ICANN76 | Foro de la comunidad – Debate del GAC: uso indebido del DNS
Martes, 14 de marzo de 2023 – 10:30 a 12:00 CUN

JULIA CHARVOLEN: Bienvenidos a las discusiones del GAC sobre uso indebido del DNS el 14 de marzo a las 10:30 hora local. Tengan en cuenta que esta sesión está siendo grabada y se rige por los estándares de comportamiento esperado de la ICANN. En esta sesión las preguntas y los comentarios presentados en el chat se leerán en voz alta si están en el formato correcto. Si están en Zoom, levanten la mano y recuerden decir en qué idioma hablarán en caso de que no sea inglés. Hablen a un ritmo razonable para permitir una interpretación correcta. Silencien todos los demás dispositivos al hablar. Todas las funciones disponibles las encontrarán en la barra de herramientas de Zoom. Sin más, le doy la palabra a la presidenta del GAC, Manal Ismail.

MANAL ISMAIL: Muchas gracias, Julia. Buenos días, buenas tardes y buenas noches a todos. Bienvenidos nuevamente. Vamos a conversar dentro del GAC sobre la mitigación del uso indebido del DNS. Tenemos una sesión de una hora. Vamos a continuar hablando de las iniciativas de la comunidad de la ICANN y de la organización de la ICANN para prevenir y mitigar el uso indebido del DNS. También vamos a darles las novedades sobre los últimos acontecimientos y los esfuerzos que están realizando los miembros del GAC junto con la comunidad en su

conjunto para apoyar la ampliación de disposiciones contractuales y posibles procesos de desarrollo de políticas para mejor abordar el tema del uso indebido del DNS.

Sin más, le voy a dar la palabra a los responsables de los temas. En este caso tenemos a Gabriel Andrews, del Buró Federal de Investigación de Estados Unidos. También tenemos a Laureen Kapin, de la Comisión Federal de Comercio de Estados Unidos y copresidenta del PSWG. Chris Lewis Evans, de la Agencia Nacional de Delito del Reino Unido y también copresidente del PSWG. Le doy la palabra a Chris.

CHRIS LEWIS-EVANS: Buenos días, buenas tardes, buenas noches a todos. Vamos a pasar a la siguiente diapositiva, por favor, directamente. Vamos a tener una sesión sobre el uso indebido del DNS y tenemos una presentación externa. Veo que tenemos aquí a quien está a cargo de la red de políticas en materia de jurisdicción y de Internet en una esquina. Espero que preparemos las diapositivas con el apoyo del personal del GAC.

Rápidamente voy a explicar por qué es importante hacer frente al uso indebido del DNS. Vamos a dar algunas estadísticas vinculadas al delito y su vinculación con el uso indebido del DNS. Vamos a ver otras actividades que se están desarrollando dentro de la comunidad. Vamos a hacer un cierre con algunas consideraciones que puedan tenerse en cuenta para nuestro comunicado en la parte de asesoramiento o de asuntos de interés para el GAC. Siguiente, por favor. Gracias.

Siento como que no necesito que repasemos esta diapositiva. Venimos hablando del uso indebido del DNS desde hace mucho tiempo. Ha habido muy buenas sesiones ya durante esta reunión sobre este tema. Hablamos siempre del taller sobre desarrollo de capacidades del sábado con una sesión muy interesante sobre uso indebido del DNS. La pueden repasar. También hay una serie de enlaces aquí a los que pueden recurrir y, como siempre, pueden hacer una búsqueda dentro del sitio web del GAC con el término "uso indebido del DNS" y los va a llevar a las secciones del comunicado. El personal de apoyo del GAC, Benedetta y el resto de los integrantes, han hecho un muy buen trabajo dejando a disposición esos recursos.

Tenemos una serie de elementos que hemos destacado y esta es una parte muy importante del trabajo del PSWG. Tenemos un plan de trabajo que se ratificó y se avaló en esta reunión. Esto es muy bueno. Esto permite que todos los funcionarios encargados de la seguridad pública y de los organismos encargados de la aplicación de la ley realmente puedan trabajar mejor con las comunidades para prevenir y mitigar el uso indebido del DNS y con otras partes de la comunidad hay muchas deliberaciones, consultas con la junta directiva, correspondencia que se intercambia con la comunidad empresarial y todo para ver la importancia que tiene para todos ellos.

Tenemos el equipo de revisión de CCT, de RDS WHOIS2, SSR2, por mencionar algunos. También el PDP sobre los procedimientos posteriores que también hacen referencia al tema del uso indebido del DNS. Más adelante en la presentación vamos a hacer referencia a las partes contratadas. Se envió una carta a la junta directiva con respecto

a la apertura de las negociaciones contractuales para ayudar a abordar el tema del uso indebido del DNS. Es un muy buen paso adelante porque demuestra que la comunidad quiere actuar y ciertamente esto es un tema que venimos considerando desde hace tiempo. Voy a hacer una pausa y ver si ya tenemos lo que venía… No. Tal vez le voy a dar la palabra a Gabriel.

LAUREEN KAPIN: Aquí es donde queremos ser flexibles y adaptarnos a las circunstancias para poder pasar a lo que haga falta.

CHRIS LEWIS-EVANS: Gracias, Gabe. Sí. Ahora te toca a ti. Vamos a pasar a la presentación sobre las tendencias actuales. Creo que podemos avanzar dos diapositivas si no me equivoco. Muy bien. Gracias. Le doy la palabra a Gabriel.

GABRIEL ANDREWS: Hola. Soy Gabriel. Hablo a título personal como miembro del grupo de trabajo de seguridad pública. Lo que esperamos hacer en esta oportunidad es algo que tratamos de hacer en forma anual siendo optimistas. Cuando se trata de entender el alcance y la escala del uso indebido del DNS además de tratar de entender esto como parte del delito es importante saber que no tenemos hechos perfectos. Lo que sí tenemos son distintas perspectivas. Al igual que estos ciegos aquí, en esta imagen que ustedes reconocerán del ejercicio que se hizo en el taller de desarrollo de capacidades, nosotros hacemos nuestro mayor

esfuerzo por observar, hablar de lo que percibimos esperando que al colaborar podamos tener una idea mejor de lo que está realmente ocurriendo.

Aquí es donde reconozco que hay muchas iniciativas en la comunidad, muy buenas, todas dirigidas a aportar datos, medidas, indicadores, observaciones sobre el uso indebido del DNS. Pensamos, por ejemplo, en el informe Compass del Instituto del Uso Indebido del DNS, que comenzó el año pasado. También la oficina OCTO y todos los informes sobre el uso indebido del DNS de parte de la ICANN.

Hace dos días estuvimos hablando con el personal ejecutivo y John Crain dijo que esperamos los informes de uso indebido a nivel del registro pero también él tiene algunas ideas sobre la incorporación de la analítica predictiva y el aprendizaje automático para ver qué podemos obtener. Todo esto son perspectivas que podemos aportar y que también los organismos de aplicación de la ley pueden contribuir. Los informes, las denuncias de las víctimas que nos llegan, también sirven.

No estamos sugiriendo que todos los delitos tengan que ver con el uso indebido del DNS sino que estamos tratando de entender el alcance y la escala del perjuicio para las víctimas que hacen las denuncias. Tal vez esto es una perspectiva que debemos considerar en nuestras deliberaciones y ver cómo se pueden traducir esos informes, esas denuncias, al uso indebido del DNS, para saber cómo ocurre y de qué manera. Creo que con esto cubrí la primera parte, Chris.

CHRIS LEWIS-EVANS: Sí. Pasemos a la siguiente diapositiva. ¿Podemos volver una atrás? En la última reunión del PSWG nosotros convocamos a todos los miembros a que nos brindaran estadísticas que tenían sobre el ciberdelito y su posible relación con el uso indebido del DNS. Por el momento no hemos recibido más información que de Estados Unidos y del Reino Unido. Si ustedes trabajan con sus propios organismos de aplicación de la ley o con las agencias de protección de los consumidores, por favor, siéntanse libres de hacernos llegar esa información. Vamos a estar muy ansiosos de ver qué es lo que están haciendo otros países y tratar de que esta revisión sea un poco más amplia a nivel de estadísticas. Tenemos la intención de hacerlo una vez por año para tener una idea del panorama general.

Si vamos a los datos del Reino Unido, en el Reino Unido tenemos un único organismo que se llama Action Fraud, que no se ocupa solamente del fraude sino también del ciberdelito. Primero tuvieron ese nombre y luego agregaron el ciberdelito a su ámbito de competencia. Las cuatro estadísticas principales no hacen un seguimiento del uso indebido del DNS. Tenemos hacking a través de las redes sociales y del email. Tenemos software malicioso y virus, que también están incluidos. En realidad esto no se alinea con lo que nosotros entendemos como uso indebido del DNS. Luego hacking a nivel personal o a nivel de extorsión. Esto tiene más que ver con el ransomware. Como ustedes pueden ver en esta diapositiva, los datos se remontan al 2014 y hay una tendencia ascendente en general en las denuncias y en los informes de este tipo de delitos. Siguiente, por favor.

Una de las cosas que también hacen son encuestas con empresas, organizaciones benéficas, para tratar de entender cómo se han visto afectadas y cómo se han manejado ante esas situaciones. Este dato que se analiza aquí tiene que ver con cuántas organizaciones han identificado algún tipo de irrupción o de ataque sobre su sistema. Se ha mantenido bastante estático, incluso del lado de las empresas con una tendencia levemente descendente pero para las organizaciones benéficas sin duda hay un alza en esta tendencia. Estas organizaciones antes del GDPR tal vez no estaban preparadas para analizar sus propias redes. Una vez que uno empieza a buscar algo tiende a encontrarlo. Este es uno de los motivos por los que vemos este aumento, porque están buscando algo y terminan encontrándolo. Que esto muestre un aumento en los ataques es difícil de decir. Podría ser pero es difícil de confirmar. Vemos este tipo de tendencia allí. Siguiente, por favor.

En esta diapositiva obviamente de todos aquellos que han sufrido algún tipo de ataque, algún tipo de infracción vemos cómo lo identifican, cuáles el vector de ataque inicial. A lo largo de los años, la respuesta para el 80% de las veces ha sido el phishing. Phishing sin duda entra en el ámbito del uso indebido del DNS. Para otros tipos de delitos que teníamos, el 80% se relaciona con la suplantación de identidad con el phishing. Cuando se reduce el phishing podemos reducir el perjuicio causado por los otros delitos con los que trabajamos a diario. En segundo lugar, parecido al phishing tenemos algo más focalizado con dominios que parecen verídicos o emails con spoofing y ese tipo de cosas. Aquí puede haber un poco de superposición también. Siguiente.

Lo mismo hicimos para las entidades benéficas y tuvimos respuestas muy similares. El 80% corresponde a phishing. Aquí hay un análisis muy contundente que muestra que si podemos ayudar a abordar el tema del phishing y del uso indebido del DNS vamos a reducir la cantidad de delitos que afectan a estas entidades benéficas y a estas empresas. Siguiente, por favor.

En el Reino Unido tenemos un servicio que se llama el servicio de denuncias de correos sospechosos. No es que seamos muy creativos con los acrónimos como en el caso de la ICANN pero aquí las personas físicas o las empresas pueden denunciar los correos sospechosos al gobierno con algunos detalles que tienen que dar. También con los mensajes de texto pueden hacerlo. Esta también es una fuente importante de denuncias relacionadas con el phishing.

Durante el 2022 recibimos 6.400.000 denuncias en nuestro servicio. Vemos que es un tema a gran escala. Muchas víctimas en el Reino Unido. Personas que denuncian este tipo de situaciones. En el 2020, que se lanzó este servicio, obviamente tuvimos parte de las respuestas por la pandemia, pero desde su lanzamiento ahora llegamos a 15.800.000 millones de denuncias. Es bueno poder ver en un gráfico esto a lo largo de los años.

En el gobierno lo que se ve a partir de todos estos informes, de estas denuncias es que se intenta simular que estos actores son entidades gubernamentales. Dentro de esos ataques de phishing tienen representaciones o tratan de fingir que son parte del Servicio Nacional de Salud o que son organismos con licencia de televisión o de ingresos de rentas y de aduanas. También de parte del gobierno, con consejos

sobre qué hacer en términos del COVID. También organismos que otorgan licencias a los vehículos y a los conductores. Hay muchos ataques a entidades gubernamentales y este servicio trata de recuperar información sobre esto.

Hablando de los individuos y de los usuarios de Internet, también son impactados y denuncian estos delitos. Hubo una revisión telefónica de un sinnúmero de víctimas que se nos reportó para entender el impacto desde la perspectiva financiera. Como pueden ver aquí, es una gráfica horrible. Pido disculpas. Es lo que me dieron.

Como pueden ver, hay un rango entre 20 y 250 libras, que es lo que pierde la gente. De pronto piensan que no es mucho dinero pero después tenemos 6.4 millones de personas que han denunciado un delito y si cada uno de ellos pierden aunque sea 20 libras, entonces 20 multiplicado por 6.4 millones es una gran cantidad de dinero. Es un buen año de trabajo. Eso se ve a gran escala. Especialmente con la crisis, con el costo de la vivienda que tenemos en un sinnúmero de países, realmente es impactante el que las personas pierdan esta cantidad de dinero. La siguiente imagen, por favor.

Hablamos también mucho con respecto al dinero con el ciberdelito pero no solo son afectadas las personas con el dinero. Los individuos sufren, es cierto. Las empresas también. A nivel individual puede ser otro tipo de impacto. Puede ser algo que emocionalmente les haga sentir mal. Tuvimos un caso de estudio con respecto a esto. Recibimos información de una víctima de 17 años de edad donde un hackers estaba pidiendo más información de contraseñas y logró tener acceso a muchas de sus cuentas de las redes sociales. Logramos hacer un

trabajo en el trasfondo de este caso. Logramos identificar al sospechoso. Nos dimos cuenta de que tenía un historial de hacer hacking de las cuentas de redes sociales a un sinnúmero de individuos. Logramos obtener una orden de captura para ir a visitar la dirección de esta persona y encontramos varios teléfonos activos que estaba utilizando para cometer esos delitos. En esos celulares logramos ver evidencia masiva de phishing. La siguiente diapositiva, por favor.

Este es un ejemplo de una de las comunicaciones de este tipo. Vemos aquí que se representa a sí mismo como una persona que encontró información sobre un individuo y dice: “Mira. Encontré imágenes de ti en una página web. Quizá quieras hacer algo”. La otra persona contesta: “¿Cuál es el enlace o el link?” y entonces este individuo pone un link, un enlace y la persona puede acudir ese enlace.

Al repasar ese celular encontramos cientos de mensajes que se mandaban generalmente a niñas o muchachas tratando de tener acceso a sus cuentas. Puede ser un dominio, una víctima, pero también un dominio y cientos de víctimas. Todo depende del tipo de malware, el tipo de ataque se utiliza. También nos fijamos en ese sitio web para ver cómo ese individuo estaba utilizando las cosas para extorsionar a las personas. Siguiente diapositiva.

Disculpen que hay mucha información allí y está en letra pequeña. Hay una razón para ello. En el lado derecho superior de la pantalla se ve un servicio de phishing que se pone en Internet que les da a usuarios registrados la posibilidad de comprar páginas de phishing para que puedan tenerlas en Internet. Hacen clic en uno de esos lugares. Puede ser Netflix, Facebook, Snapchat u otras aplicaciones. Hasta puede

seleccionar el idioma. Está en letra pequeña aquí pero sí existen inglés, francés, español, ruso. Puede uno seleccionar el idioma. Pagan por ese servicio.

En la parte de abajo a la izquierda, al hacer clic allí eso crea un dominio malicioso que manda un mensaje y le provee los detalles. En la foto de abajo hay un ejemplo del dashboard que ellos crean donde puede ver uno todas las credenciales que han logrado. Al tener las credenciales, entonces pueden hacer la extorsión, toman los datos de allí. Puede ser de un Drive de Google, incluso uno que no se comparta en las redes sociales. Esto tiene un gran impacto en las personas.

Logramos entonces desactivas este sitio web con el apoyo del registrador. Esta persona se enfrenta a procesos judiciales el próximo mes pero por el momento ha sido arrestado debido a la amenaza que existe para un sinnúmero de víctimas. Hemos tratado de comunicarnos con cada víctima que hemos logrado identificar para decirles que hemos removido esos datos y les sugerimos que actualicen sus contraseñas. Es importante cómo les impactó esto a estas personas. Recibimos comentarios como: “Gracias por eso. No sabía cómo solucionar eso”. Eso es clave, que nosotros sepamos cómo solucionar esto y remover estos daños que se están causando. La siguiente imagen. Creo que le doy la palabra a Gabe.

LAUREEN KAPIN: Me pregunto en qué momento estamos, a ver si nuestro colega Bertrand está preparado para mostrar su presentación o no. ¿Qué hacemos?

CHRIS LEWIS-EVANS: Disculpe. Tengo una diapositiva más. Este es un resumen de lo que tiene que ver con datos empresariales. El informe más reciente es de 2020 a 2021. En el Reino Unido se recibieron 875.000 informes de fraude y ciberdelito, combinados los dos. Eso supone una pérdida de 2.350 millones. El 80% de ese fraude fue facilitado por algo cibernético, ya sea por un correo electrónico phishing o de otra forma. Una gran cantidad de esa pérdida fue debido a algún tipo de actividad facilitada cibernéticamente. Esos correos electrónicos de phishing fueron un 80%. Realmente eso facilita a los delincuentes que puedan usar esos ataques cibernéticos. Esta es la última diapositiva. Gracias.

GABRIEL ANDREWS: ¿Podemos ver la siguiente diapositiva? Gracias. Desde la perspectiva de los Estados Unidos y, como dijo Chris, esperamos que existan otras personas que puedan animar a sus organismos de cumplimiento de la ley a que compartan esta información. El FBI la semana pasada publicó el informe de delitos del año 2022. Es información reciente y es bueno que podamos compartir esta información anualmente mientras esté la información fresca, por decirlo así.

Estos datos son un resumen de todas las querellas de las víctimas que llegan a nuestro Centro de Delitos de Internet. Es un portal central donde nosotros recibimos estas cifras. Después ellos preparan informes en base a esto. Esto no es un cuadro total de todos los delitos cibernéticos que existen pero sí nos da una idea. La siguiente diapositiva.

En los últimos cinco años, el IC3, que es el Centro de Denuncias de Delitos en Internet, recibe un promedio de 650.000 quejas al año. Pueden llegar a 2.000 querellas al día. Todavía no representa el delito que en realidad existe. Sabemos que no recibimos todas las querellas todo el tiempo.

Si nos damos cuenta, es bastante estable en los últimos tres años pero el volumen de las pérdidas ha aumentado y quisiera tener una buena explicación en cuanto al porqué. No tenemos muy buena explicación en este momento pero es interesante hacerlo notar. Muestra que los daños continúan aun si las querellas se mantienen estables. La siguiente imagen.

Como mencionó Chris dentro de su categoría de delitos, nosotros no rastreamos el uso indebido del DNS como categoría tampoco. Sin embargo, hay categorías del uso indebido del DNS que sí se rastrean dentro de nuestros informes de IC3. Aquí particularmente en la parte de abajo se dice phishing. Cuando vemos las primeras cinco categorías, vemos que el phishing es la principal.

En los últimos cinco años se puede ver que por una razón u otra el phishing ha aumentado tremendamente en los últimos cinco años según las querellas que hemos recibido. De nuevo, esto es algo que muestra todas las categorías de delitos, no solo los primeros cinco, y cómo el phishing está relacionado con eso.

Chris ya mencionó algo que quiero hacer resaltar. El phishing, aunque se rastrea dentro de su propia categoría, normalmente es el método inicial que los delincuentes utilizan para comprometer a las víctimas

hacia otro sinnúmero de delitos. Por ejemplo, se puede preguntar: ¿Es el ransomware un uso indebido del DNS? No. Ransomware es cuando un delincuente coge sus datos de su máquina y lo codifican y no permiten que uno los acceda a no ser que uno pague un dinero. Pero si se hace la pregunta: ¿El ransomware lo propaga el phishing? La respuesta es sí.

Hubo información reciente que se recibió de Royal Ransomware, una de nuestras agencias hermanas. En su informe se indicó que el 67% de las infecciones de ransomware surgieron del phishing. De nuevo, estamos rastreando las categorías iniciales pero tiene un impacto descendente.

Para enfatizar el punto, cuando nuestros amigos, colaboradores y colegas de la comunidad de ICANN que existen a nivel de registrador o registratario, cuando ellos toman acciones para solucionar estos dominios, cuando se utiliza phishing, ellos están usando no solo el reporte que nos llega comúnmente sino también otras categorías facilitadas por esto.

Además de compartir esas estadísticas del informe anual, yo le pregunté a sinnúmero de colegas qué es lo nuevo, qué es lo que está de moda o la tendencia en los últimos meses. Lo que nos dijeron es que lo están llamando malvertising, que es como una combinación de malware con publicidad. Una palabra que combina las dos cosas.

Ha tenido mucha atención de diciembre al año pasado y los primeros meses de este año. Como el phishing, el delincuente obtiene un nombre de dominio que es similar a otro y de pronto consigue un

nombre de dominio que se parece a un paquete de software, a alguna marca confiable y en vez de usar eso en el correo electrónico, ellos más bien van a los proveedores de búsqueda y compran publicidad. En este caso, como pueden ver en la diapositiva, esto viene de DHC, de su Twitter feed. El delincuente está haciéndose ver como si tiene una página web, un sitio web similar al verdadero.

No lo están compartiendo por ser buena gente. Si uno va al sitio de publicidad de ese delincuente en la parte de arriba uno recibiría ese mismo software junto con el malware. Es como un tipo de troyano. Si uno se inscribe o entra en ese software, entonces ellos pueden sacar su información o sacar su dinero si es una cuenta bancaria y cosas así.

¿Esta nueva tendencia acaso es phishing? Tal vez no porque no hay una conexión de un correo electrónico pero tiene el mismo resultado. Lo hago resaltar porque, número uno, es nuevo; segundo, es algo directo con el DNS y también, tercero, porque tenemos que reconocer que tenemos que ser un poco ágiles y flexibles al responder a lo que realmente está ocurriendo en el mundo. Realmente incorporar estas nuevas tendencias en nuestras ideas de cómo nosotros combatimos esto. Como dije antes, los registradores responsables que toman acción en cuanto a estos registros de dominio están tomando acción en cuanto a esto y esto es algo bueno. Ahora mi última diapositiva.

Quiero enfatizar el punto. El phishing es común en todos los miembros de la comunidad de ICANN y se denomina como uso indebido del DNS. Aprendí recientemente en el informe que es el número uno en ciberdelitos que se denuncian. La acción rápida en cuanto a estos dominios registrados maliciosos importa y políticas tras esto importa.

Ese es el mensaje que les quiero dejar. Gracias por su atención. Creo que ahora que Bertrand está aquí a mi lado podemos hacer el cambio y le doy la palabra.

MANAL ISMAIL: Adelante, Bertrand. Muchísimas gracias al equipo de jurisdicción e Internet. Gracias por todo el trabajo, por todo el trabajo que realizan vinculado con el uso indebido del DNS. Es un tema de mucho interés para el GAC.

BERTRAND DE LA CHAPPELLE: Gracias, Manal. Es un placer estar nuevamente aquí en el GAC. Solía estar aquí como representante de Francia hace muchos años, incluso en una vicepresidencia del GAC. Veo muchos rostros conocidos de aquella época. Realmente es un placer tener la oportunidad de hacer esta presentación aquí. Soy director ejecutivo de la red de política de Internet y jurisdicción. Es una organización que cofundé hace 10 años ya. Estoy muy complacido de poder venir a hablarles sobre este debate que ha generado tanto interés en la comunidad de la ICANN durante varios años.

Les quiero contar en qué estuvimos trabajando para seguir avanzando en nuestra tarea y encontrar soluciones. Aquí tenemos al director de programas. En realidad es una iniciativa de múltiples partes interesadas que convoca a los gobiernos, a las empresas, operadores técnicos, miembros del ámbito académico y la sociedad civil, y organizaciones internacionales para tratar las cuestiones

jurisdiccionales vinculadas a Internet. Pasemos a la siguiente diapositiva.

Tenemos tres programas. No voy a detenerme en los dos primeros pero uno de ellos corresponde al tema de los dominios y la jurisdicción cuando corresponde trabajar a nivel de DNS para abordar el tema de los usos indebidos. Hay un grupo de contacto que ha estado trabajando durante más de cinco años con unos 40 integrantes de distintas comunidades. Manal y otros integrantes aquí han estado participando activamente en esa actividad y estoy sumamente agradecido a Manal por la alta responsabilidad que ha asumido al dedicar el tiempo para participar. Es muy importante.

Si pasamos a la siguiente diapositiva lo que tenemos que resaltar es que aquí estamos hablando de cómo luchamos contra los usos indebidos que existen en línea. Este tipo de usos indebidos son sumamente diversos. La presentación que acabamos de escuchar muestra que el ingenio humano no tiene límites. Todos los medios que posibiliten un uso indebido van a ser utilizados para un uso indebido. Todos los sabemos.

El desafío clave, y este es el segundo punto, es un problema transnacional. Es interesante destacarlo aquí, en el ámbito del GAC, porque todos ustedes son representantes gubernamentales. Yo fui un representante gubernamental y todos sabemos que el motivo por el cual tenemos un problema al abordar el tema de los usos indebidos en línea es porque carecemos de las herramientas de cooperación entre los gobiernos para poder actuar a nivel transnacional. Tenemos una

arquitectura internacional que se basa en la separación de soberanías y la cooperación es sumamente difícil.

Uno de los programas que nosotros tenemos hace referencia al acceso transfronterizo de evidencia electrónica y es sumamente problemático este tema. Nos llevó años organizar el debido proceso entre los países para poder realizar investigaciones utilizando las pruebas electrónicas. Nos vemos frente a esta situación. No solamente la red es mundial. No solamente los agentes actores con estos fines maliciosos trabajan más allá de las fronteras sino que también tenemos que abordar esto de esta manera y no somos eficientes. Aquí necesitamos facilitar la cooperación entre gobiernos.

Para poder resolver estos problemas debemos comprender mejor cómo funciona la Internet en sí misma. Cuando hablamos del sistema del DNS, hay falta de conocimiento, de entendimiento en muchos círculos. Ustedes se darán cuenta cuando hablan con colegas de que a veces se desconoce cómo funciona esta arquitectura. Si queremos saber cómo contactarnos con un registrador vamos a encontrar la función de WHOIS para poder llegar al registrador y eso no es tan sencillo.

Algo también importante es que yo estaba hablando de la falta de herramientas pero también hay una cuestión que tiene que ver con las competencias. Los operadores de DNS básicamente están poniendo a disposición los nombres de dominio y no tienen competencia en analizar si algo se trata de phishing o de malware o si dependen de notificadores confiables. Cuando hablemos de los usos indebidos relacionados con el contenido, cómo manejamos todo el tema de la

legalidad del contenido con todo este patchwork que tenemos de jurisdicciones. Para tratarlo en cientos de miles, esto lleva tiempo.

En consecuencia, este es un problema para todos. Es un problema para los gobiernos porque ustedes se preocupan legítimamente porque no se puede resolver este tema. Es un problema para las empresas porque también son víctimas o tienen la responsabilidad también de abordar este tema y también es un problema para los usuarios. Siguiente, por favor.

Algo que también es bastante básico, todos ustedes lo conocen, pero lo quiero compartir. Lo suelo compartir con personas fuera de nuestro propio entorno porque no necesariamente saben cómo funciona el sistema. La relación entre el registratario, el registrador, el registro y los usuarios. Las consultas que van de una entidad a la otra y las reglas que los distintos actores utilizan para que la Internet funcione de la manera en que esperamos que funcione. Esta es una arquitectura que puedo explicar pero hay cuatro acciones que pueden tomar los operadores de DNS con respecto a los nombres de dominio. Veamos la siguiente diapositiva.

La primera es bloquear el dominio. Básicamente no se puede modificar la información proporcionada por el registratario. No se pueden hacer transferencias, eliminaciones o modificaciones y tampoco se puede cambiar el servidor o la dirección de IP que se menciona. Es importante destacar que esta acción no hace que el contenido sea inaccesible. Se puede bloquear. Es bueno para la investigación posterior pero no cambia nada con respecto al funcionamiento.

El segundo elemento es el de suspenderlo y en ese sentido ponerlo en pausa. Se retira del archivo de la zona raíz de TLD pública y entonces no hay resolución. Tampoco se puede modificar la información en el servidor pero el sistema sigue funcionando. Si se utiliza la dirección de IP, se puede tener acceso a este elemento que está puesto en pausa.

Luego tenemos el redireccionamiento. Esto es para poder hacer un sinkholing de los dominios en una investigación donde se edita el archivo de la zona para hacer un redireccionamiento a otro servidor para poder identificar las víctimas y analizar el comportamiento.

El tercer y el cuarto elemento tienen que ver con la transferencia cuando se pone esto a otro registrador. Por ejemplo, la registración se hizo de manera incorrecta en un registrador en particular, entonces se hace esta transferencia. Por algún motivo hay interés en llevarlo a un registrador de último recurso. Es algo en lo que Benedict Addis trabaja muy activamente. También podemos tener la eliminación pero esta no es una acción recomendada por muchos motivos.

¿Actuar a nivel del DNS con estas cuatro acciones es el instrumento correcto para abordar el tema del uso indebido del DNS? La respuesta es sí en algunos casos y no en otros casos. No es la panacea perfecta. Algunas personas fuera de nuestras comunidades tienden a considerar esto como un gran panel de control. Si hay un problema con un nombre de dominio simplemente se toca un botón y el problema desparece. No es así la situación pero es bueno tener acciones disponibles en algunos casos.

Los interrogantes clave que tenemos que resolver son los siguientes. Este es un instrumento que sirve no solamente para el servicio de acceder al sitio de un nombre de dominio sino también a muchos otros servicios auxiliares como el correo electrónico, la transferencia de archivos. Aquí es un instrumento romo. Además, tiene un impacto global. A todo el mundo afecta. No podemos tener un bloqueo geográfico para la suspensión de un nombre de dominio. Lo podemos considerar como una función o como un defecto, como un bug. Si es un defecto, no tiene un impacto global, pero qué pasa cuando no tenemos cooperación internacional. A veces tener este efecto global puede ser beneficioso.

Luego podemos acceder a la mayoría de los servicios a través de la dirección de IP. Los operadores de DNS son parte del ecosistema y tenemos que tener en cuenta la arquitectura en su conjunto. Los proveedores de hosting, los proveedores de servicios de Internet y otros que también pueden llevar adelante acciones y actuar al nivel correcto es algo muy importante.

En los acuerdos de acreditación de los registradores y registros sigue habiendo algunas obligaciones con respecto a tener puntos de identificación de uso indebido e investigar pero son limitadas las obligaciones que aclaran qué es lo que se requiere hacer. Esto nos lleva a una situación en la que hemos sido testigos durante mucho tiempo de que ha habido un debate muy prolongado dentro de la ICANN durante muchos años sobre el término uso indebido del DNS y cuál es su significado. Ha habido distintas posiciones respecto de esto.

Tuvimos muchas sesiones para definir este tema del uso indebido del DNS. También hubo críticas mutuas entre las unidades constitutivas e incluso tensiones dentro de estas unidades con respecto a cuánta acción debería llevarse adelante o no. No alcanza con decir que son agentes con fines maliciosos o delincuentes. Eso lo entendemos pero no hay una manera clara de llegar hacia un consenso aquí.

Si hacemos la pregunta incorrecta, posiblemente no vamos a tener la respuesta correcta. Hay que reformular el problema y reformular el problema significa ver cuándo es apropiado actuar a nivel del DNS para prevenir usos indebidos en línea. Creo que esta es una formulación con la que todos podemos estar de acuerdo como una formulación válida que tiene en cuenta los distintos elementos. La siguiente diapositiva.

Como parte de esta reformulación hemos estado trabajando con el grupo de contacto que mencioné antes durante mucho tiempo. Hemos tratado de acotar las posibilidades para entender el uso indebido del DNS que en algún momento denominamos uso indebido técnico pero, con la ayuda de algunos de los actores, hemos acotado esto. Decimos que el uso indebido del DNS debería ser considerado como estas cinco situaciones: circulación de malware, botnets, phishing, pharming y spam en la medida en que se utiliza como un mecanismo de entrega para los otros anteriores.

Podemos encontrar más detalles sobre la definición de estas cinco situaciones en los abordajes operativos que nuestra red produjo en el 2019, que llevó a la incorporación de estas definiciones sobre uso indebido del DNS en el marco para abordar el uso indebido producido

por varios actores, agentes dentro de la comunidad, en diciembre de 2019 y luego, más adelante, el informe del SSAC, el SAC115 de 2021, que incorporó esta definición del uso indebido del DNS.

Tal vez no sea una definición perfecta pero es un elemento muy importante para distinguir entre esto que sí podemos denominar uso indebido del DNS, donde todos los actores entienden que hay un motivo para esa investigación, y esto entra en el ámbito de competencia de los operadores, el uso indebido relacionado con el contenido del que hablaré luego. Se puede hacer esa diferenciación.

Hemos producido, y no voy a entrar en todos los pormenores, un conjunto de herramientas en el 2021, este toolkit, como lo llamamos, para ayudar a los operadores de DNS, a los notificadores y a los legisladores o los organismos de aplicación de la ley para que entiendan los distintos parámetros y tengan ciertas pautas, ciertos elementos para la convergencia y para trabajar en conjunto.

En la siguiente diapositiva se menciona un elemento importante que es que hay un flujo de trabajo con cuatro elementos que hay que considerar al tratar cualquier tipo de uso indebido. En primer lugar la identificación del uso indebido en sí mismo. Puede ser a partir de los notificadores o a partir de los propios operadores. El segundo elemento es la evaluación de este uso indebido. ¿Justifica una acción a nivel del DNS? ¿Cuál es la acción que debe implementarse de esas cuatro que mencioné? Hay una quinta que todavía no hemos discutido. Cuáles son los caminos para tener algún tipo de recurso cuando hay que cambiar una decisión. Puede haber errores.

Para cada una de esas etapas hemos producido un sinnúmero de cosas como el definir más claramente los tipos de abuso. Mencionar los elementos con respecto a qué deben hacer los notificadores con respecto a diligencia debida para documentar esos incidentes. No es simplemente dar una notificación sin ninguna evidencia sostenible. ¿Cuáles son las condiciones para notificarles a los registratarios cuando hay este tipo de delito?

La pregunta clave también es cuáles son los umbrales, los criterios para este tipo de acción. Qué se necesita para cumplir con eso. En cuanto a las acciones, hay diferentes tipos de acciones y hay un documento que precisamente explica las imágenes que les mostré anteriormente.

Finalmente, en cuanto al recurso, existe el tema de los canales para recursos y evidencia de transparencia. Esto es un proceso. Todo lo que está enlazado con las investigaciones para mitigar el uso indebido pasa por diferentes etapas y es la colaboración de diferentes actores. Si paso a la siguiente imagen, el grupo de contexto ha producido una serie de documentos que yo espero que sea útil para ustedes como comunidad pero también para poder debatirlo.

Primero, ¿las notificaciones deben componerse de qué? ¿Qué se necesita para la evidencia? El segundo es cuáles son los tipos de notificadores. ¿Es lo mismo ser un notificador de imágenes de abuso sexual infantil o si tiene que ver con algún incumplimiento de alguna marca de alguna empresa y cuál es la debida diligencia que deben tener los notificadores para asegurarse de que la responsabilidad de validar esto no cae totalmente en los operadores? ¿Cuáles son los tipos

de arreglos que se puedan hacer entre notificadores confiables? ¿Cuál es el arreglo?

Quiero aclarar algo. Nadie puede decir por su propia cuenta que es un notificador confiable. Lo que puede decir es que tiene pericia en ese tipo de campo, que lo hace como un notificador experto, pero una relación con un notificador confiable es una comunicación bilateral. Uno puede ser un notificador confiable para un operador pero no para otros. Es una distinción importante. Tenemos que trabajar esto con los notificadores.

Un documento dedicado habla de la cuestión de botnets. No tengo tiempo para entrar en detalle pero es un tema importante que se llama dominios generados por algoritmos. Buscar una mejor cooperación entre los organismos de cumplimiento de la ley, ICANN y los operadores de DNS es algo muy importante. Podemos hablar de esto en el futuro.

Finalmente tenemos phishing y malware. Hablamos con los grupos de contacto para que exista un organigrama claro de los diferentes roles a través de las diferentes etapas entre los registradores y los registratarios y cuál es el canal de información.

Estoy contento de poder mencionarles, ya que está aquí en la esquina Graeme Bunton, y algunos de ustedes lo han visto antes, que esto ha llevado a dos buenas iniciativas. Estoy muy contento por esto y fueron creados por la base que tenemos del trabajo de I&JPN, y gracias también a la ayuda del PIR. Es una información que hablamos dentro

del grupo de contacto, que habla acerca de reportar este uso indebido en una plataforma que se llama NetBeacon.

Brian Cimbolic y su colega fueron responsables por esto. Él es el coordinador del grupo de contacto que nosotros tenemos en ING y este trabajo es increíble para mí porque es el resultado de cinco años de trabajo que llevó a elementos concretos, algo operativo, no simplemente discusión o escrito en papel sino que realmente es operativo. Me quito el sombrero por ellos de haber hecho el trabajo. Esto es importante porque esto ha llevado a discusiones que han tenido lugar aquí, en ICANN76, con respecto a los acuerdos de acreditación. Cierro esta sección pero tengo otra corta después. Se trata del uso indebido del DNS y se entiende como los cinco elementos de los cuales hablamos. La siguiente imagen, por favor.

Creo que en resumen hay un acuerdo entre los actores responsables en que el uso indebido del DNS entendido de esta manera es algo que es realmente justificado actuar a nivel del DNS cuando hay suficiente evidencia, a no ser que se haya visto comprometido el sitio. Pensamos que estamos en una dirección adecuada para tener una cooperación implementable.

También existe la cuestión del uso indebido relacionado con el contenido. Esto es un poco complejo porque esto es más un espejismo. A nivel de DNS, no es el lugar debido de hablar acerca del uso indebido relacionado con el contenido. Debido a que no es suficiente granular es difícil de acomodarlo a los asuntos legales o ilegales de un lugar a otro, y también la competencia en cuanto a evaluar si hubo un uso indebido

o no es diferente. No es algo que técnicamente conozcan los operadores.

Hablando en general, no es una herramienta eficaz porque el contenido sigue disponible en muchos casos. Sin embargo, hay unas situaciones en que sí es una excepción donde hacerlo al nivel de DNS cuando se ha cumplido con los requisitos. En lo que implementamos en el 2019 antes del congreso global en Berlín, hay cuatro elementos que tentativamente se pueden tomar en cuenta para poder evaluar o adivinar cuándo sí es apropiado actuar a nivel de DNS para el uso indebido relacionado con el contenido. Qué acuerdo global se ha hecho para entender si el contenido en cuestión es ilegal o no. Hay extremos y hay diversidad con respecto a legislativas a través de todo el mundo en cuanto a lo que es legal o no. También la proporción del sitio que está dedicado al contenido infractor.

También cuál fue el propósito, si fue de buena fe o de mala fe de parte del registratario o el operador de sitio. También saber si se ha gastado otros niveles con respecto al operador o el registratario.

Es importante hacer la distinción entre esas dos categorías. Ambas cosas son importantes pero no se deben tratar de igual manera. Uno de los grandes retos es que nosotros no tenemos un espacio para poder hablar del segundo problema. ICANN es el lugar adecuado para hablar con respecto al uso indebido del DNS como lo hemos descrito anteriormente. Ha sido muy claro que, según los mandatos, y la comunidad está completamente alineada con esto, ICANN no es el lugar para hablar acerca del uso indebido relacionado con el

contenido. Han existido posts de que ICANN no es la policía del contenido y eso se entiende.

El problema es que no hay ningún otro lugar donde se pueda hablar de esto. Esta es la razón por la que en el pasado, en mayo de 2022, una porción significativa de quienes participaron en el grupo de contacto de ING nos han pedido que básicamente nosotros seamos el lugar donde sí tenemos conversaciones con respecto al uso indebido relacionado con el contenido para que se pueda explorar ese tema para esas situaciones excepcionales de buscar los umbrales, los criterios y los mecanismos. Eso es lo que hemos hecho este año. Es algo preliminar. Apenas comienza pero yo creo que es importante para esta comunidad del GAC, para que ellos vean todo el conjunto, y que entiendan que ICANN está progresando en base al trabajo que hemos hecho conjuntamente con respecto al uso indebido del DNS. No es perfecto. Hay que implementarlo y fortalecerlo pero realmente estamos progresando en ese sentido. Más claridad, mecanismos y cooperación.

Con respecto al uso indebido relacionado con el contenido, aunque no se trata del tema en ICANN, nosotros como I&JPN estamos trabajando en esta actividad en base a los siguientes elementos que se ven en esta diapositiva. Número uno. Las etapas con respecto al uso indebido relacionado con el contenido se motivan porque hay razón para ir a ese lugar directamente o porque es el último recurso después de haber pasado por diferentes niveles en el stack. La pregunta es cómo se comunica uno con el operador de sitio, el registratario, el proveedor de hosting. Esa es la primera conversación.

El segundo elemento es cómo formular el criterio del umbral de este tema. Para dar un ejemplo, uno puede decir: “Todo el sitio debe dedicarse a la actividad infringida”, o se puede decir que no hay otro contenido legítimo en el sitio aparte de esto. Uno puede decir que el intento del operador del sitio es hacer X, Y y Z. Estamos facilitando estas conversaciones en cuanto a este tema.

Finalmente, la noción de ser alcanzable. Cuando hablamos de que hay un camino incremental, cómo mandamos una notificación y cómo nos comunicamos con el registratario, el operador del sitio o el proveedor anfitrión con respecto a esto. Vamos a explorar esto en más detalle porque no hay un equivalente claro del WHOIS en cuanto a los proveedores anfitriones y dónde se va a alojar un sitio particular es un poco más complicado al compararlo con buscar un registrador.

Finalmente, hablé acerca de los acuerdos de notificadores confiables. Es un punto muy importante, especialmente para el uso indebido relacionado con el contenido. Aun más para phishing pero para el uso indebido relacionado con el contenido no habrá una solución para esto sin la cooperación de las tres categorías de actores, los organismos de cumplimiento de la ley, los notificadores de los diferentes recursos que tienen que amplificar o escalar sus esfuerzo, y también los operadores de DNS en los acuerdos corrientes.

Si se acuerdan de la afirmación del compromiso entre NTIA y ICANN en años anteriores, yo creo que hay un concepto del marco de trabajo que tiene que ver con una afirmación mutua de compromisos. Necesitamos mecanismos que puedan reunir a los notificadores y los organismos de

cumplimiento de la ley y los operadores para que todos puedan tratar los casos cuando sea apropiado hacerlo al nivel del DNS.

Quiero resaltar que de lo que estamos hablando no es de regular estas plataformas grandes. No son los Facebooks o los Twitters de ese mundo. Ustedes no van a pedir desactivar facebook.com porque exista algún contenido en alguno de los subgrupos que existen allí. Cuando alguien simplemente monta un sitio web tras un nombre de dominio para tener una intención maliciosa, el buscar a estas personas y básicamente pararlos pero no pararlos en solo un pequeño sitio y después en otro sitio sino más bien buscar a las personas tras eso. Eso es lo que se necesita hacer. Ese es el tipo de cooperación que necesitamos.

Mi punto es que esta es una responsabilidad compartida, que necesita la cooperación de los diferentes actores. Este modelo interseccional es para facilitar esto entre las múltiples partes interesadas. Nosotros estamos contentos de que esto ha llevado a un progreso dentro del ambiente de ICANN. Es la única forma de poder solucionar estas cuestiones.

Desapareció mi imagen. Hay una diapositiva que muestra todas las conexiones y los enlaces que los llevan a los documentos que les presenté. Aquí, en esta última diapositiva, está mi información de contacto y de Ajith Francis, por si quieren hablar con nosotros después de esta sesión. Muchas gracias por la oportunidad de dar mi presentación.

MANAL ISMAIL: Gracias por su presentación. Quiero darle también el reconocimiento a la persona que pacientemente tiene su mano alzada, de Irán. Después le daré la palabra. Primero le damos la palabra a Chris.

CHRIS LEWIS-EVANS: Sí. Hemos tenido muchas aportaciones, mucha información. Hemos hablado bastante. Si tienen alguna pregunta o algún comentario con respecto a las últimas ponencias, los aceptamos en este momento. Vamos a cubrir actividades de continuo en el mundo de ICANN y también lo que va a estar en el comunicado. Solo de las últimas dos presentaciones podemos aceptar alguna pregunta o comentario.

MANAL ISMAIL: Gracias. Kavouss, ¿algo que usted quiera decir en cuanto a la última parte de la sesión? Por favor, adelante.

KAVOUSS ARASTEH: Muchas gracias, Manal. Permítanme expresar mi sincero agradecimiento a todas las personas que están aquí, en la mesa principal. En mi opinión, esta fue una de las conversaciones más interesantes que hemos tenido sobre el uso indebido del DNS. Si bien no quiero hacer una comparación, la última parte para mí fue sumamente interesante.

Como mencioné ayer, tenemos problemas. Hemos resuelto algunos problemas pero lo que recomiendo, distinguida presidenta, a usted y al futuro presidente del GAC, a Nico, es que el orden del día del GAC de

la próxima reunión destine más tiempo para tratar este tema. No es posible en forma superficial ver este tema y no profundizar en el corazón del problema. No tenemos tiempo. Tengo algunas sugerencias. No sé qué me sugiere usted a mí pero creo que podemos avanzar de esa manera.

Quiero hacer referencia a un punto. El colega distinguido a la derecha del podio habló de la cooperación intergubernamental. Esto se discutió muchos años. No es una cuestión que le competa a la ICANN porque la ICANN no es una organización intergubernamental y el GAC no es una organización intergubernamental sino que es un comité asesor gubernamental. Los gobiernos son intergubernamentales en otras partes. Perdón. Soy muy sincero con todos.

Muchas veces queremos abordar este tema. Hablamos de la cooperación intergubernamental y siempre hay algún gobierno que se opone a ello. Cuando hablamos del ciberdelito, se considera que es una cuestión nacional y que no debe tratarse a nivel internacional. Dicen que toda cooperación intergubernamental podría resultar útil si condujera a un tratado y no es posible tener un tratado sobre esta materia.

Profundicemos en la situación. No en esta sesión porque ya estamos llegando al final pero, distinguida presidenta del GAC, si pudiéramos dedicarle más tiempo a discutir este tema, se han expresado puntos muy interesantes pero más que nada se han formulado aquí los problemas. Todavía no tenemos soluciones propuestas. Eso es importante.

A veces es fácil, no diría muy fácil. Es más fácil plantear el problema pero no es fácil sugerir las soluciones. Es más difícil. ¿Dónde están las soluciones? Es necesario tener un enfoque pragmático. No recurrir a la legislación y ver qué podemos hacer sino categorizar prioridades, qué podemos hacer. La cooperación intergubernamental en este momento no es tan fácil pero hay muchos otros aspectos que podemos tratar. Hemos recibido los informes del Reino Unido y de Estados Unidos pero habría que preguntarles a todos los miembros del GAC si tienen la misma experiencia. ¿Dónde están sus informes? Yo personalmente me enfrenté a este problema pero no hubo denuncias.

Ayer también hablamos de una llamada diplomática con un 10% del precio. Mi hijo me dijo: “No abras ninguna de estas comunicaciones”. Si tienen una dirección de correo y no conocen al remitente, no abran ese correo porque inmediatamente puede terminar en problemas.

Luego hay otros abordajes. Algunos de los proveedores de correos tienen doble seguridad. Es decir, si la contraseña es secuestrada por alguien, además de la computadora, nadie puede utilizarlo con otro dispositivo porque tiene el segundo factor de seguridad. Tenemos que darles consejos a las personas. Algunas precauciones que pueden considerar. Todo lo que se puede hacer de su parte para reducir este problema. Hay muchas otras cuestiones para tratar. Les pido disculpas por ser tan franco pero bueno, eso es lo que quería decir.

MANAL ISMAIL: Gracias, Irán. Si me permite, Chris, tenemos otros dos pedidos de intervención y tal vez pueda responder a todos. Tenemos solamente 20

minutos y tengo a la República Democrática del Congo y Estados Unidos. Adelante.

BLAISE AZITEMINA FUNDJI: Muchas gracias, Manal. Gracias a todos los panelistas. Al igual que Kavouss, quisiera mencionar cuán importante ha sido esta presentación porque desde la perspectiva del gobierno para la mayoría de los gobiernos, sobre todo de África, la expectativa con respecto a los representantes delegados en el GAC tiene que ver con que puedan resolver este tema del uso indebido. Por supuesto, aquí hablamos de uso indebido pero quisiera preguntar si hay alguna acción que se pueda tomar en los gobiernos para prevenir porque por supuesto hablamos de remediar, de sanar, pero en francés utilizamos una frase para esto, y ver si hay alguna acción que podamos llevar adelante.

Por supuesto, hablamos de ciberseguridad donde hay problemas que ponen en riesgo la soberanía de las naciones pero en cuanto a consejo para los gobiernos y las empresas, ¿cuál es el consejo? ¿Cómo podemos prevenir esto? Vimos una presentación del FBI y también del Reino Unido con sus experiencias. Entiendo que hay algunos estudios, hay ciertas estadísticas que tal vez puedan ayudar a entender por qué tenemos este tipo de uso indebido.

Sabemos que para los usuarios finales en general el problema está en el phishing, en las contraseñas que están comprometidas, los correos fraudulentos pero los gobiernos y las empresas, ¿qué pueden hacer

para prevenir en lugar de llegar a la etapa de tener que subsanar los problemas?

MANAL ISMAIL: Gracias, Congo. Estados Unidos y Francia. Sean breves, por favor. Luego le voy a dar la palabra a Chris. Adelante.

SUSAN CHALMERS: Gracias, Manal. No tengo problema en esperar la respuesta a la pregunta del colega.

MANAL ISMAIL: Gracias, Estados Unidos. Francia.

JONAS ROULE: Voy a hablar en francés. Primero quiero agradecer a los colegas por su presentación. Es un honor ocupar el lugar que ocupaba mi colega hace un tiempo. Esta intervención es sobre todo para alimentar un poco las discusiones. Soy nuevo en el GAC y tengo la impresión de que antes de ponerme a trabajar debería aprender sobre algunas cuestiones que tendrían que ser planteadas.

En primer lugar, como recién llegado aquí, querría explorar pistas para limitar ciertos abusos desde el punto de vista externo. Tengo la impresión de que la política bastante agresiva y el precio ventajoso que proponen algunos actores conducen a ciertos usos maliciosos de los nombres de dominio. Habría que ver entonces cómo se podría

trabajar por ejemplo viendo cuál es la tasa de renovación. Esto podría ayudar a la comunidad a trabajar al respecto. Sabemos cuáles son los actores que no juegan verdaderamente limpio y creo que hay que ser capaces de decirlo y encontrar medios para descubrirlos y para llegar hasta el fondo del problema. Algunas de las dificultades que se observan tienen que ser evidenciadas. Me parece que es algo interesante que tendríamos que hacer. Muchísimas gracias por su atención.

MANAL ISMAIL: Muchas gracias, Francia. Veo que Ruanda también ha levantado la mano. Por favor, podrían ser breves.

VINCENT MUSEMINALI: Muchas gracias. Simplemente quería agradecer a los panelistas o los presentadores por los informes de Estados Unidos y del Reino Unido sobre ciberdelito. Creo que necesito algo de aclaración. Estamos aquí frente a algunos desafíos presentados por el ciberdelito con las criptomonedas en particular. Hay dominios que se cierran y las personas que han hecho su inversión allí pierden su dinero. ¿Cómo se puede hacer un seguimiento de esa inversión? ¿Cómo se puede cooperar en ese sentido?

MANAL ISMAIL: Muchas gracias, Ruanda. Chris, le doy la palabra. Perdón que lo presione con el tiempo pero queríamos escuchar a los colegas del GAC. Adelante.

CHRIS LEWIS-EVANS: Muchas gracias por todos estos aportes. Voy a trata de resumir las respuestas. Con respecto a los consejos que nos pidió nuestro colega de Francia, no los vamos a tratar aquí. Hay muchos consejos, muchas cosas que pueden hacer. Tal vez puedan utilizar el taller de desarrollo de capacidades en el futuro para hablar de eso. Tal vez esto sería algo que podría considerar el GAC. Necesitaríamos una sesión mucho más extensa para darles toda esa información. Por ahí pueden considerar esa opción.

Con respecto a lo que podemos hacer proactivamente, NetBeacon, como se mencionó aquí, es una herramienta de denuncias. Es un mecanismo de acción para combatir este flagelo. Sabemos que hay muchas actividades en curso y quisiera resaltar algunas iniciativas dentro de la comunidad que ayudan a trabajar contra el uso indebido del DNS. En estas diapositivas están.

Con respecto a las criptomonedas, creo que esto tiene que ver con lo que dijo Bertrand. Pasamos de phishing en un correo electrónico al uso indebido del DNS o estamos hablando aquí de una cuestión vinculada al contenido. ¿Cuáles son los mecanismos que hay allí?

Si hablamos de las actividades de la comunidad, hay mucho trabajo que se está desarrollando. Los registros que están trabajando para compartir voluntariamente sus estadísticas, los registros también apoyan esto. Tenemos acidtool.com. Es una herramienta que permite identificar a los proveedores de hosting y de correo electrónico, registradores y registratarios. Es una herramienta que ayuda a

identificar el punto correcto al que deben dirigirse para poder llevar adelante acciones efectivas. Es importante identificar ese punto, ver si es un revendedor, un registro, un registrador. Creo que eso es sumamente importante.

Nuevamente, hacemos referencia a NetBeacon como un método para la acción. Esto está muy en línea con las recomendaciones del SAC115. Tuvimos una presentación interesante al respecto y estas son todas actividades que están ayudando a mitigar lo que está ocurriendo en el momento. El Instituto del Uso Indebido del DNS ha compartido el trabajo que ha hecho en materia de análisis, recolectando información sobre las denuncias de uso indebido del DNS. Tal vez esté hablando demasiado rápido para los intérpretes así que les pido disculpas. Ahora voy a desacelerarme.

El equipo reducido de GNSO también en cuanto al uso indebido del DNS ha sido muy activo y sus hallazgos o determinaciones son de igual importancia a las cuestiones de importancia del comunicado del GAC en cuanto a si el trabajo de PDP con respecto al uso indebido del DNS se debe personalizar o hacerlo de una manera para que tengan resultados trabajables. Como se mencionó anteriormente, sé que hay frustración en cuanto a las cosas no ocurriendo con suficiente rapidez.

También dentro de ICANN tenemos el equipo de OCTO, que tiene el sistema DAAR. Tiene que ver con analizar datos relacionados con 1.145 gTLD. Me sorprendió la cantidad. También hubo 21 ccTLD. De nuevo, es un mejor cuadro para un mejor entendimiento de lo que está ocurriendo, para poder tomar una acción más eficaz. La siguiente imagen.

Este es un recordatorio de ese camino y con quién comunicarse. Es un espacio un poco complejo. Este es un diagrama de ICANN. Qué bueno que lo están mostrando aquí porque yo para nada puedo dibujar eso. Escuchamos acerca de ir a la persona adecuada para tomar el paso adecuado en el momento adecuado y, desde mi perspectiva, logramos ver que si hacemos esto, esto reduce el daño. Si entendemos adónde ir y adónde ir rápidamente, es muy importante, especialmente utilizando herramientas como NetBeacon, ACID Tool, eso ayuda mucho. El cuadro es un poco complicado. Al lado derecho tenemos el registrador y el revendedor. A veces hay un revendedor. A veces hay más de uno. Por eso el entender eso es importante también para buscar el lugar adecuado donde acudir. La siguiente diapositiva, por favor.

Para marcar lo que hablamos del revendedor durante esa fase 1 con respecto al EPDP se recomendó que el registrador debe regenerar un elemento del registro que esté directamente correlacionado con el registratario. Existe en este momento un campo del revendedor pero no en todos los lugares, por eso es importante que nosotros podamos acudir a la persona a quien pueda dar una respuesta más eficaz y más rápidamente. Eso también se reflejó en la revisión del CCT. Ahora le doy la palabra a Laureen. Disculpe por hablar rápido. Quería llegar al segundo grupo de preguntas.

MANAL ISMAIL: Ya tenemos una pregunta del piso. Vamos a aceptar la pregunta primero, si está bien con Laureen. Nigel.

NIGEL HICKSON: Laureen puede ir primero y yo puedo hacer mi pregunta después.

LAUREEN KAPIN: Sí. Gracias, Nigel. Mi nombre es Laureen Kapin. Estoy hablando como una de las copresidentas del grupo de trabajo de seguridad pública y una de las peritas en este tema muy importante. La siguiente diapositiva. Aunque estoy feliz de que esta sesión ha sido interactiva aun antes de este momento… Hay muchas conversaciones, perspectivas e información con respecto a… Voy a reformular esto. Hay mucha información y perspectivas compartidas. Ahora hemos llegado al punto donde podemos hablar con respecto a qué quiere hacer resaltar el GAC en el comunicado con respecto a cuestiones potenciales.

Vale la pena decir varias veces que es una categoría con respecto a negociaciones de contrato entre los registros, los registradores y ICANN. De nuevo, la meta de este proceso es mejorar las obligaciones de contrato con respecto a tomar acción en contra del uso indebido del DNS. Obligaciones, no esfuerzos voluntarios. Estas obligaciones son con el fin de reflejar una obligación que va a cubrir a todos. Esperamos que eso incluya también a los actores maliciosos y así darle a ICANN aun más herramientas de las que ya tiene para poder lidiar con esas situaciones con respecto al uso indebido del DNS.

De nuevo, esto es solo el paso número uno y pueden existir más pasos en el futuro pero este puede ser un momento oportuno para que el GAC reconozca y aplauda que estos esfuerzos han sido continuos y se hicieron debido a la iniciativa de las partes contratadas. Este es un

paso proactivo que siempre aceptamos. Este es el primero de varios pasos. Tenemos pronosticado trabajo continuo en cuanto a la política y quiero reforzar lo que dijo mi colega de ICANN, que es importante darle prioridad a esto, y así nosotros poder aplicar estos dos principios guiadores en el PDP.

Sé que no siempre ha sido conocida como una acción rápida y enfocada pero lo puede ser dentro de este contexto. También pueden existir oportunidades para más negociaciones entre las partes contratadas y ICANN. Existirá una oportunidad para comentarios públicos una vez que las partes contratadas presenten los resultados de sus esfuerzos, que estamos ansiosamente esperando y después existirán oportunidades para que el GAC decida qué tipo de aportación va a querer difundir. La siguiente diapositiva.

Este tema con respecto a los revendedores también se ha identificado y la razón por la que eso está conectado con el uso indebido del DNS es porque es muy importante. Como ya lo mencionó nuestro colega de la Sociedad de Jurisdicción y de Internet, Bertrand, es importante acudir a la entidad adecuada cuando tratamos del uso indebido del DNS. Ese tema ha sido también una aportación del GAC en diferentes formas relacionado con el informe final del CCT y más recientemente la fase número uno de las recomendaciones de datos de registración del nombre de dominio.

Ahora les doy la palabra a mis colegas del GAC para que den sus aportaciones con respecto a sus ideas sobre qué se puede incluir en el comunicado del GAC. Sé que, como el tiempo es corto, tenemos

sesiones para redactar el comunicado del GAC pero sería el momento adecuado para saber qué están pensando ustedes.

MANAL ISMAIL: Muchas gracias, Laureen. Tenemos al Reino Unido, Irán y la Comisión Europea. Tenemos tres minutos. Espero que por favor puedan ser breves. Reino Unido, adelante.

NIGEL HICKSON: Muchas gracias, Manal. Muchas gracias a ustedes que están en la mesa por presentar una sesión bastante útil como han hecho notar los miembros del GAC. Brevemente, mis puntos son los siguientes. Número uno, quiero reiterar nuestra postura en cuanto a las negociaciones de contrato. Fue algo increíblemente positivo. Tuvimos la sesión ayer con los registradores y los registratarios. Eso fue excelente. Esperamos la consulta pública. No queremos interferir en esas negociaciones para nada. Esperamos la información actualizada y, como se mencionó ayer por parte de los representantes, este es el primer paso. Lo más probable es que puedan existir otras iniciativas con el EPDP al fijarnos en otros aspectos del uso indebido del DNS.

Con respecto al comunicado, yo creo que debemos ser muy claros en el comunicado con respecto a cómo aceptamos estas iniciativas pero también cómo puntualizar estos diferentes tipos de ideas que se deben marcar con respecto a este uso indebido. Hay ciertos pasos a tomar antes de que nosotros sigamos con el proceso SubPro. Gracias.

MANAL ISMAIL: Gracias, Reino Unido. El siguiente es Irán. Después lo cerramos con Japón. Irán, adelante.

KAVOUSS ARASTEH: Gracias, Manal. He hablado con colegas distinguidos, incluida usted. El tema del uso indebido del DNS es un tema a largo plazo de ICANN. Es algo importante. Sin embargo, todos, la junta, la organización de ICANN, los miembros, todos están estudiando el tema. No se necesita asesoramiento del GAC en cuanto a esto. Dejen que las personas reflexionen, lo piensen, digieran el asunto y no hacer más de lo que tengamos que hacer. Ellos ya saben el problema.

Por otro lado, la cuestión importante para el GAC es mencionar primero que hay que reconocer las negociaciones que se están llevando a cabo en la junta de ICANN y las partes contratadas y los registradores. Después debemos mencionar que necesitamos un informe de progreso con respecto a eso para nuestra siguiente reunión de ICANN, el ICANN77 en Washington DC.

Esperamos que el informe final sea en ICANN78 o 79, pero con suficientes medidas para poder aconsejarles al GAC cómo combatir, como mencionó mi colega, cómo contrarrestar esta situación y ver otros elementos indicados en el informe según mencionaron Chris, Laureen y Gabriel, presentando cuestiones importantes para el GAC. Tratar de enfatizar lo importante de estos temas, trabajar en el texto para que sea algo más conciso, preciso y más claro, y tomar pasos de seguimiento en cuanto a esto. Yo no creo que debamos incluir nada

con respecto al uso indebido del DNS en el asesoramiento del GAC en esta etapa.

MANAL ISMAIL: Tengo a la Comisión Europea y después Japón. Por favor, les recuerdo que sean breves. Comisión Europea, adelante.

GEMMA CAROLILLO: Gracias. Brevemente quiero hablar acerca de los puntos y consideraciones con respecto al comunicado, como lo pidió Laureen. Definitivamente estamos de acuerdo en que esto es algo que hemos estado pidiendo por mucho tiempo en el GAC. Esto es algo que definitivamente debemos apoyar.

Con respecto a información adicional, tal vez añadir en la sección de uso indebido del DNS otros temas de importancia. Primero, por ejemplo, la importancia de medidas preventivas. Nos preocupa que hasta ahora lo que hemos escuchado tiene que ver con las medidas activas pero la prevención para el uso indebido del DNS también es clave según nuestra perspectiva. Lo escuché previamente de uno de los colegas también. La posibilidad de explorar el tema de incentivos. Este tema surgió de los colegas del PSWG.

Por último, con respecto a lo que dijo Nigel en cuanto a la siguiente ronda de los nuevos gTLD, queremos asegurarnos de que el trabajo anterior no se olvide, especialmente con las medidas razonables para impedir el uso indebido del DNS. El GAC ha sido muy fuerte en enlazar la exactitud de los datos de la registración del nombre de dominio y el

uso indebido del DNS, y eso es algo que se indicó en el comunicado 71, 72 y 73. Esperemos que el trabajo se haga en cuanto a la exactitud de la registración de nombres de dominio, que esto no se pierda para prevenir el uso indebido del DNS.

MANAL ISMAIL: Ahora va a hablar Japón.

NOBU NISHIGATA: Muchas gracias, Manal. Buenas noches porque ya es de noche en Japón. Buenos días y buenas tardes de parte de Tokio. Gracias a la organización por esta excelente sesión de hoy. Quiero responder a la presentación de Laureen con respecto al comunicado. Japón quiere expresar su apoyo con respecto a las negociaciones de contrato que están en progreso. Aceptamos el progreso hasta ahora.

Por otro lado, Japón sí quiere sacar a relucir un tema con respecto al acuerdo de acreditación del registro según el artículo [3.18.1] que requiere que los registradores denuncien actividades ilegales. El gobierno japonés sigue pidiendo que se mejore el texto o los términos del contrato cuando tiene que ver con denunciar estas actividades ilegales.

Todavía hay muchas evidencias que se pueden pedir como por ejemplo el informe de auditoría de ICANN o los informes de la GNSO. Japón está esperando este informe preliminar y estamos ansiosos de poder hablar intersesional con respecto al progreso de esto y poder expresar nuestras inquietudes. Sin embargo, sí queremos expresar

nuestro aprecio con respecto a la información actualizada de las negociaciones y estamos ansiosos de poder continuar esta conversación con ustedes.

MANAL ISMAIL: Gracias, Japón. Gracias, Bertrand, Gabe, Chris y Laureen. Gracias a todos. Vamos a volver a reunirnos a las 3:00 hora de Cancún. Por favor, estén aquí a tiempo para la sesión bilateral de la junta. Gracias.

[FIN DE LA TRANSCRIPCIÓN]