios y preguntas solo se leerán si están presentadas en la ventana de Zoom. Se puede acceder a esta funcionalidad a través de la ventana de herramientas de Zoom. Yo leeré las preguntas y seré el moderador de la sesión.

Esta sesión incluye transcripción en tiempo real así como interpretación. Para seleccionar la transcripción en tiempo real, por favor, haga clic en la tecla de subtitulado que está en la barra de herramientas de Zoom. La interpretación para esta sesión incluye árabe, chino, inglés, francés, ruso y español. Se llevará a cabo utilizando Zoom y la plataforma de interpretación simultánea remota operada por Congress Rental Network. Los participantes podrán descargar la aplicación de Congress Rental Network de acuerdo con las instrucciones que están en el chat de Zoom y en el documento con los detalles de la reunión que está disponible en el sitio web de la reunión.

Si desean hablar, por favor, levanten la mano en la sala de Zoom y una vez que el facilitador de la sesión lo llame por su nombre, el personal técnico le permitirá habilitar su micrófono. Por favor, digan su nombre para los registros y el idioma en el que van a hablar si hablan en un idioma que no es inglés. Al hablar, por favor, silencien todos los demás dispositivos incluida la aplicación de Congress Rental Network. Por favor, hablen también claramente y a una velocidad razonable para permitir una correcta interpretación. Quisiera subrayar el hecho de que los participantes remotos no pueden hacer clic sobre la tecla de micrófono y habilitar su propio audio durante la sesión. Necesitan el apoyo del personal del técnico para ello.

En la sesión podrán hacer comentarios en el chat. Para eso, por favor, usen el menú desplegable que está en la ventana de chat y hagan clic en “Responder a todos los participantes”. De esta forma, todos podrán ver sus comentarios. Por favor, tengan en cuenta que el chat privado solo es posible entre los panelistas en el formato de seminario web. Si un participante quiere enviarle un mensaje a otro, este mensaje será visto por los anfitriones, coanfitriones y panelistas de la sesión. Habiendo dicho esto le voy a dar la palabra a Thomas Rickert. Thomas.

THOMAS RICKERT: Muchas gracias, Ozan. Buenos días, buenas tardes, buenas noches. Soy Thomas Rickert. Estoy a cargo de nombres y números. Trabajo en ECO, que es uno de los anfitriones y espónsores de esta sesión. Estoy en Alemania. Me encantaría haber viajado a Hamburgo para verlos a todos pero lamentablemente no fue posible esta vez. Espero que

tengamos la oportunidad de interactuar en el futuro cercano. Espero que todos estén seguros. Pasemos ahora a la próxima diapositiva.

Tal como ya se dijo, esta sesión tratará acerca del uso indebido del DNS. Lamentablemente, a lo largo de la historia de la ICANN hemos tenido muchas sesiones sobre uso indebido del DNS y la razón por la cual este tema nos mantiene ocupados es porque hay muchas cosas que tienen lugar en Internet, muchos malos actores que están tratando de explotar la falta de conocimiento de los usuarios y que están tratando de engañarlos con lugares a los que no deberían ir y están tratando de generar daños financieros y de otro tipo.

Para la ICANN, este es un tema muy especial considerando el mandato y la jurisdicción limitada de la ICANN en función de sus estatutos. Esta es la razón por la cual es importante continuar hablando acerca del uso indebido del DNS, entender cuál es el problema, entender cuáles son los roles y responsabilidades de los diferentes actores en el ecosistema de Internet y también ver cuáles podrían ser las soluciones potenciales. Durante esta sesión espero que podamos hacer un poco de todo lo que acabo de decir. Vamos a tratar de centrarnos en las soluciones y en el camino que tenemos por delante.

Hoy tendremos una sesión de 90 minutos que tendrá lugar de la siguiente forma. Tendremos presentaciones de los oradores que van a introducir el tema que yo voy a presentar en un momento. Luego de cada intervención haremos una breve pausa para ver si ustedes escribieron alguna pregunta en la ventana de preguntas y respuestas. Vamos a tratar de responder las preguntas que ustedes escriban y, por

favor, dirijan las preguntas al orador que acaban de escuchar para que si hay algo que no queda claro en la presentación, lo podamos aclarar en ese momento. Luego de los oradores tendremos una sesión de preguntas y respuestas al final de toda esta sesión de 90 minutos. Esta será la oportunidad que ustedes tendrán para plantear preguntas más generales y podrán hacerlo tanto en la ventana de preguntas y respuestas como levantando la mano y la gente del personal técnico les habilitará el micrófono para que ustedes puedan participar en el debate mediante intervenciones orales también.

Mis comentarios iniciales van a terminar en breve para que podamos hablar acerca del tema importante que nos reúne, para que ustedes sepan quiénes serán los oradores que hablarán acerca del uso indebido del DNS. Hoy vamos a escuchar a David Conrad en primer lugar. Luego Jeff Bedser, Mason Cole, Chris Lewis-Evans, James Bladel. Luego tendremos un debate general con todos los oradores y en los últimos minutos yo trataré de hacer un resumen de lo que escuchamos. Pasemos ahora a la próxima diapositiva, por favor. Esta es la primera diapositiva de David, perfecto. Esto debería darles entonces una idea general de lo que vamos a hacer hoy. Habiendo dicho esto le voy a dar entonces la palabra a David Conrad de la oficina de OCTO y él va a hablar acerca del uso indebido del DNS desde su visión.

DAVID CONRAD: Muchas gracias, Thomas. En el tiempo previo a esta sesión me pidieron que tratara de hablar acerca del panorama de las amenazas a la

seguridad de los dominios en el periodo de septiembre de 2019 a septiembre de 2020. Si se fijan en los informes de DAAR, los informes de actividad de uso indebido de dominios disponibles en el sitio web de la ICANN, los datos publicados en esos informes se retrotraen a los últimos nueve meses y me pidieron que hablara acerca del último año. Por lo tanto, mi equipo creó un informe con datos estadísticos generales. En el último año hemos visto reducciones de phishing, malware y botnet pero hemos visto un aumento en el spam. Debido a cómo predomina el spam también han cambiado los datos estadísticos de uso indebido del DNS. Hay un sesgo en este sentido pero si básicamente comparamos 2019 y 2020 vemos que la cantidad de uso indebido de dominios representa un 20% pero el porcentaje general aproximadamente se mantuvo igual. La próxima diapositiva, por favor.

Sin embargo, los datos que tenemos en DAAR se retrotraen a 2017. Si miramos hacia atrás vemos que hay algunas tendencias muy obvias. Aquí vemos las líneas con las tendencias que demuestran obviamente que la cantidad de gTLD está creciendo y pueden ver distintos aumentos y reducciones a lo largo del tiempo pero las tendencias son muy claras.

En el gráfico número dos vemos la cantidad de amenazas a la seguridad totales. Todas las cosas que consideramos dentro del proyecto DAAR que es comando y control de botnet, phishing, distribución de malware y spam. Pueden ver que la tendencia a lo largo del tiempo es decreciente, lo cual es obvio. Si se fijan en el gráfico tres básicamente aquí normalizamos los datos en función de la

cantidad de dominios en una zona en particular. Ven que hay una tendencia decreciente a lo largo del tiempo. Hay un pequeño aumento al final.

El gráfico cuatro muestra el rojo que es spam que sigue predominando y el otro punto a tener en cuenta con respecto a estos cuatro gráficos es que la línea roja o azul aparece cuando se implementó GDPR. Podrán ver que no se observa un impacto significativo en la cantidad de uso indebido de nombres de dominio, al menos lo que podemos detectar dentro del contexto de DAAR.

Si vemos entonces qué ocurre con las amenazas individuales durante el mismo periodo, octubre de 2017 a octubre de 2020, una vez más vemos aquí las tendencias en estas líneas. Hay algunos hechos interesantes. Esto se compara con los datos estadísticos que les mostré en la primera diapositiva donde phishing, malware y comando y control estaban decreciendo. Si volvemos a octubre de 2017 vemos exactamente lo contrario. Phishing, malware y comando y control todos están creciendo pero un poco más lentamente mientras que el spam a lo largo del mismo periodo está cayendo significativamente.

Hay un punto con el que tenemos que tener cuidado con respecto a estos gráficos. Tenemos que asegurarnos de comparar el eje de la Y correctamente. En general vemos que spam tiene un orden de magnitud más que todos los demás. Esto es algo a tener en cuenta. La próxima diapositiva, por favor.

Acá vemos otro junto de datos que recabamos en la oficina del CTO. Los indicadores de sanidad, de tecnologías de identificadores, comenzamos con estos indicadores en 2018 y hacemos un seguimiento de diferentes indicadores asociados con la sanidad del sistema de identificadores. Hay un indicador especial. La métrica M2, que es uso indebido de nombres de dominio, y aquí vemos la tendencia a lo largo del tiempo con uso indebido por cada 10.000 dominios, la cantidad de uso indebido dentro de registradores y gTLD, los que representan el 50% de las amenazas de seguridad informadas.

Si se fijan en las tablas que tenemos en el sitio web del ITHI, es una interfaz de usuario que quizá les recordará lo que ocurría a principios de los 90. Los índices de uso indebido muestran, por ejemplo en el caso del phishing, un 10%. 10 registros representan el 90% de las amenazas de seguridad de phishing detectables. Estos porcentajes, 0.3% en el caso de los registros y 0.1% en el caso de los registradores.

Los datos de los registradores deberían tomarse con pinzas ya que la información de registradores que tenemos proviene de nuestro proveedor y estos datos se recaban en una base de datos a lo largo del tiempo porque nosotros no tenemos acceso dentro del sistema DAAR a la información de los registradores asociadas con nombres de dominio individuales. La información quizá esté algo desactualizada. La información de registradores es algo que debemos tomar con cuidado y utilizar como índice y no necesariamente como un valor absolutamente exacto. También debería señalar que los datos de ITHI también provienen de los mismos datos crudos utilizados por DAAR

más alguna información adicional relacionada con los registradores. La próxima diapositiva, por favor.

Otro proyecto que llevamos a cabo dentro de la oficina de OCTO en relación con el uso indebido del DNS es lo que llamamos sistema de informes, recopilación, identificación de amenazas a la seguridad de los nombres de dominio. Estos son datos que empezamos a recabar en enero de 2020 y la idea era tener información relacionada con dominios relacionados con la pandemia. Esto fue al principio de la pandemia y aquí vemos los diferentes registros que se registraron. Hubo una inundación de registraciones asociadas con la pandemia. Hay ciertas implicancias que indican que podrían utilizarse con fines ilegales. Nosotros nos centramos en la distribución de phishing y malware como amenazas a la seguridad.

Durante el periodo de mayo de 2020 a septiembre de 2020 recabamos de manera uniforme datos y durante un análisis de estos datos identificamos a través de nuestro sistema que de las 134.000 registraciones detectadas, 1.7% teníamos la seguridad suficiente como para llamarlos indicación de uso indebido. En junio empezamos a denunciar estos dominios y a informar a los registradores.

Si consideramos los datos en el periodo informado de este enero de 2020 a septiembre de 2020 vemos que hay 80.000 dominios relacionados con la pandemia registrados. 170 generaron informes enviados a los registradores que indicaban una conducta que podría amenazar la seguridad desde nuestro punto de vista. Después vamos a hablar un poco más sobre este tema. El nombre de dominio fue

registrado en el sistema de nombres de dominio. Tenía por lo menos un informe identificado en las listas de proveedores de reputación y cuando analizamos la registración propiamente dicha, el sitio web asociado con ese dominio tenía material que indicaría que había algún tipo de amenaza a la seguridad. Lo que queríamos hacer era minimizar la cantidad de falsos positivos. De los 170 informados a 6 de octubre, 87 no existen ya en el sistema de nombres de dominio. Se eliminaron. 56 ya no cumplen con los criterios de informes o denuncias que les mencioné. Es decir, ya no hay una resolución con ese dominio o el dominio ya no representa una amenaza de seguridad. 20 directamente no tienen resolución. Son registros DNS que no responden a consultas y siete de los 170 aún al parecer son maliciosos. Habiendo dicho esto, con todo gusto voy a responder cualquier pregunta que puedan tener. Thomas, le doy la palabra para que presente al siguiente orador.

THOMAS RICKERT: Muchas gracias, David. Tenemos un par de preguntas. No sé muy bien si las vamos a responder todas en este momento pero podemos probar. Elizabeth [inaudible], espero pronunciarlo bien, está preguntando por el spam. ¿Esto representa los emails no solicitados o los emails de spam tienen otra forma de uso técnico como malware o phishing? En otras palabras, si un email de spam también contiene otras formas de uso indebido, ¿de qué maneras se categoriza ese uso indebido?

DAVID CONRAD: La información que tenemos nosotros viene de las listas de proveedores de reputación y no distinguen entre los mecanismos que se utilizan para distribuir amenazas de seguridad. Lo que vemos entonces es información que está vinculada al spam, que se reporta en los distintos proveedores de reputación. En nuestro informe DAAR y también a partir del documento de metodología nosotros hacemos una lista de los proveedores de reputación que utilizamos y qué es lo que estos proveedores nos dicen para darles una idea de la información que nosotros estamos recolectando.

THOMAS RICKERT: Gracias, David. Vamos a tomar otras dos preguntas. Las reducciones no se ven como lo que se está describiendo. Estamos hablando de phishing y de spam. A mí me parece que el aumento tiene que mostrar el phishing también. Gran parte del phishing se perpetúa a través del spam. ¿Cómo pueden reconciliar esto los números? Debería ser en paralelo. Otra pregunta de Laurie Schuman. Para los diez registros que aparecen en los peores actores cuáles son las medidas de incumplimiento que se han tomado. ¿Cuál es el estado actual?

DAVID CONRAD: En relación a la correlación entre phishing y spam, la información que nosotros recolectamos proviene de los proveedores de reputación. Si alguien lista algo como spam y es distribuido como phishing, es posible entonces que las dos categorías como están reportadas de múltiples maneras aparezcan de modo diferente. Tratamos de

remover las entradas redundantes, de eliminarlas pero, sin embargo, podría haber algunos casos en los que esos nombres queden duplicados. Es poco probable hasta donde yo sé. La información que nosotros recolectamos no la modificamos de ninguna manera. Esta es información que nosotros agregamos a través de varios proveedores. Si la gente ve estadísticas diferentes en relación con el uso indebido del DNS y las amenazas, sería muy interesante poder entender cuáles son las fuentes que usan para proveer esa información, esos datos. Podemos trabajar con el sistema DAAR para ver si podemos incorporar esos conjuntos de datos en el sistema DAAR y en otros sistemas que estamos utilizando.

En cuanto a la segunda pregunta, vamos a verla… El número absoluto, la cantidad absoluta de registros o registradores que son responsables por el 90% del uso indebido debe ser contextualizado, no en datos normalizados. Quizá no es sorprendente que hay una sólida correlación entre la cantidad total de registraciones y la cantidad de uso indebido de esas registraciones. Si miramos los datos no normalizados, los registros y registradores que tienen la mayor cantidad de registraciones tienen también la mayor cantidad de dominios con uso indebido. Es en realidad mejor mirar todo esto en el contexto de los números normalizados que son relativos a la cantidad de registraciones. Cuando empezamos a ver esos números es menos obvio quiénes son los malos actores.

THOMAS RICKERT: Muchas gracias, David. Creo que tenemos que pasar al próximo orador para que todos puedan tener sus 10 minutos para hablar. David, yo sugeriría que mientras escuchamos a Jeff quizá puede ir al recuadro de preguntas y respuestas y dar respuesta por escrito, así también hacemos lo mismo para los próximos oradores y las preguntas pueden resolverse y luego volvemos, al final de la sesión. Creo que esta es una forma aceptable. Vamos a pasar ahora a Jeff Bedser, que es el presidente del grupo de trabajo de uso indebido del DNS del SSAC. Jeff, adelante.

JEFF BEDSER: Buenos días, buenas tardes y buenas noches. Gracias a todos. Quiero indicar que este es el grupo de trabajo establecido por SSAC hace aproximadamente un año. Tuvo una carta orgánica muy abarcativa que incluyó varios asuntos de uso indebido que aún no hemos cubierto. Este es nuestro primer producto que cubre los asuntos del uso indebido del DNS. Todo esto no se ha publicado, esta norma de SSAC. Se va a publicar en las próximas semanas. Esperábamos tenerlo listo para ICANN69 pero el proceso interno no se concluyó. Esperamos poder tenerlo pronto.

Primero quiero que quede claro que una de las cuestiones que surgieron en este producto es que nosotros invitamos a personas de fuera de SSAC para que participen. Estos fueron invitados de PSWG, del grupo de partes interesadas de registro y algunos de estos invitados aportaron sus conocimientos que nos enseñaron a entender

mejor las cuestiones de política y algunos temas también de uso indebido. Pido disculpas. La aplicación de traducción se encendió.

El grupo está compuesto por personas que son de fuera de SSAC además de SSAC. Nos dan también un contexto de política, de uso indebido y de personas que vienen de registros, registradores y de sitios de contenido. Una de las cuestiones que le escucharon decir a David Conrad es referirse a las mediciones de los datos de uso indebido. Una de estas cuestiones es que no ocurren en un día en particular y uno de los asuntos también es cuánto dura el uso indebido. Cada hora, cada día de un dominio que continúa siendo abusado, hay más potencial de más víctimas, más pérdidas y como nos ha dicho Chris Evans, vamos a escuchar sobre las pérdidas asociadas al uso indebido.

Internet en sí tiene uso indebido en una cierta medida. Los informes que recibimos los recibimos internamente. También de organismos de aplicación de la ley. Pero no hay duda de que existe el uso indebido. Nadie debe esperar que el uso indebido se detenga con el DNS porque el ciberdelito va a continuar sin duda y va a continuar habiendo víctimas. El problema que enfrentamos aquí es que hay una falta de confianza donde los usuarios finales de Internet sean comerciales o personales o no comerciales. Cualquiera que sea su actividad deben poder confiar en el sistema y también los proveedores de sistema de la infraestructura.

El informe que se va a publicar pronto trata de abordar la metodología y la cooperación necesaria para reducir el uso indebido del DNS. Trata

de establecer buenas prácticas y solamente se puede lograr con la cooperación de las distintas partes del DNS. Se debe tener en cuenta que esas partes contratadas son solo una pequeña parte de la totalidad del sistema del DNS que está siendo utilizado para la mecanización. Hay proveedores de alojamiento, de email, de sistemas de entrega de contenido, distintas estructuras y partes contratadas que son una parte del ecosistema total. Siguiente diapositiva.

Los puntos clave de este documento son los siguientes. Alentar definiciones estándar de abuso o de uso indebido. El documento no hizo un intento de redefinir o de aplicar definiciones nuevas sino que utilizó definiciones existentes que fueran lo suficientemente vernáculas como para describir el problema. Cuando uno enfrenta un problema, las definiciones estándares quizá sean la mejor forma de avanzar.

El punto siguiente fue determinar el punto primario apropiado de responsabilidad de la resolución del uso indebido. Cada tipo de uso indebido tiene un sabor específico y de la manera en que esto se pueda resolver quizá pueda ocurrir a nivel de registro, a nivel de alojamiento. Podría ser en cualquier parte del ecosistema. Hay ciertos tipos de uso indebido que siempre van a tener su lugar y su punto más adecuado para que este uso indebido se resuelva. Identificar las mejores prácticas para la aplicación de los estándares de la evidencia. Esto es un poco complicado y reconocemos que las cuestiones legales en las distintas jurisdicciones tienen distintos requisitos para poder probar algo. Esto quizá sea un poco problemático porque el fraude es un delito pero si hay un estándar o una normalización de la evidencia

donde se dice: “Este incidente es de un botnet de comando y control“, se debe demostrar que es un botnet a cualquier persona que esté solicitando que haya una actuación en relación con ese botnet.

Establecer los caminos de escalamiento estandarizado para la resolución del uso indebido. Todos nosotros entendemos que un dominio tiene un ciclo de vida y que hay distintos actores hasta que se resuelva. La realidad también es que en algunos lugares a veces hay una no respuesta a ese punto primario. Se deben establecer entonces formas de escalamiento que permitan que las distintas instancias en el ecosistema digan: “Vamos a un proveedor de alojamiento”. Quizá no se puede contactar, no se tiene la suficiente información de contacto y no hay respuesta a ese contacto. En ese caso, cuál es el camino de escalamiento adecuado para que ese dominio se resuelva. De nuevo, la meta es reducir la victimización y que haya menos víctimas.

Determinar plazos específicos para la acción en cuanto a los informes de uso indebido. La mayoría de las partes hoy permiten que haya 24 horas para responder. Es decir, si una parte reporta un abuso, un uso indebido en el lugar inadecuado en el ecosistema, necesita tiempo para que el dominio se resuelva. Determinar un plazo específico para la acción también reduce el periodo de tiempo en el que el dominio está vivo. También analizamos la recomendación del desarrollo de programas de notificación que van a hacer que sea más eficiente y más rápido la resolución del uso indebido. Hay muchas entidades comerciales y no comerciales pero hay otra tendencia que indica que hay ciertas empresas que están reportando el uso indebido y que esa cantidad está subiendo a medida que más consumidores y marcas

están detectando el uso indebido y también hay varios actores que deben entender en términos de los servicios o incluso necesariamente cómo funciona el DNS. Un programa de notificación ayudaría con eso.

Crear un mecanismo para la disponibilidad de información de contacto para el uso indebido. Este es un tema de registración de datos dentro del GDPR. En realidad esto no es así. Se trata de entidades que quieren controlar un dominio. A veces la información de contacto es fácil de encontrar, otras no. El mecanismo que permite que esto sea así está disponible y se debe reportar un dominio con la evidencia que tenemos dentro del ecosistema.

Finalmente crear un mecanismo para garantizar que haya una calidad razonable de la información de contacto y que haya una mitigación del uso indebido. Como presidente del grupo de trabajo, espero que el informe salga en las próximas semanas. Thomas, ahora sí, le doy la palabra. Adelante.

THOMAS RICKERT: Muchas gracias, Jeff. Hizo un trabajo muy bueno limitándose a los 10 minutos asignados. Muy bien. Veo que en la ventana de preguntas y respuestas se habla mucho acerca de preguntas para David. Si tienen preguntas para Jeff, por favor, escríbanlas ahora en la ventana de preguntas y respuestas. Tal como hicimos con Dave, si después surgen preguntas para Jeff, escríbanlas en la parte de preguntas y respuestas y ahora pasamos al siguiente orador, Mason Cole, que es miembro de CSG. Va a dar la perspectiva del grupo de partes interesadas

comerciales acerca del uso indebido del DNS. Le doy la palabra, Mason.

MASON COLE: Hola, Thomas. ¿Me escuchan bien?

THOMAS RICKERT: Sí, lo escuchamos bien.

MASON COLE: Buenos días, buenas tardes, buenas noches a todos. Voy a comenzar. No creo que tarde 10 minutos pero vamos a ver. La próxima diapositiva, por favor. Estamos aquí de nuevo para hablar acerca del uso indebido. El problema es que, tal como dijeron Jeff y otros, es un problema que al parecer no desaparece y probablemente nunca lo hará. Pasan los años y periódicamente el problema se ve magnificado por eventos de fuera como vimos en marzo con la epidemia y también ocurre cuando hay desastres naturales, problemas sociales, problemas mundiales. El tema común, por supuesto, es que el DNS se utiliza con fines ilegítimos, ilícitos. Esta creo que es la cuarta reunión plenaria consecutiva de la ICANN sobre uso indebido del DNS. Creo que para muchos de nosotros sería mejor poder seguir hablando de este tema de manera productiva y de las soluciones productivas que podemos plantear para poder hacer algo al respecto. La siguiente diapositiva, por favor.

Como vemos aquí, en cuanto a las estadísticas, al parecer ya todos tienen datos. Si uno escribe uso indebido del DNS se encuentra con todo tipo de datos estadísticos. Estos datos publicados antes del informe de SSAC son los datos del Interisle Consulting Group publicado hace poco tiempo. Durante el periodo del estudio que fue del 1 de mayo al 31 de julio de este año, el estudio se centra en phishing. Los informes afectaron a más de 99.000 nombres de dominio y 439 TLD en 414 registradores. De este total, Interisle identificó 60.000 nombres de dominio maliciosos. Sabemos que existe el problema de phishing aunque no sabemos exactamente cuál es la magnitud del problema y la [redacción] de los datos de WHOIS contribuye a la subdetección del problema. La siguiente diapositiva, por favor.

De acuerdo con SSAC, lo que sabemos es que el uso indebido del DNS y el ciberdelito resultante continúa afectando a millones de víctimas todos los años y reduce la confianza en Internet incluido el DNS. Quería referirme a lo que dijo Jeff antes cuando dijo que esto tiene que ver con la confianza de Internet. Sabemos que es importante poder operar, llevar a cabo nuestro trabajo y, por lo tanto, como lugar para realizar actividades personales, comerciales y no comerciales, es importante contar con esta confianza. Gracias por esta diapositiva.

Los datos estadísticos y cuáles son los puntos en los que deberíamos estar de acuerdo. Creo que todos deberíamos acordar diferentes perspectivas de este tema. Aparentemente ya hemos tenido cuatro sesiones sobre este tema. El uso indebido del DNS quizá esté creciendo en función de los datos o quizá esté cayendo en función de la fuente de los datos. Sin embargo, lo que sí deberíamos acordar es que cuando

ocurre el uso indebido del DNS, tiene el impacto que hemos mencionado sobre la confianza de Internet. Creo que tenemos que tomar medidas proactivas y enfatizo la palabra proactiva. Creo que tenemos que ser más proactivos en cuanto a nuestra capacidad de perseguir el uso indebido del DNS.

No quisiera abrir una discusión en la ICANN acerca de si tenemos que ocuparnos de él, no si tenemos que ocuparnos del uso indebido del DNS sino cómo hablamos del uso indebido del DNS. No es una guerra que tenemos que mantener entre nosotros. Tenemos que apuntar hacia los malos actores. La siguiente diapositiva, por favor.

Se han hecho avances, tal como ya dijeron otros oradores. Quisiera aplaudir una vez más el marco voluntario creado por registros y registradores a principios de este año o quizá fue a fines del año pasado. Tuvo un impacto medible sobre el uso indebido del DNS. Creo que es un esfuerzo que deberíamos aplaudir. Quiero reconocer el trabajo de las partes contratadas por su aporte en este sentido. La siguiente diapositiva, por favor.

Tal como vemos, en este caso en algunas áreas no se han hecho avances y tenemos que mejorar. Los marcos voluntarios son muy buenos pero no son totalmente inclusivos. Sabemos que siempre se refiere a estos 8 a 10 malos actores que la ICANN dice que conoce y sabe dónde se esconden pero sería útil que tratemos de perseguir los resultados fáciles y también poder ir más allá para poder ir más allá del marco ya establecido. La próxima diapositiva, por favor.

Como vemos aquí, volvamos a Montreal. A esta altura el año pasado tuvimos la primera reunión plenaria sobre uso indebido del DNS y quería mostrarles aquí una intervención de Elliot Noss de Tucows que me pareció especialmente útil. Tenemos que enfrentar los problemas que tenemos frente a nosotros y si el departamento de cumplimiento de la ICANN puede identificar de manera eficaz que hay elementos específicos del contrato que los ayudarán a hacer cumplir las medidas para que no actúen los malos actores, entonces hablemos de eso. Yo no creo que necesitemos a los malos actores. Yo no creo que necesitemos nada más que lo que ya se está haciendo en los contratos. Tenemos que tomar medidas proactivas y utilizar las herramientas con las que ya contamos para identificar los malos actores y perseguirlos.

Es mi última diapositiva. No se puede escalar el monte Everest en un solo paso. Tenemos que dar pequeños pasos, subir en etapas. Tenemos una oportunidad de abordar el uso indebido del DNS en etapas. Además de las recomendaciones de SSAC, estas son algunas ideas acerca de lo que podríamos hacer juntos para perseguir a los malos actores. Podemos, una vez más, quitar de delante de nosotros los resultados más fáciles, que en este caso son los 8 a 10 malos actores conocidos que crean los principales problemas en el espacio de nombres. También tenemos que hablar después acerca de la definición de uso indebido y si se necesitan nuevas herramientas, considerar incentivos para limpiar registros y registradores. La organización de la ICANN tiene la oportunidad de ser proactiva con su función de cumplimiento. Quisiera también pedirles a las partes

contratadas que sean proactivas en términos de mitigación y prevención ya que tenemos que identificar el uso indebido del DNS pero no solamente actuar en manera posterior al hecho sino también ocuparnos de la prevención. También tenemos que convertir estos temas de reuniones plenarias que ocurren una vez por reunión en informes sobre los avances presentados a la comunidad. Esto es lo que quería decir acerca del uso indebido del DNS. Esta fue mi última diapositiva. Thomas, le doy la palabra.

THOMAS RICKERT: Muchas gracias, Mason. Hay dos preguntas para usted. Sugiero que respondamos a ambas preguntas antes de continuar. Le pido una respuesta breve, por favor. Mason, ¿usted sabe quién financió el informe Interisle?

MASON COLE: No, no lo sé. Lo lamento.

THOMAS RICKERT: [inaudible] pregunta: “Mason, ¿podría explicar brevemente en qué manera la redacción del WHOIS afecta a la detección de phishing? Yo creo que el seguimiento de las personas que están por detrás de los intentos de phishing podría ser más difícil pero la cantidad de nombres de dominio de los que se está haciendo un uso indebido sigue siendo la misma”.

MASON COLE: Gracias por la pregunta. Trataré de responder esa pregunta por escrito ya que implica mucha información. ¿Le parece bien que responda a esta pregunta por escrito después?

THOMAS RICKERT: Sí, por supuesto. Veamos si hay un par de preguntas más. Si hay preguntas que aún no han sido respondidas también trataremos de responderlas por escrito. Sé que mientras tanto todo el mundo tiene acceso a las pregunta. Si hicieron una pregunta, fíjense si su pregunta o preguntas parecidas ya han sido respondidas para no duplicar esfuerzos y no volver a plantearles más preguntas. El siguiente orador es Chris Lewis Evans que representa el grupo de trabajo de seguridad pública del GAC y trabaja en la Agencia Nacional de Delito del Reino Unido.

CHRIS LEWIS-EVANS: Muchas gracias, Thomas. Gracias por estar con nosotros en esta plenaria. Quisiera hablar acerca de lo siguiente. Vamos a la siguiente diapositiva. ¿Por qué hablamos de uso indebido del DNS? Tal como ya dijeron Jeff y Mason, este es un tema que hemos tratado en muchas sesiones diferentes. La razón principal es el impacto que tiene el uso indebido sobre los usuarios de Internet. Yo aquí puse cinco datos estadísticos que se refieren a diferentes niveles de abuso. El centro de reclamos de delitos de Internet del FBI recibió 467.000 reclamos en 2019. Un promedio de 1.300 por día. Esto es realmente una gran cantidad y vemos un alto valor en pérdidas también. Esto afecta a

todos los usuarios de Internet, empresas, personas individuales, todos. En el Reino Unido dentro de las estadísticas nacionales podemos ver que el 85% de los fraudes denunciados es ciberfraude o utilizan herramientas cibernéticas. Podrán ver que el impacto de estos sobre los usuarios individuales es muy grande.

Con respecto a la escala del daño y de los perjuicios, creo que el ransomware tiene un gran impacto. Vemos un aumento de 715% con respecto al año pasado. Es un enorme aumento en los perjuicios. No son solamente perjuicios financieros a personas o empresas. También se trata de datos filtrados por parte de malos actores. En el Reino Unido más del 60% de los incidentes registrados son filtración de datos debido a phishing o malware y esto está dentro del área de uso indebido del DNS. Reconocemos dentro del marco de uso indebido del DNS este tipo de filtraciones tal como ya dijeron los oradores anteriormente. La próxima diapositiva, por favor.

Tal como Maxime mencionó en el chat tenemos una serie de lugares donde nos podemos ocupar del uso indebido del DNS. Dentro de la ICANN obviamente nos concentramos en los registros, los registradores, dentro de la ICANN propiamente dicha, pero para ocuparnos de ese tema y para reducir los perjuicios y los daños precisamos una respuesta de todo el ecosistema. Los proveedores de email, de servicios de Internet, los ISP, las redes, los RIR, la lista es muy extensa. Es todo el entorno en el que trabajamos. Necesitamos algo que nos ayude a enfrentar el problema del uso indebido y llegar al lugar correcto.

Quisiera hablar aquí de un facilitador común. La ICANN es un facilitador común y estamos hablando de uso indebido del DNS y esto tiene impacto sobre otras áreas. Tal como dijo Mason, hay un trabajo proactivo que se está llevando a cabo y que es clave. Es fundamental poder tomar medidas proactivas para poder superar este problema y para que sea más difícil que se ocasionen todos estos perjuicios. Tenemos a la ICANN que es un facilitador común en este entorno, en este grupo de partes interesadas pero no tenemos a alguien que cubra todo el ecosistema. Pasemos a la próxima diapositiva, por favor.

¿Qué podemos hacer? Como organismo de aplicación de la ley, yo también formo parte de la ICANN, por supuesto. Hemos tenido muchísimas reuniones muy buenas con los grupos de registros, registradores y otras partes interesadas. Puedo utilizar mis conocimientos para derivar los reclamos por uso indebido de la manera correcta pero esto no es lo mismo que lo que hace la autoridad de aplicación de la ley o de ciberseguridad. Hay evidencias de suspensión de dominios, gente que recurre a la ICANN porque no sabe adónde recurrir. Dependiendo del tipo de uso indebido del DNS tenemos que ver dónde vamos a poder lograr los principales cambios. Tal como ya se dijo, tenemos información sobre malware. Dar de baja el nombre de dominio no es necesariamente la primera respuesta que buscamos. Sin embargo, quizá sea la respuesta correcta dado que significa que se reducen los perjuicios ocasionados al ecosistema de Internet.

¿Qué ocurre entonces si no se toman medidas? ¿Cómo escalamos la situación? Esto se remite nuevamente al tema de un facilitador común.

Tenemos publicación de contenido, no ocurre nada. Tenemos que ver cómo hacer el escalamiento, el registrador no responde, cómo escalamos y cuáles son los siguientes pasos. Contar con este mecanismo es otro paso práctico que podemos tomar. Es muy importante para realmente complicarles la vida lo máximo posible a los malos actores, a los delincuentes para evitar todos estos perjuicios y daños.

No vamos a poder resolver todo siendo proactivos. Lamentablemente siempre habrá alguna forma de sortear el sistema y por lo tanto debemos contar con un buen sistema que también sea reactivo y permita tomar las medidas adecuadas. Creo que es clave que en todo proceso con el que contamos actuemos de manera oportuna y podamos llevarlo a cabo de la forma más efectiva posible. Creo que ya se dijo también que es clave saber que no se trata simplemente de golpear la puerta de alguien y pedir los datos. Es necesario que existan controles y verificaciones. Tener un acuerdo de datos compartidos probablemente nos permitirá lograr esto. No queremos enfrentarnos con un incidente y tener que hablar con un registro o un registrador o alguien que esté publicando datos y preguntarle qué están haciendo. Es importante tener un marco, llegar a un acuerdo para que todos conozcan el proceso, los controles y verificaciones, tal como dijo Jeff anteriormente. Tenemos que saber cuáles son las normas que se necesitan. Esto sirve realmente a reducir los daños y perjuicios. Creo que es clave.

Yo creo que hay mucho que podemos hacer. Creo que hay muchas medidas proactivas que podemos tomar. Estamos hablando aquí de

reducir los daños ocasionados por el uso indebido del DNS, reducir la cantidad de dominios no necesariamente siempre significa reducir los daños. Los delincuentes utilizan los nombres de dominio de diferentes formas y tenemos que encontrar una forma de detener los daños ocasionados. Habiendo dicho esto, le doy la palabra nuevamente a Thomas.

THOMAS RICKERT: Gracias, Chris. Voy a leer una pregunta de Maxime. Quiere saber si tienen planeado incluir a los RIR en el proceso porque todo el uso indebido ocurre a través de IP.

CHRIS LEWIS-EVANS: Así es. Los RIR son los que menor cantidad tienen en el registro. Definitivamente es una parte clave del ecosistema y es algo con lo cual nosotros trabajamos muy bien. Trabajamos bien con RIPE dentro de la región y esto es algo que es clave. Gracias.

THOMAS RICKERT: Otra pregunta que tenemos de Maxime es que hay muchas llamadas de un enfoque proactivo. ¿Puede alguien explicar cómo predecir las futuras acciones y situaciones donde no haya nada malo que se haya hecho todavía para los dominios en cuestión?

CHRIS LEWIS-EVANS: Es muy difícil obviamente poder predecir cuándo el delito va a ocurrir y no es algo que uno pueda evitar. Hay sistemas que están listos para enfrentar el uso indebido cuando ocurre. Esa es una medida proactiva. Tener los sistemas correctos y tener la posibilidad de tomar medidas creo que es un buen paso. Hay muchas actividades de datos que las partes contratadas están haciendo en el marco del uso indebido del DNS y los detalles de eso. Quizá puedan estar dentro de este contexto. Creo que hay mucho que podemos hacer proactivamente para detener el uso indebido.

THOMAS RICKERT: Gracias, Chris. Creo que esta es un área que debemos tomar cuando hablamos con los grupos de panelistas. Probablemente, si podemos pasar al último orador, tengo una pregunta, si me permite. En una de las diapositivas usted dijo que el 85% de los casos de fraude son permitidos a través de lo cíber. ¿Es eso algo que también denominamos uso indebido?

CHRIS LEWIS-EVANS: No. No es uso indebido. Eso incluiría spam directo que dependiendo de la definición de uso indebido de DNS y lo que nos ha dicho Jeff, qué es el uso indebido del DNS. Hay otros mecanismos por los cuales también se incluyó las estadísticas del ICO para poder entender qué es el uso indebido.

THOMAS RICKERT: Veo una pregunta que viene de Monica y la voy a tomar porque está hablando de la diversidad de género. Vamos a tratar de responder esa pregunta. La pregunta es: ¿Se pueden compartir detalles sobre el 60% de los actos indebidos de datos atribuidos a phishing y malware? ¿Tiene detalles de las cifras, las fuentes de las cifras? ¿Puede explicar un poco más qué significa que son atribuidos? Quizá pueda explicar cuál es el modus operandi.

CHRIS LEWIS-EVANS: Los datos de ICO, que es la autoridad de protección de datos en el Reino Unido se los puedo compartir en el chat.

THOMAS RICKERT: Muchas gracias, Chris. Ahora vamos a pasar a nuestro último orador que es James Bladel, de GoDaddy. Nos va a hablar de parte del grupo de partes interesadas de registros.

JAMES BLADEL: Espero que me puedan escuchar bien. Bienvenidos a la mitad de la noche a todo el mundo. Gracias por incluirme en esta conversación. Uno de los beneficios de ser el último en el programa es que uno puede hacer comentarios sobre lo que han dicho los oradores anteriores y eso demuestra que presté atención y tomé notas en las sesiones.

Quería presentar la perspectiva de la cámara de partes contratadas y ustedes van a ir viendo a medida que avancemos a qué me refiero. En general, el uso indebido online, en cuanto lo relacionamos con lo que

nos dijo Thomas, es un desafío para nuestra industria. También es una prioridad para las partes contratadas. Esto nos lo indican todas las inversiones en sistemas que se han hecho hasta ahora. El desempeño tanto en números como nos mencionó David y el informe de las partes contratadas más importantes y operadores en ICANN, todo esto demuestra que esa inversión está recibiendo beneficios y que el uso indebido del DNS está siendo detectado y mitigado en escala. Yo lo que creo es que debemos reconocer una distinción entre el uso indebido general, el uso indebido del contenido y otros tipos de uso indebido que son específicos al DNS. De nuevo me refiero a lo que dijo Thomas sobre el rol limitado y las limitaciones que tiene ICANN por lo que figura en el estatuto en cuanto al DNS en sí.

La misión de la ICANN de nuevo es asegurar la seguridad y estabilidad del DNS pero especialmente en cuanto al spam y algunas otras prácticas fraudulentas online todo esto depende mucho del contenido y ahí es donde empezamos a salir de lo que está dentro del alcance del mandato de la ICANN. La capacidad de un registro o de un registrador de poder mitigar el uso indebido o el contenido abusivo es bastante restringida. Nos referimos a esto como una opción nuclear porque solo hay una palanca que uno puede mover como registro o registrador que es dar de baja o suspender un dominio. Ciertamente esto no es adecuado para el uso indebido del contenido. Hay muchas cosas que se orquestan a través de una página de Facebook y no podemos dar de baja facebook.com. Hay productos también que se venden en eBay y no podemos suspender ebay.com. No es la respuesta adecuada. Por eso decimos que tenemos solamente una palanca, una opción nuclear

que podemos aplicar. Los registros y registradores también están situados en otras partes del ecosistema. Por ejemplo, GoDaddy es un registro y un registrador. También es quien aloja contenido.

Hay más formas de mitigación que podemos utilizar y las podemos presentar cuando detectamos el uso indebido. Creo que esta una de las razones por las cuales escuchamos que las partes contratadas nos dicen que solamente una parte del problema del uso indebido online está dentro del paraguas del alcance de la ICANN pero como industria nos hemos organizado en otros esfuerzos que están por fuera de la ICANN para enfrentar los distintos tipos de uso indebido. Siguiente diapositiva, por favor.

En septiembre del año pasado, esto fue antes de lo que ocurrió, fue en Montreal cuando todavía nos reuníamos, los registros y registradores lanzamos un marco para el uso indebido del DNS. Este fue un esfuerzo para hacer precisamente lo que alguno de los oradores anteriores ya han expresado. Es una definición estandarizada del uso indebido, cuáles son las acciones esperadas y la identificación, creo que fue Jeff, del informe del SSAC, que nos habló sobre identificar cuáles son las pares responsables para las distintas situaciones y cuáles son las actividades típicas de mitigación. Hemos tenido más de 50 firmas de este marco. Como Mason nos dijo, está teniendo un impacto, está impulsando diría yo la tolerancia de aquellos que tienen menos capacidades y ha ayudado a construir todas las capacidades generales de la industria y ha impulsado a estos actores abusivos a salir.

Ayer algunos de los participantes de estos firmantes volvieron a actualizar el documento. Lo pueden encontrar en el sitio de la ICANN. Quiero explicar qué es este marco y cómo operamos. Más que bombardear esta sesión con muchos gráficos y estadísticas quiero alentarlos a que hagan clic en ese link dnsabuseframework.org y que vean una actualización de quiénes son los miembros de este marco.

En 2019, también en mayo, un poco más temprano, la red de política de jurisdicción e Internet publicó un documento donde se establecen todos los desafíos y las prácticas de mitigación del uso indebido del DNS. Esas definiciones también están alineadas con el marco pero incluyen también el fast flux hosting, que no está incluido en ese marco.

Por fuera del uso indebido, cuando analizamos el contenido hay muchas industrias, alianzas y asociaciones, coaliciones, equipos. Son todas cuestiones con las que ustedes están familiarizados. Quizá no. Son categorías específicas del uso indebido como el spam, como el abuso de niños, el contraterrorismo, las farmacéuticas. Este punto aquí nos indica que por el hecho de que no veamos las acciones en una categoría específica bajo el paraguas de la ICANN eso no significa que el trabajo no se esté haciendo. Hay muchas partes contratadas que se cambian el sombrero y participan en las distintas organizaciones dependiendo de dónde estén situadas. Siguiente diapositiva, por favor.

Vamos a hablar de la actualidad. Este año ha sido muy complicado. Todo el mundo empezó a moverse online como un modo de

supervivencia casi en respuesta a la pandemia del COVID-19. Específicamente me refiero a pequeñas empresas. Todos conocen su restaurante favorito, su empresa que les hace envíos a domicilio, aquellos que tienen hijos en las escuelas saben que la experiencia se transformó completamente, las organizaciones políticas, religiosas, todas pasan a un entorno un poco más virtual, más que a uno físico. Por supuesto, lo mismo se aplica para la ICANN. Lo digo porque nuestra industria ha contribuido a ese pivot y todas estas son tendencias que están en marcha pero que el COVID-19 simplemente las aceleró. Esto ocurrió en un periodo de meses. Lo que esperamos es que cuando esto termine todos seamos un poco más flexibles en poder responder a esa transformación pero no debemos sorprendernos de que todos los criminales y los malos actores, los delincuentes siguen también esa transición y también evolucionan en su enfoque y en su táctica a ir siguiendo dónde están sus víctimas y sus víctimas ya no participan en un mundo físico o casi físico o en una economía casi física. Pueden refocalizar el aspecto virtual de sus ataques.

Dicho todo esto, los datos no indican que estos malos actores nos muestren que Internet se esté desarmando. Debemos volver entonces a las estadísticas de David. Nuestra industria ha visto aumentos en los informes de phishing y en uno de los gráficos que vimos, vimos esa tendencia con algunos picos en la primavera y luego también algunos en el verano.

En líneas generales, creo que hemos visto un crecimiento bastante modesto y me refiero específicamente a GoDaddy y no a la industria en total. Estamos viendo un crecimiento del 15%, nada que no se vea en

un orden de magnitud como una suba en la actividad ni tampoco nada que indique que haya un nuevo tipo de ataque que se haya desarrollado. En este momento GoDaddy está procesando alrededor de 2.000 informes de phishing por día. No son nombres de dominio. No son incidentes específicos. Son solamente informes y algunos de estos provienen, por ejemplo, de tool bars de Internet que manda muchas duplicaciones y que van individualmente a eliminar esos duplicados. Ese es un esfuerzo significativo.

Cuando nosotros damos cuenta de esto, esto representa alrededor del 3% de esos informes que son accionables y que quizá ya no funcionan o que les falta información. Hay mucho ruido entonces en este canal. Es muy difícil llegar a incidentes legítimos y específicos. Esto también es algo que podemos analizar desde el punto de vista operativo y tratar de focalizarnos en el problema legítimo. Siguiente diapositiva, por favor.

Esto no está exactamente vinculado pero parte del mismo tema es focalizarse en las campañas de fraude asociadas con la pandemia. Esto, por supuesto, dominó los titulares en la primera parte del año y creo que Mason se refirió a los picos que vimos en marzo y en abril cuando prácticamente todo el mundo estaba de algún modo en algún tipo de cuarentena. Creo que lo importante aquí es que estas fueron cuestiones focalizadas en el contenido y que no eran nuevas. Lo que sí veíamos es que tenían un envoltorio diferente. Las ansiedades que las personas tenían al principio de la pandemia sí lo indicaban pero por debajo de ese mismo tipo de fraude que nos hemos encontrado en los últimos años, en nuestro caso, en GoDaddy, a nosotros no nos pareció

que teníamos que hacer nuevos términos de servicio, políticas o capacidades. Encontramos que nuestra caja de herramientas funcionaba muy bien contra las amenazas, los fraudes del COVID-19. Parte de esa mitigación también iba ocurriendo como web host y no necesariamente con ataques en el DNS.

Creo que aquí hubo unas preguntas y unos comentarios de Chris sobre las medidas preventivas o proactivas. Nosotros recibimos muchas propuestas e incluso presión de gente de la política, figuras de la política. Nos dijeron simplemente: "Bloqueen COVID en el DNS. No permitan que nadie registre ese nombre, que nadie registre coronavirus. Todo va a ser cosas malas con eso". Yo reconozco este tipo de solución pero debo decir que es mucho más complicado que eso en el campo. La mayor parte de los usos abusivos que vemos no se refieren al COVID ni al coronavirus específicamente y no pueden ser detectados por un método. Al mismo tiempo, nosotros estamos viendo muchas autoridades de salud y canales de noticias locales, y otros que utilizan todo esto para actualizaciones de noticias.

Cuando vemos la sofisticación en ICANN, lo que vemos por fuera de ICANN donde nos piden que bloqueemos cosas en el DNS como solución, todos reconocemos que si bien esto es tentador no es necesariamente el enfoques que se debe tener ni tampoco es efectivo ni tiene un nivel aceptable de falsos positivos. Siguiente diapositiva, por favor. Creo que es la última.

Esta es mi última diapositiva. El punto es que obviamente el uso indebido es algo importante. No es que lo estemos poniendo debajo

de la alfombra pero nuestra función como registros, registradores y nuestros contratos con la ICANN indican que tenemos funciones muy limitadas. Tenemos algunas herramientas que podemos utilizar en otros ámbitos. Pensamos que es importante hablar acerca de estos temas en la ICANN para facilitar el intercambio de ideas para tener más perspectivas de otras áreas de la comunidad, la investigación que está haciendo SSAC y OCTO es importante. Recopilar datos de toda la industria resulta útil.

Creo que esto no va a sorprender a nadie. Creo que vamos a ver ciertas dudas en las partes contratadas en cuanto a lanzar nuevos proyectos de desarrollo de políticas o límites contractuales en este sentido. En primer lugar creo que necesitamos definir muy ajustadamente qué es lo que está dentro del ámbito de la jurisdicción de la ICANN y, en segundo lugar, y esto se remite a lo que dijo Elliot en relación con la diapositiva de Mason, creo que tenemos que asegurarnos de agotar todos nuestros mecanismos contractuales actuales para apuntar a esa pequeña cantidad de malos actores o al lugar donde se concentran en lugar de redactar nuevas políticas que podrían o no probarse para ver si funcionan con esto. Si tenemos algunos métodos que ya funcionan, cómo podemos utilizarlos para adoptarlos e implementarlos más ampliamente. Este es el fin de mi presentación. Thomas, gracias por incluirme y por invitarme.

THOMAS RICKERT: Gracias, James. Tenemos una pregunta dirigida a usted de modo que quisiera leerla. Es de [inaudible]. Una pregunta para James. ¿Los

sistemas de notificación de confianza serían una buena mitigación para todo el ruido que usted mencionó?

JAMES BLADEL: Creo que sí. El sistema de notificación de confianza es una buena forma de contar con un filtro para esos falsos positivos e informes duplicados. Todo lo que podamos hacer para que nuestros equipos y nuestras herramientas estén centrados en la amenaza propiamente dicha creo que vale la pena explorarlo.

THOMAS RICKERT: Muchas gracias. Tenemos 17 minutos antes de llegar al fin de la sesión. Hay preguntas en la ventana de preguntas y respuestas que ya están respondiendo los panelistas. Quisiera dejar que eso siga ocurriendo en la ventana de preguntas y respuestas. Jeff Neuman mencionó el siguiente punto. Es una pregunta en torno al formato de estos debates en reuniones plenarias. Apunta a que debería producir recomendaciones o resultados concretos. Creo que ya todos hemos escuchado presentaciones similares pero no sé si siempre terminamos con los mismos mensajes de cierre. Quisiera ver si puedo pedirles a ustedes que me den algunos mensajes de cierre de forma tal que podamos terminar con un resultado más concreto.

En primer lugar, quisiera pedirles al público y a los miembros del panel que se refieran a la definición de uso indebido del DNS porque las medidas pueden ser proactivas o reactivas. Pueden ser llevadas a cabo por diferentes partes. Dependen de esta definición. Tanto en la

presentación de Chris Lewis Evans como en la presentación de James Bladel se habló acerca del marco del uso indebido y hay algunos puntos que se han subrayado con respecto a malware, botnet, phishing, farming con ciertas calificaciones en torno al tema de spam. Esta es una pregunta para Jeff. ¿No sería una idea posible que usted con SSAC trabajen a partir de eso dado que usted mencionó que está trabajando en torno a las definiciones? Quizá sería muy útil para todos contar con una forma común de entender qué es uso indebido y qué es lo que no es uso indebido.

Si tienen preguntas, por favor, pónganlas en la ventana de preguntas y respuestas. El personal de la ICANN me dice que considerando que tenemos poco tiempo quizá sea mejor no ir habilitando el audio de los participantes y es mejor que escriban las preguntas y nosotros vamos a leer y responder las preguntas. Jeff, ¿podría responder usted esta pregunta?

JEFF BEDSER: Gracias, Thomas. Un marco común para las definiciones es fundamental para resolver el problema pero cuando surjan nuevos tipos de delitos cibernéticos quizá no encajen dentro de esta definición. Creo que es un componente clave para todo tipo de soluciones en relación con el uso indebido, tener definiciones, un depósito de definiciones al que todos podamos recurrir para determinar si un fraude o un evento en particular encaja dentro de una categoría en particular.

THOMAS RICKERT: ¿SSAC consideró las definiciones ofrecidas por el marco de uso indebido del DNS y el documento correspondiente?

JEFF BEDSER: Muchas gracias, Thomas. Sí. Menciona esos dos trabajos específicamente en el capítulo acerca de las definiciones.

THOMAS RICKERT: ¿Hay algún otro miembro del panel que quisiera referirse, no digo en cuanto a estar de acuerdo sino referirse en términos generales a las definiciones? Si hay silencio, ¿puedo considerar que están de acuerdo con el hecho de que el documento del marco de uso indebido del DNS es un buen punto de partida para comenzar con las definiciones de uso indebido del DNS? No me refiero a ninguno de los miembros del panel en particular. Tenemos poco tiempo así que el que quiera hablar puede hablar y decirnos si les parece que las definiciones son adecuadas o no.

JAMES BLADEL: Thomas, yo podría referirme brevemente a este tema. Creo que es un buen punto de partida. Tal como ya se dijo, el informe de SSAC toma parte de ese trabajo tradicional. Creo que también hubo preguntas en el chat acerca de cuáles son los próximos pasos. No quiero que sigamos repitiendo lo mismo en la reunión 70, 71 y 72 de la ICANN. Quizá una forma de detener esta calesita es justamente ponernos de

acuerdo en las definiciones que están en el marco sobre la base del informe de SSAC y luego incluir allí el análisis de por qué es o no es adecuado por parte de la ICANN dentro de su función limitada y sus mecanismos limitados con registros y registradores hacer esa definición. El segundo punto es ver si hay otra parte responsable que debería ocuparse de esto. En ese caso tenemos que transferir el tema a esa parte responsable. Quizá ese es el abordaje que podríamos tomar. Creo que tenemos que avanzar en este sentido. Gracias.

THOMAS RICKERT: Gracias, James. Veamos entonces… Mason Cole. Adelante, Mason.

MASON COLE: Quería hablar acerca de lo que dijo James. Estoy de acuerdo con él en términos generales pero el marco y el informe de SSAC son buenos puntos de partida para comenzar a trabajar con las definiciones. Quiero repetir algo que dije en mi presentación. No quiero que trabajemos demasiado con estas definiciones. Creo que este es el momento de tomar medidas correctivas. Quizá dejemos de lado las medidas correctivas mientras tratamos de definir el problema. Creo que esto no debería ser así. Nos gustaría que la ICANN tome algunas medidas al respecto. Con respecto a lo que dijo [Michele], creo que podemos seguir reuniéndonos una y otra vez y hablar del uso indebido del DNS pero lo que realmente necesitamos hacer es tomar medidas concretas, dar pasos concretos. Espero que no nos quedemos demasiado restringidos a hablar de las definiciones.

JAMES BLADEL: Quizá la idea no es que hablemos entre los diferentes miembros del panel, no lo sé. Creo que tenemos una diferencia en este sentido, Mason. Contar con la definición y entender completamente la definición creo que es necesario para poder dar los próximos pasos. Quería enfatizar esto porque quizá no lo cubrí muy bien en mi presentación o no lo dejé muy en claro. No es que falte trabajo con respecto a este tema. Quizá sea menos visible dentro de la ICANN porque tiene lugar en otras áreas y con otros grupos de partes y empresas pero no es que estemos trabados en el mismo lugar y no estemos trabajando aquí sino que estamos trabajando en otras áreas.

MASON COLE: Estoy de acuerdo con eso. Tampoco es que quiera que haya un debate entre los miembros del panel pero siempre hablamos de los 8 a 10 malos actores. Quizá haya algunas otras cosas que estén teniendo lugar y quizá las partes contratadas estén ocupándose de esto detrás de escena y nosotros no lo veamos. Yo no sé si podemos verificar de alguna forma que haya un abordaje correctivo para esto. Me parece que no llegamos al punto deseado todavía. Muchas gracias, Tom.

THOMAS RICKERT: Gracias, Mason y James. Creo que esto es lo que viene esperando la gente, la interacción entre los miembros del panel. Me alegra que tenga lugar este debate. Creo que nadie debería tomarse el trabajo de políticas como excusa para no tomar medidas. Creo que las partes

contratadas al menos todas las representadas aquí están trabajando mucho en este sentido y creo que la parte de definiciones es crucial para hacer las cosas correctamente. Tenemos que asegurarnos de que los registros y los registradores tengan el espacio en el ecosistema y puedan tomar medidas adecuadas en función de lo que pueden hacer.

Lo mismo se aplica a la ICANN. Por ejemplo, ECO, la asociación con la que yo trabajo, también opera y habla con el público general acerca de CASM. James habló de esto en su presentación. Yo les pregunto si esto tendría que ocuparse de los registros o de los registradores o de las empresas de hosting y la respuesta que recibí es que deberían ocuparse de las empresas de hosting y dar de baja los sitios porque hay material ilegal que en muchos casos se publica y que tiene relación con el uso indebido y tenemos que ver que esto no siga siendo distribuido en la fuente. Tenemos que hacer eso correctamente.

El último punto al que quería referirme brevemente es que al parecer hay discrepancias en los datos estadísticos. Algunos dicen que los números están cayendo, otros dicen que el problema no se está resolviendo, que sigue igual. David, usted ya escuchó lo que dijeron los miembros del panel y usted también participó en los intercambios en el chat. ¿Podría explicarnos cuáles son los diferentes mensajes que escuchamos en relación con los datos estadísticos?

DAVID CONRAD: Lo que yo entiendo es que estamos viendo diferentes partes del mismo elefante. ¿Qué es exactamente el uso indebido del DNS, qué es lo que

se está midiendo exactamente? Alguno de los comentarios que hice en el chat en respuesta a algunas indicaciones de que algunos grupos están viendo números muy diferentes de los que estamos viendo nosotros en nuestros datos es que a nosotros nos interesaría mucho ver los datos de otros. Nosotros estamos tratando de recopilar todos los datos posibles, de brindar información a la comunidad para poder tener debates informados y cuantos más datos podamos darle a la comunidad, mejor esperamos que podremos entender la realidad subyacente bajo el uso indebido del DNS. Desde mi punto de vista, creo que los datos que tenemos sugieren que a lo largo del tiempo el uso indebido del DNS ha estado cayendo. Hay otros que consideran que el uso indebido está aumentando. Me gustaría mucho entender cuáles son los datos que están considerando y que llevan a estas conclusiones y estadísticas diferentes.

THOMAS RICKERT: Muchas gracias, David.

JAMES BLADEL: Creo que en parte es una indicación de la forma despareja en que está distribuido el problema en todo el sistema de DNS y de Internet. En la diapositiva de David vi que había algunos que estaban un poco alejados del núcleo estadístico. Algunos datos diferentes de los que vimos nosotros. Podría ser que el nivel de la marea no cambie pero de vez en cuando, una vez por año, quizá hay inundaciones. Quizá esta sea una de las diferencias que nosotros estamos observando. No es

que los números sean totalmente diferentes sino que quizá los estemos mirando desde un ángulo levemente diferente y en un periodo levemente diferente.

THOMAS RICKERT: Muchas gracias, James. Hay una pregunta más para Chris. Ahora que ya James y David también hablaron creo que sería útil recibir todos los datos estadísticos posibles para tratar de entender cuáles son los diferentes datos y diferenciar lo que estamos viendo, ver la diferencia entre datos y hechos. ¿Hay algunos debates o acciones que tomaría la comunidad de aplicación de la ley en relación con las definiciones para que todos trabajemos a partir de la misma base? ¿Quién podría responder?

CHRIS LEWIS-EVANS: Gracias, Thomas. Los organismos de aplicación de la ley están atravesando grandes cambios a lo largo de los últimos años. Están tratando de ser más transparentes en sus informes para que se entiendan las políticas subyacentes. Tenemos los informes de IC3, que son una buena indicación de este caso. ¿Cómo los alineamos a nivel global? Esto es algo muy interesante siempre y hemos tenido bastantes dificultades dentro de la ICANN para acordar un conjunto de estándares. Sin duda hay trabajo por hacer. Sin embargo, creo que lo que es más importante es comunicar los datos de la forma más transparente posible porque esto nos permitirá trabajar de forma más colaborativa y tomar medidas en todo el ecosistema.

THOMAS RICKERT: Muchas gracias, Chris. Nos quedan solo dos minutos. Voy a tratar de resumir y luego dar por cerrada la sesión. Hay muchos aspectos comunes, lo cual creo que es muy bueno. Creo que estamos alineados no solamente los miembros del panel están alineados sino que hay una alineación más general en torno a la necesidad de contar con definiciones comunes del problema, datos estadísticos comunes o puntos de datos comunes. Creo que también quedó claro que el problema podrá ser mayor, menor o diferente de lo que compartimos pero deberíamos encararlo juntos, con evidencias o con fuentes de datos que luego podrán correlacionarse con lo que tenemos. Hay un pedido de que se tomen medidas y se considera que esto va a ser muy útil.

También quisiera volver a un punto que señaló Jeff en su presentación. La educación. Hay usuarios que caen en los ataques de phishing u otro tipo de actividades. Creo que es una combinación de diferentes cosas, diferentes soluciones que podrían ser implementadas por parte de los diferentes actores, cada uno en su función respectiva dentro de la ICANN, cumplimiento contractual, aplicación de la ley u otros. Si pudiéramos trabajar en este sentido sería un muy buen punto de partida.

Yo no estoy involucrado en la creación del documento del marco de uso indebido del DNS pero hay muchos que apuntan a ese documento. Quizá esa podría ser una recomendación que podría actuar como base para hablar acerca de cosas tales como definición, notificación de

confianza, etc. Creo que no deberíamos reinventar la rueda sino aprovechar el trabajo ya realizado.

Finalmente, quisiera agradecer a los miembros del panel. Quiero agradecer al personal de la ICANN y en particular al equipo técnico por habernos ayudado a organizar esta reunión sin ninguna dificultad técnica. También quiero agradecerles a ustedes, los participantes. Es muy difícil participar de manera remota en reuniones que duran horas y horas sin poder encontrarse con la gente a tomar un café entre una reunión y otra. Muchas gracias por su participación, por su atención. Les agradezco a todos nuevamente. Doy por cerrada la sesión.

[FIN DE LA TRANSCRIPCIÓN]