ICANN73 | Foro virtual de la comunidad – Sesión de actualización del GAC sobre el PSWG y el uso indebido del DNS
Martes, 8 de marzo de 2022 – 14:30 a 15:15 AST

GULTEN TEPE: Bienvenidos a la ICANN73, informe actualizado del PSWG del GAC seguido por la sesión del uso indebido del DNS y deliberación sobre rondas posteriores del 8 de marzo a las 18:30 UTC. Hoy no vamos a nombrar a todos los asistentes para ahorrar tiempo pero sí van a figurar todos los nombres de los miembros del GAC presentes en el comunicado y en las actas.

Para asegurar la transparencia en el modelo de múltiples partes interesadas de la ICANN les pedimos que se conecten a las sesiones de Zoom utilizando su nombre completo. De lo contrario pueden ser retirados de la sesión. Si desean formular una pregunta o hacer un comentario, escríbanlo en la función de chat, e inicien y terminen la oración con la palabra QUESTION o COMMENT para que todos los participantes puedan ver esa intervención.

Las sesiones del GAC tendrán interpretación simultánea en los seis idiomas de Naciones Unidas y portugués. Los participantes pueden elegir el idioma en el que desean hablar y escuchar haciendo clic en el icono de interpretación que se encuentra en la barra de herramientas de Zoom.

Finalmente, esta sesión, como el resto de las actividades de la ICANN, se rige por los estándares de comportamiento esperado de la ICANN. En caso de que quieran interiorizarlo, pueden encontrar el enlace en el chat. Habiendo dicho esto, le doy la palabra a la presidenta del GAC, Manal.

MANAL ISMAIL: Muchísimas gracias, Gulten. Gracias por volver rápido de la pausa. Vamos a hablar del uso indebido del DNS durante 45 minutos y después sobre las rondas posteriores en los próximos 45 minutos. Tenemos aquí a los responsables de cada tema y también a oradores invitados sobre la mitigación del uso indebido del DNS. Vamos a tener a la gente del grupo de trabajo de seguridad pública: Laureen Kapin, Comisión Federal de Comercio de los Estados Unidos, copresidenta del PSWG; Chris Lewis-Evans, de la Agencia Nacional de Delito de Reino Unido, también copresidente del GAC; Gabriel Andrews, del FBI de Estados Unidos; nuestro orador de parte del GAC es Sumitaka Shirakabe, de Japón, Ministerio del Interior y Comunicaciones. Tenemos un orador invitado además del representante de Japón que es Ivett Paulovics, coautora de un estudio de uso indebido del DNS en la Comisión Europea. Tenemos muchos temas para hablar. Sin más le voy a dar la palabra a nuestros disertantes. El primero, por favor. Adelante.

LAUREEN KAPIN: Esta vez soy yo. Voy a hablar esta vez como copresidenta del grupo de trabajo de seguridad pública. Siguiente imagen, por favor. Aquí tenemos una hoja de ruta de qué es lo que vamos a hacer en esta sesión breve y condensada. ¿Por qué la mitigación del uso indebido del DNS es importante? Vamos a escuchar hablar de un estudio reciente de la Comisión Europea sobre el uso indebido del DNS. Tenemos aquí a quien hizo parte de este estudio y nos va a presentar información adicional.

También vamos a hablar de unos hechos recientes que tienen que ver también con la nueva iniciativa del grupo de estudio técnico sobre la seguridad del DNS. Parte del trabajo realizado por el SSAC también tiene que ver con esta nueva herramienta de informes realizados sobre el uso indebido centralizado que tiene que ver con el Instituto de Uso Indebido de los Nombres de Dominio. También tenemos a representantes de la GNSO, que forman parte del equipo reducido sobre el uso indebido del DNS.

También vamos a hablar de la sesión plenaria que va a tener lugar sobre el uso indebido del DNS y se va a hablar de un tema muy importante. Las diferencias entre dominios registrados maliciosamente y dominios comprometidos, qué significa esto desde el punto de vista del uso indebido del DNS. Vamos a hablar de nuestro trabajo futuro. Vamos a escuchar a nuestro colega de Japón, que va a hablar también de cómo puede haber disposiciones mejoradas en los contratos y también de las mejores prácticas en las evaluaciones y estudios. Ahora pasemos a la siguiente imagen.

Una vez más, siempre tratamos de dar algún tipo de historia o antecedentes de qué se tratan estas cuestiones, por qué son importantes para el GAC. Vamos a escuchar hablar mucho. Va a haber discusiones y debates sobre las definiciones pero queremos dar parte de cuáles son los distintos rangos de definiciones. Cuando hablamos del uso indebido del DNS fue entendido como amenazas a la seguridad. Puede ser phishing, software malicioso, botnets. Todo esto surge de las medidas de protección de Pekín del GAC. Este texto, esta redacción es la que figura en los contratos, que son amenazas a la seguridad que deben ser tenidas en cuenta por los registros pero también existen otras definiciones. Por ejemplo, el equipo de revisión de confianza, seguridad del consumidor.

Hubo una definición que era parte también de un estudio anterior de ICANN o un documento previo de la ICANN que habló de actividades no solicitadas, engañosas, que hacen uso activo del DNS y los procedimientos utilizados para registrar los nombres de dominio y también voy a hablar entonces de una declaración del GAC sobre uso indebido del DNS que incluye más detalles, actividades que pueden constituir un impacto sobre los consumidores y también hay algo que resulta bastante familiar y que tiene que ver con el estatuto de la ICANN, que habla de una amenaza para la infraestructura del DNS. Cuando hablamos del DNS estamos hablando del sistema de nombres de dominio y todas estas actividades que pueden afectar su infraestructura, la seguridad, la estabilidad y la flexibilidad.

Nos vamos a concentrar también en el uso indebido del DNS en los temas de seguridad pública porque sabemos que este grupo es un

canal también que, junto con la gente de protección, seguridad y elección del consumidor ha dado asesoramiento y apoyo al Comité Asesor Gubernamental sobre estos temas porque ellos también son expertos al respecto.

En 2015 se formó el grupo. Tuvimos un plan de trabajo haciendo referencias a las formalidades que tenían que ver con ser un grupo de trabajo dentro del Comité Asesor Gubernamental. No se trata solamente del GAC y el grupo de trabajo de seguridad pública sino que hay muchas partes interesadas dentro de la ICANN que han hecho del uso indebido del DNS una de sus prioridades porque reconocemos que los contratos actuales de la ICANN no proveen obligaciones legalmente vinculantes y oponibles para mitigar el uso indebido del DNS.

Este tema se puede encontrar en declaraciones de cumplimiento de la ICANN, discusiones en la comunidad, correspondencia de la junta directiva también, donde hay una carta específica del 12 de febrero de 2020 de la junta directiva que hace referencia a que hay algunas disposiciones del contrato que no eran suficientemente claras como para que las obligaciones fueran oponibles. El GAC también ha dado sus aportes en distintos lugares que incluyen equipos de revisión, comentarios públicos sobre el trabajo de estos equipos de revisión y también participación en los trabajos de desarrollo de políticas. Estos son los antecedentes. Aquí tienen varios enlaces que son muy útiles. Después pueden ir a estos enlaces y visitar esos documentos donde van a obtener información valiosa. Siguiente imagen, por favor.

Vamos a hablar un poco entonces de algunos hechos recientes. Algunos de ellos son muy detallados y uno de ellos es el estudio muy detallado de la Comisión Europea sobre el uso indebido del sistema de nombres de dominio. Yo voy a dar una breve introducción antes de darle la palabra a mi colega. Fue un estudio nuevo que fue encomendado por la Comisión Europea, presentado a fines de enero. Se le comunicó al GAC a principios de febrero. Tuvimos la suerte en el grupo de trabajo de seguridad pública de tener una presentación en una llamada en conferencia en febrero.

Algunas observaciones generales sobre este estudio. Es muy práctico. Se concentra en los roles y las responsabilidades de todo el ecosistema, cosa que resulta muy útil. No se concentra solamente en las partes que sufren ese uso indebido, los atacantes y quienes hacen uso indebido sino también los intermediarios. No solamente las partes contratadas de la ICANN, por así decirlo, sino incluso entidades no partes que también son parte del sistema. Cuando digo esto, quiero decir que no estamos hablando solamente de los registros y los registradores sino que habla también de qué pueden hacer los que proveen hosting y los revendedores, como otros intermediarios. También qué es lo que pueden sumar los organismos de seguridad y la educación al consumidor al respecto.

Hay muchas recomendaciones y observaciones en el estudio que también aparecieron en otros trabajos de la comunidad. Por ejemplo, el SSAC, el Comité Asesor de Seguridad y Estabilidad, y otros equipos de revisión que incluyen al de seguridad, flexibilidad y estabilidad 2, y el CCT, que también mencioné anteriormente.

Una de las cosas que realmente es interesante y necesaria es la observación de que es muy difícil hacer una diferencia entre el abuso técnico y el de seguridad que puede ser phishing, pharming, botnets, software malicioso y lo que tiene que ver con el uso indebido vinculado con el contenido. Muchas veces, la línea divisoria realmente está borroneada entre los distintos tipos de uso indebido.

Hay un ejemplo, más de un ejemplo debería decir, en el estudio pero uno habla del phishing, que puede incluir también un dominio registrado maliciosamente. Uno puede recibir un correo electrónico que diga: "Haga clic en este enlace" pero entonces se accede a sitios web que tienen un contenido malicioso. No es nada más que un tema de seguridad técnica del uso indebido del DNS sino que aquí también estamos hablando de un uso indebido del DNS vinculado con el contenido.

Podemos hablar también de un software malicioso, por ejemplo, que nos puede llevar a un sitio web con contenido malicioso. Va a haber toda una sesión plenaria sobre los dominios registrados maliciosamente y los dominios comprometidos. Aquí tenemos dos temas paralelos. Quiero que ustedes entiendan la complejidad de todo el ecosistema aquí. Es muy importante también entender cómo esto se relaciona con los estatutos de la ICANN y qué es lo que puede hacer la ICANN al respecto. Vamos a la siguiente imagen, por favor.

Aquí tenemos la última observación que voy a hacer yo antes de escuchar directamente de uno de los autores del estudio. Estos son algunos de los hallazgos, algunos de los hechos que surgieron. Algunos

son de importancia específica para el GAC. Los nuevos gTLD están dentro de los grupos que más uso indebido sufren de los TLD. Pueden ver aquí una flecha que está hablando de más de un 6%. Ese es el porcentaje de los nuevos gTLD que están en el mercado. De todos los TLD, los nuevos gTLD son el 6% pero cuando miramos el uso indebido en los dominios, podemos ver que ese porcentaje que tienen los nuevos gTLD en el caso del uso indebido de dominios aumenta mucho más que ese 6%. Aquí estamos hablando de más de un 20%.

Esto es muy importante sobre todo cuando estamos hablando de las nuevas rondas de gTLD que se van a desarrollar en breve. En cuanto a los que sufren más uso indebido, estamos hablando de 41% que sufre la totalidad del uso indebido. Está concentrado. No son todos los nuevos gTLD pero sí hay algunos nuevos gTLD que sufren esta concentración de uso indebido. Esto se da a nivel de los registradores. También aquí vemos alguna concentración. Los cinco registradores con mayor uso indebido representan el 48% de todos los nombres de dominio registrados maliciosamente. También se puede observar que los registradores y los proveedores de servicio que sufren el uso indebido también pueden responder a los informes de uso indebido y pueden tomar una acción rápida y decisiva para tener un impacto sobre el perjuicio del uso indebido.

Los gobiernos también tienen que informar de este uso indebido porque muchas veces los proveedores de servicios y los registradores toman esto con mucha seriedad. Habiendo dicho esto, le voy a dar la palabra directamente a la autora del estudio de la Comisión Europea.

Quiero agradecerle específicamente por estar con nosotros, Ivett, y compartir parte de lo dicho en este estudio.

IVETT PAULOVICS: Muchas gracias, Laureen. Muchas gracias por recibirme. Debido al tiempo que tenemos disponible voy a pasar directamente a mi presentación. Les pido que por favor la pongan en pantalla. Muchas gracias. Bien. Voy a hablar acerca de los objetivos del estudio que la Comisión Europea nos encomendó, la metodología utilizada, los plazos, la definición que estamos proponiendo para uso indebido del DNS, la magnitud de nuestras mediciones, las buenas prácticas que hemos identificado y nuestras recomendaciones. Siguiente diapositiva, por favor.

Los objetivos de este estudio eran bastante amplios. El estudio fue encomendado para identificar una definición de uso indebido de DNS, ver las tipologías, las categorías, el rol de los actores implicados y también evaluar la magnitud de este fenómeno de uso indebido del DNS. También tenemos que tener en cuenta las políticas, las leyes y las prácticas internacionales y las prácticas de la industria. Dentro de lo posible, el objetivo era identificar buenas prácticas que se pudieran aplicar a otros actores intermediarios y también a nivel de la ICANN y de la Unión Europea. Además, el objetivo fue identificar medidas necesarias para abordar el uso indebido del DNS.

Con respecto a la metodología aplicada, por una parte hicimos una investigación directa con mediciones en tiempo real, encuestas,

entrevistas y talleres. Contamos con la participación de una gran cantidad de expertos. Durante las mediciones en tiempo real analizamos más de 2.700.000 incidentes y alrededor de 1.68 millones de nombres de dominio que fueron objeto de uso indebido y que estaban incluidos en listas de mala reputación de URL. Asimismo, hicimos una amplia revisión de informes presentados por terceros en nuestra investigación secundaria. El estudio insumió un año. Hicimos las mediciones en el segundo trimestre de 2021. Siguiente diapositiva, por favor.

Con respecto a la definición de uso indebido del DNS, Laureen ya mencionó la limitación de cierta terminología que se utiliza y se viene utilizando hasta el momento. Vemos que es bastante difícil diferenciar entre amenazas relacionadas con cuestiones técnicas y con contenido debido a que se superponen frecuentemente este tipo de amenazas. Por lo tanto, proponemos utilizar una definición más amplia. El uso indebido del DNS es toda actividad que hace uso de nombres de dominio o del protocolo del DNS para realizar actividades ilegales o que pueden causar un daño.

Nuestro enfoque es un enfoque desde las bases. Analizamos cada incidente y lo que cabe señalar con respecto a nuestro enfoque es que diferencia entre nombres de dominio registrados con una intención maliciosa y nombres de dominio que están comprometidos. Es decir, aquellos que están registrados por sus registratarios pero que más adelante se ven comprometidos por distinto tipo de actores maliciosos.

¿Cómo categorizamos el uso indebido del DNS? Tenemos tres categorías. En primer lugar tenemos a los nombres de dominio que fueron registrados de manera maliciosa. En segundo lugar el uso indebido relativo a la operación del DNS y a otras infraestructuras y en tercer lugar el uso indebido en relación a dominios que se usan para distribuir contenido malicioso. Con respecto a esta tercera categoría, incluimos los dominios comprometidos o registrados con fines maliciosos.

Este enfoque es importante porque permite diferenciar entre nombres de dominio registrados con fines maliciosos y nos permite ver quién tiene que responder y actuar con respecto a este uso indebido del DNS. Luego tenemos en estos dominios algunos dominios que se generan con algoritmos para comunicaciones de comando y control. En nuestra opinión, esto se puede remediar a nivel del DNS. Los intermediarios que tienen que actuar están en ese nivel, en el nivel del DNS.

Con respecto al contenido malicioso, se puede distribuir mediante dominios registrados con fines maliciosos. Por ejemplo, dominios destinados a phishing. En ese caso, las medidas de remediación se tienen que hacer a nivel de host y también a nivel del DNS. Esto se debe a que la mitigación de este tipo de uso indebido en un solo nivel no sería efectiva.

En caso de distribución de contenido malicioso a través de un dominio comprometido. Por ejemplo, dominios comprometidos que distribuyen contenido de phishing, no sería de utilidad resolver este

uso indebido a nivel del DNS porque puede causar un daño colateral al registratario legítimo y también a los usuarios. En ese caso, proponemos que la remediación se haga a nivel del host. Con respecto al uso indebido en cuanto a las operaciones del DNS, debe ser abordado a nivel del DNS. Vemos que con nuestra definición propuesta también vienen acciones de remediación.

Ahora hablemos acerca de la magnitud del uso indebido del DNS. Laureen mencionó uno de los gráficos, lo describió. Es uno de los gráficos del estudio. Nosotros hicimos una medición en los TLD y vimos si el uso indebido se da en dominios maliciosos, si se implica a la reputación del registrador o la de otros actores.

Con respecto a los TLD, como dijo Laureen y vemos en este gráfico, se compara la participación del mercado de cinco grupos de TLD. Nuestra conclusión es que los ccTLD de la Unión Europea son los que sufren la menor cantidad de uso indebido en ambos casos. Lo podemos ver en los gráficos. Vemos que los ccTLD de la Unión Europea tienen el 14.44% de participación del mercado y menos del 1% del uso indebido.

En términos relativos los nuevos gTLD, como dijo Laureen, tienen una participación de mercado que vemos en el gráfico. Son los que sufren el mayor porcentaje de uso indebido. Vemos también en los resultados del estudio no significa esto que todos los nuevos gTLD sufran uso indebido. Vemos que la mayoría de estos gTLD representan aproximadamente el 41% de todo el uso indebido. Siguiente diapositiva, por favor.

Ahora vemos la distribución de los dominios comprometidos y registrados de manera maliciosa. Aquí vemos que aproximadamente el 24% y el 41% de dominios donde hay phishing y malware están comprometidos a nivel del host mientras que la vasta mayoría que se utilizan para spam y botnets y comando y control fueron registrados de manera maliciosa. Siguiente diapositiva, por favor.

Aquí vemos la distribución de los dominios comprometidos y registrados de manera maliciosa a nivel de los TLD. Siguiente diapositiva, por favor. Como les dije, hicimos una medición de la reputación de los registradores y observamos que los registradores que son objeto del uso indebido representan el 48% de todos los nombres de dominio registrados de manera maliciosa. También notamos que entre los proveedores de hosting hay una concentración desproporcionada de nombres de dominio dedicados al spam. Vemos que las extensiones de seguridad del DNS y su nivel de adopción y los protocolos para protección de correos electrónicos continúan a un nivel que sigue siendo bajo. Siguiente diapositiva, por favor.

Por último, después de analizar todas las políticas a nivel internacional, a nivel de la ICANN, a nivel de la Unión Europea y también normas regulatorias identificamos buenas prácticas de distintas categorías. Las analizamos, las categorizamos en preventivas, reactivas y también buenas prácticas en materia de transparencia e información. Hemos identificado intermediarios. Pueden verlos allí, en los ejemplos. Tenemos ejemplos de ccTLD y de algunos registros de gTLD también. Debido al tiempo disponible, no voy a entrar en más detalle acerca de las buenas prácticas. Este estudio incluye un análisis

exhaustivo al respecto. Ahora voy a pasar a la próxima diapositiva, por favor.

Finalmente, en el estudio formulamos 27 recomendaciones y las agrupamos en seis áreas para mejorar las medidas de mitigación del uso indebido del DNS. También tenemos recomendaciones de carácter técnico. No las puedo mencionar todas. También recomendaciones en materia de políticas. Por ejemplo, tenemos recomendaciones que tienen que ver con los intermediarios.

Con respecto a los revendedores, a los registros, a los registradores, recomendamos un sistema de informe de uso indebido que sea centralizado para identificar los datos de registración del dominio correspondiente y poder así actuar y monitorear los índices de uso indebido y también aplicar sanciones e incentivos para que los niveles de uso indebido estén por debajo de un umbral predeterminado. Con respecto a los proveedores de servicio de hosting, tenemos recomendaciones similares. Es decir, monitorear los niveles de uso indebido que tendrían que estar por debajo de un umbral determinado.

En la última de las áreas tenemos el tema de la colaboración. Nosotros recomendamos hacer una unificación de la operación de los ccTLD en el marco de buenas prácticas que permita colaborar con las instituciones gubernamentales, con las autoridades de cumplimiento de la ley y con notificadores confiables. Con lo cual, tenemos varias recomendaciones que, como dijo Laureen, tienen que ver con distintos tipos de estudios y análisis. En este caso en particular, este estudio

apunta a brindar una reseña completa de este fenómeno observado en el año 2021.

Esa fue mi última diapositiva. En la próxima diapositiva pueden ver los enlaces para acceder al estudio, para descargarlo. Por supuesto, se pueden poner en contacto conmigo o con la persona que redactó el informe junto conmigo. No puede estar en esta sesión porque está en este momento en una sesión de la unidad constitutiva de negocios. Muchas gracias por su tiempo y por su atención.

LAUREEN KAPIN: Muchas gracias. Veo que hay preguntas en la sala de chat. Veo que hay gente que quiere tomar la palabra. Vamos a concentrarnos en las preguntas que tienen que ver con el estudio en particular. También vamos a pedirles a todos que sean conscientes de los temas tratados. Creo que Finn, Susan y Gemma están formulando preguntas. Finn pregunta si hay algo en cuanto a las recomendaciones que sería particularmente fácil para poder tomar medidas a la brevedad posible. Ivett, creo que esa pregunta es para usted.

IVETT PAULOVICS: Sí, Laureen. Gracias. Claramente no es una pregunta sencilla. Este estudio fue encomendado por la Comisión Europea. Por ejemplo, para la Comisión Europea sería mucho más fácil dirigirse a los ccTLD dentro de la Unión Europea para unificar las operaciones, el funcionamiento de los ccTLD y adoptar buenas prácticas. Dentro de la ICANN quizá haya otras prioridades y otras recomendaciones que se podrían

adoptar con mayor facilidad porque hay otras áreas de trabajo en curso y en paralelo.

ESTADOS UNIDOS: Gracias, Laureen. Realmente agradezco el estudio que hicieron sobre el uso indebido del DNS. Me parece que es un recurso muy importante para los formuladores de política, para que podamos entender mejor lo que tiene que ver con la parte técnica y comercial así como las actividades legales que tienen lugar en la Internet.

Me parece que en este momento la definición del uso indebido del DNS es muy amplia para poder ser utilizada dentro de ICANN. Estamos hablando de las actividades ilegales que también se dan por fuera de la ICANN y por fuera de sus estatutos pero creo que este es un lugar donde se puede facilitar el intercambio y también donde pueden intervenir los expertos del gobierno en temas de Internet.

Si bien algunas de estas cuestiones quizá están por fuera de lo que marcan los estatutos de la ICANN, agradecemos este estudio, reconocemos su utilidad y también reconocemos que el uso indebido del DNS, si la definición es correcta, puede ser utilizada tanto dentro de la ICANN como fuera de la ICANN. Muchísimas gracias.

LAUREEN KAPIN: Le doy la palabra a Gemma.

GEMMA: Espero que me escuchen bien porque tengo algunos problemas de audio y además me veo a mí misma. Muchísimas gracias, Ivett, por la presentación y también [inaudible] estuvo hablando en otras sesiones en paralelo. En primer lugar muchas gracias porque nuestros contratistas han sido muy útiles en difundir el trabajo realizado y además porque desde nuestro lugar también fue como un impulso para ellos, para participar de un diálogo con la comunidad de la ICANN en diversos foros, en la mayor cantidad posible de hecho. Muchísimas gracias, Ivett.

Como Laureen mencionó al comienzo, hubo una presentación también muy extensa del PSWG. Realmente tuve una respuesta positiva al resumen que hizo Laureen al principio. De hecho, hay cosas que fueron debatidas dentro del PSWG y creo que pueden ser consideradas en estas cuestiones porque realmente es algo que puede verse dentro del contexto del contrato o los contratos con la ICANN. Tiene que ver con el uso indebido del DNS, tiene que ver con la ICANN. Se debatió muchísimo después de la emisión del informe del SSR2 y también es algo en lo que está trabajando el PSWG.

Quiero decir un par de cosas. En primer lugar, nuestra metodología o nuestro enfoque es que este es un estudio independiente. Nosotros se lo pedimos a expertos por fuera de la Comisión Europea. Yo diría que quisimos hacer este estudio incluso sin un plazo específico para una iniciativa de política que es lo que suele suceder en la Comisión Europea porque este es un tema de mucha importancia para nosotros. Queremos evitar todo este uso indebido del DNS que además es algo

central en lo que tiene que ver con la estrategia de ciberseguridad europea del 2020.

Nuestra intención para darle la visibilidad más amplia posible y además el tiempo de poder debatir este estudio en la ICANN tiene que ver con que la ICANN es igual al DNS para decir algo simplista. Nosotros nos seguimos recordando que la ICANN es el lugar donde hay que debatir el DNS y donde hay que tomar acciones respecto del DNS. Es por eso que queríamos que el estudio fuera muy visible en la agenda de la ICANN y es muy importante que las distintas unidades constitutivas tengan la posibilidad de hacer comentarios al respecto. Esto no es la biblia. Es un estudio independiente nada más. Es por eso que hay elementos aquí que tienen que ser revisados o comentarios que puedan ser expresados, incluso porque hay diferencias pero este no es un estudio sobre la ICANN. De ninguna manera.

Creo que es la segunda o la tercera vez que se presenta este estudio. Quiero detener la retórica sobre qué puede hacer la ICANN. Esto está por fuera del área de incumbencia de la ICANN. Yo creo que todos en la comunidad están interesados en evitar el uso indebido del DNS. Es un tema muy complejo este porque, como fue presentado muy bien por Ivett, no comienza y termina con un registro malicioso de un nombre de dominio. Puede suceder después de la registración del nombre de dominio. Puede darse mucho después y puede implicar a distintos actores. Creo que los esfuerzos que han hecho los contratistas sobre todo analizando el uso indebido del DNS de manera holística yo creo que es el principal valor agregado. Estamos mirando el uso indebido del DNS desde quienes lo sufren.

Hay una definición estricta sobre qué es exactamente el uso indebido del DNS. Si puede ser detenido, puede ser pausado como para decir: "Esto es lo que está sucediendo bajo el paraguas del uso indebido del DNS". Está sucediendo a través del uso o del registro malicioso en el DNS y estos son los actores que participan. Los podemos ver claramente y el estudio que es muy largo obviamente y no puede presentarse enteramente en este contexto mira explícitamente qué hacen los registros, registradores, revendedores, porque es un entorno muy complejo pero todo esto está identificado en el estudio y también qué es lo que pueden hacer los proveedores de hosting porque en algunos casos se identifica uso indebido de tipo uno, dos, tres, dependiendo del nivel en el que se dé el uso indebido y participa más de un actor.

En primer lugar hay que ver cuál es la aplicabilidad de los actores para informarle a uno y otro de qué es lo que está pasando. Esto tiene que ver con esta fruta madura, por así decirlo. Lo que surge rápidamente. Realmente fue una pequeña recomendación muy clara que marca muchas diferencias. Cuál es la responsabilidad de la organización, después qué hace con estas solicitudes y si los actores quieren comunicar que a nivel del DNS se pueden poner en contacto con los responsables de todo esto. También queda clara la necesidad de tener buenos registros de WHOIS que es obviamente otra de las conclusiones claras del estudio.

Por supuesto, es un tema muy largo y obviamente no quiero remplazar la presentación hecha por Ivett pero sí quiero decir que la gente de la comunidad de la ICANN tiene que tomar del estudio lo que les parece

útil. Hay muchas recomendaciones para los operadores. La Comisión Europea, como formuladores de política, vemos qué es lo que estamos haciendo de nuestro lado. Estamos evaluando las recomendaciones desde ese punto de vista pero queremos ver si la comunidad realmente puede tomar algo, consideran que hay algo que es valioso y ver qué es lo que sucede en el tiempo con esto, si hay mejoras o no. Realmente quiero decirles que veamos lo que se puede hacer en lugar de concentrarnos en el ámbito de incumbencia amplio o estrecho de la ICANN. Esto no tiene que ver solo con la ICANN sino con todo el DNS. Pido disculpas por esta larga intervención pero quería aclarar esto.

LAUREEN KAPIN: Gracias, Gemma. Manal, no sé si quizá podamos tomar unos minutos más porque hay preguntas y declaraciones sobre el estudio que realmente son muy útiles. Obviamente, cuando las cosas son útiles, nos demoran más tiempo. No tiene por qué responder esta pregunta ahora. Vamos a volver a las diapositivas. Vamos a reordenar las cosas un poco más. Bien. ¿Podemos ir directamente a mi colega de Japón para tener su material y después evaluar si podemos hacer una presentación general del material que nos queda? Le doy la palabra a mi colega de Japón. Muchísimas gracias por su paciencia.

SUMITAKA SHIRAKABE: ¿Me escuchan?

LAUREEN KAPIN: Sí.

SUMITAKA SHIRAKABE: Gracias, Laureen. Realmente agradezco esta oportunidad de poder hablar con ustedes. También sé que el tiempo es muy limitado. Rápidamente voy a compartir con ustedes esta imagen y les voy a contar algo breve. Durante la reunión del GAC en la ICANN72 compartimos el tema de lo que nosotros llamamos el salto de un registrador a otro o el hopping que hace un registratario para seguir haciendo uso del mismo nombre de dominio. Pasa de un registrador a otro registrador.

Ahora la cuestión es que querríamos compartir un caso en el registratario que parece ser el mismo y continúa haciendo un uso indebido utilizando distintos nombres de dominio registrados con el mismo registrador. Este es el tema actual desde nuestro punto de vista, desde el punto de vista japonés, donde podemos sugerir dos cosas. Una es garantizar un cumplimiento entre la ICANN y el registro y el registrador. Por supuesto, algunos colegas ya mencionaron este tema y es importante corregir la información que existe, la exactitud de esa información que existe en el momento de registrar el dominio. También es muy importante llevar adelante una auditoría continua y eficaz sobre el cumplimiento de parte de los registradores con el cumplimiento contractual de la ICANN.

Por otro lado podemos considerar algunas medidas en cuanto al uso indebido que se hace de los nombres de dominio. Podemos considerar

la posibilidad de utilizar algún tipo de programa de notificador confiable. Creo que esto sería útil, sobre todo cuando hablamos de un contenido malicioso específicamente y también podría sugerir la cooperación y la discusión con otras organizaciones de apoyo o comités asesores de la ICANN.

Me parece que en la reunión del GAC de ICANN72 hubo una reunión con ALAC donde se habló de promover este tema, quizá de armar un grupo reducido entre GAC y ALAC. Realmente esperamos ver esa acción. Hoy a la mañana también se mencionó el grupo de la ccNSO, que podría haber una acción más amplia dentro de estos grupos y la idea es colaborar con el GAC y con otros grupos también. Algunos colegas ya mencionaron que el tema de autenticación también es algo importante y que nosotros podríamos ver que la ICANN tomara una acción mayor aunque se ve limitada en algunos casos. Muchísimas gracias, Laureen, por haberme dado la palabra. Se la devuelvo.

LAUREEN KAPIN: Muchísimas gracias, Sumitaka. Le agradecemos la presentación.

MANAL ISMAIL: Sí, perdón por interrumpir, Laureen. Muchísimas gracias, Sumitaka. He hablado con Luisa y Jorge. Ustedes van a tener unos minutos más.

LAUREEN KAPIN: Ahora entonces querría ir para atrás para llegar… Perfecto. Esta era la que quería mostrar. Gabe, no sé si quiere aceptar entonces darnos esta misión general de este material que tenemos aquí.

GABRIEL ANDREWS: Gracias. Fue una excelente presentación sobre el estudio de la Comisión Europea pero no es el único estudio que ha publicado recientemente algunos datos. Quiero hablar de este trabajo que tiene que ver con la iniciativa de facilitación de seguridad del DNS y el grupo de estudio técnico. Esto es algo que el director ejecutivo de la ICANN solicitó en el 2020 y fue una respuesta a varios ataques de alto perfil que se dieron en el DNS en el 2018 y 2019, como pueden ser el Sea Turtle y DNSpionage, que creo que lo leyeron en las noticias.

El TSG, o el grupo de estudios técnicos, se concentró no solo en estos ataques sino en otros del mundo real. Tenemos ejemplos tomados de estos incidentes. Una de las mejores prácticas comunes que pueden darse para abordar estos incidentes podría decir que las recomendaciones tienen que ver con lo que se envió como recomendación a la oficina del director técnico de la ICANN. También puede haber otra comunicación que surgiera después de este estudio pero no hay una acción urgente que tenga que tomar el GAC al respecto pero quería señalar esto que había sucedido.

Si recuerdan bien, el año pasado el comité asesor de estabilidad y seguridad, el SSAC, publicó el SSAC115, que fue un informe sobre cómo abordar el uso indebido y cómo manejarlo. Tenía una

recomendación. Esa recomendación hablaba de la creación de un facilitador de respuesta común ante el uso indebido. Un año después estamos empezando a ver lo que puede ser un candidato posible para este facilitador de respuesta común ante el uso indebido. Puede ser el Instituto de Uso Indebido del DNS. Ellos están probando en este momento lo que llaman la herramienta de informe de uso indebido centralizado. Me parece que no es el nombre oficial pero por ahora lo llamamos CART.

Quizá pueda ser presentado en junio y quizá puede automatizar el enrutamiento e incluso en algunos casos mejorar la información sobre estos usos indebidos. Esto es algo nuevo. Es interesante y creemos que quizá en la próxima reunión de la ICANN podamos profundizar un poco más en esta herramienta.

Para cerrar con los otros hechos que se han dicho, tenemos entonces un equipo reducido de la GNSO que fue creado recientemente sobre el uso indebido del DNS. Como parte de su trabajo empezaron a compartir preguntas, preguntas también presentadas ante el GAC para entender un poco más cuáles son las expectativas de la GNSO y cómo las políticas futuras podrían contribuir a las iniciativas.

No voy a profundizar en las preguntas que están en la pantalla pero quiero que todos las tengan en cuenta porque este es el equipo reducido de la GNSO que quizá está buscando algunas respuestas antes del 21 de marzo. Si alguno quiere participar, por favor, responda estas preguntas.

Finalmente, aquí estamos. Mañana hay una sesión plenaria sobre los dominios comprometidos vs los registrados maliciosamente. Se va a hablar de este estudio de la Comisión Europea pero también se va a hablar de cómo hacer los escalonamientos, que es lo que tenemos con la herramienta que tenemos. Este es un panel que va a profundizar sobre este tema. Creo que nos puede resultar interesante. Ahora le devuelvo la palabra a Laureen.

LAUREEN KAPIN: La próxima, que creo que es la última. Este es el trabajo futuro. Acabamos de resaltar cuáles son las cosas sobre las que seguimos trabajando. La idea es mejorar los requisitos contractuales. También tenemos algún texto que incluimos en el último comunicado y que tenía que ver con disposiciones en los estatutos. La ICANN también puede negociar acuerdos que incluyan compromisos en pos del interés público en servicios de su misión. Esto se puede hacer junto con las partes interesadas y la ICANN para mejorar las disposiciones contractuales y que puedan entonces responder mejor al uso indebido del DNS.

También tenemos evaluaciones sobre el uso del DNS que deben hacerse y que tienen que ver con lo que recomendó el comité asesor sobre seguridad y estabilidad antes de lanzar la nueva ronda de nuevos gTLD que creo que esto tiene que ver también con la próxima sesión porque cuando estamos considerando una nueva ronda de gTLD obviamente siempre tenemos que mirar qué es lo que

aprendimos sobre el uso indebido del DNS en la última ronda y en general.

Habiendo dicho esto entonces, voy a pedir disculpas porque no podemos tener más tiempo para las preguntas que ustedes querrían formular pero sí los invito a trabajar en el grupo de trabajo de seguridad pública y a hablar con nosotros, no solamente durante estas reuniones sino en cualquier momento para poder mantener conversaciones con todos ustedes. Ahora sí estoy a tiempo como para entregarle la palabra al siguiente grupo.

MANAL ISMAIL: Sí. Muchísimas gracias, Laureen, Gabriel, Sumitaka e Ivett. Realmente fueron unas presentaciones muy interesantes. Muchísimas gracias realmente por el apoyo que nos dan a todos nosotros. Ahora entonces sin más le voy a dar la palabra a nuestros responsables del tema sobre los procedimientos posteriores.

[FIN DE LA TRANSCRIPCIÓN]