ICANN71 | Foro virtual de la comunidad – Discusión del GAC sobre la mitigación del uso indebido del DNS
Lunes, 14 de junio de 2021 – 14:30 a 15:30 CEST

GULTEN TEPE: Bienvenidos a la sesión del GAC de la reunión 71 de ICANN sobre la mitigación del uso indebido del DNS, para ahorrar tiempo no vamos a nombrar a todos los asistentes, pero los nombres de los miembros del GAC presentes se incluirán en el anexo al comunicado y a las actas del GAC.

Recordamos a los miembros del GAC presentes que por favor escriban su nombre y a quién representan cuando ingresan a la sala de Zoom, si desean formular una pregunta o hacer un comentario, por favor escríbanlo insertando la palabra “question” o “comment” entre corchete angulares para que todos los participantes puedan verlo.

Las sesiones del GAC tendrán interpretación simultánea a los seis idiomas de Naciones Unidas y el portugués, hagan clic en el ícono de interpretación en Zoom que aparece en la barra de herramientas para elegir el idioma que desean escuchar y en el que desean hablar.

Los micrófonos estarán silenciados durante toda la sesión, a menos que se haya solicitado la palabra, si desean hablar levanten la mano en la sala de Zoom. Por favor digan su nombre para los registros al hablar e indiquen el idioma en que lo harán, si no es inglés.

Les pedimos que hablen en forma clara y a una velocidad adecuada para permitir una interpretación correcta. Finalmente, tengan presente que esta sesión, como el resto de las actividades de la ICANN, se rigen por los estándares de comportamiento esperados, incluimos el vínculo correspondiente en el chat para referencia.

Por favor silencien todos sus dispositivos y notificaciones para evitar el ruido ambiente. Habiendo dicho esto, le cedo la palabra a Manal Ismail.

MANAL ISMAIL, GAC CHAIR: Gracias, Gulten. Bienvenidos a todos, tenemos una sesión ahora de 90 minutos donde vamos a hablar de la mitigación del uso indebido del DNS, esperamos en 60 minutos… Si podemos terminar entonces en estos 60 minutos, después vamos a tener 30 minutos para hablar del comunicado, comenzar a debatir algunos de los temas que pueden estar incluidos en el comunicado, así como también quienes los pueden redactar.

Veo que ya tenemos una lista larga de oradores del grupo de trabajo de seguridad pública del GAC, nuestro colega japonés también ha invitado a gente del grupo de trabajo de abuso de mensajes, mensajerías y móviles.

Sin más entonces, quiero ver quien empieza. Laureen, perfecto. Gracias.

LAUREEN KAPIN: Soy una de las copresidentas del grupo de trabajo de seguridad pública del GAC, también está conmigo Chris Lewis-Evans copresidente y el

colega del FBI Gabe Andrews que se está levantando muy, pero muy temprano, como también sé que muchas otras personas.

Tenemos para este tema, en particular, invitados especiales, Shinya Tahata de Japón y también disertantes invitados que vienen a mostrarnos estudios sobre ingreso a registración de datos de nombres de dominios.

Bueno, como usted pudo ver, Manal… Pido disculpas antes de empezar si es que tomamos o si nos excedemos un poco más del tiempo para llegar a estos 90 minutos, pero bueno, yo creo que la idea es que todos puedan entender de qué estamos hablando y vamos a dejar las preguntas en general para la parte final, excepto lo que es la presentación de MAAWG y quizás la de nuestro colega de Japón, que quizás quieran responder las preguntas al final de sus presentaciones.

Vamos a empezar entonces con lo que nos compete, como ya se dijo, el uso indebido del DNS es uno de los temas sobre los que volvemos reunión tras reunión porque es muy importante, es un tema que en su mayor parte lo vemos en las noticias todos los días, hay amenazas a infraestructuras críticas, sistemas financieros, energía y esto impacta en la vida diaria de las personas donde puede haber robo de identidad y, además, estos malhechores utilizan el DNS para realizar sus delitos.

Vamos a hablar de distintos temas que tienen que ver con el uso indebido del DNS y también de qué forma nosotros como comunidad podemos mitigar este uso indebido, también va a haber un informe actualizado sobre un documento de SSAC.

Gabe del FBI va a hablar de un trabajo en colaboración realmente que ha hecho con nuestros colegas de las partes contratadas, un tema específico que tiene que ver con el uso indebido del DNS, temas asociados también con botnets y software malicioso.

También se va a hablar de cuánto tiempo lleva responder a los pedidos de datos de registración, nosotros sabemos que esta información puede resultar crucial para los investigadores porque a veces quieren explotar el DNS, también vamos a hablar de lo que son las recomendaciones del equipo de revisión de confianza, elección de los consumidores y competencia.

También se va a hablar de los registratarios del DNS, cómo pueden ir y recurrir a las partes que deben recurrir, y no a quienes quizás no tengan la información que están procurando.

Y después nuestros colegas del MAAWG van a dar una presentación interesante, también el colega de Japón, obviamente cumplimiento contractual de ICANN es uno de los actores clave en este tema y vamos a ver cuáles son los pasos futuros, es decir, la agenda está bastante completa, es un menú completo, por lo que vamos al primer plato directamente, a Chris Lewis-Evans del Reino Unido.

Voy a saltear esta diapositiva porque básicamente habla del programa y la verdad que la ICANN les ha dado mucha información sobre los eventos que se van a realizar sobre este tema, así que, Chris, ahora le pido que nos hable un poco del informe del SSAC.

CHRIS LEWIS-EVANS: Gracias, Laureen. Bueno, vamos a hablar de este documento SSAC 115 que tiene un enfoque interoperable para ver cómo poder solucionar el manejo abusivo del DNS, tiene un marco propuesto donde abarca una gran cantidad de documentos.

Muchos de estos documentos nos resultan más interesantes para el PSWG o para la política, y el primero tiene que ver con el punto primario de contacto para resolver estos casos de uso indebido. Una de las cosas con las que luchan las autoridades es ver cómo llegar a una resolución de estos problemas y cómo se ve en la industria en general.

A veces lo que sucede es que, en lugar de ir al lugar adecuado, se envían avisos de uso indebido a los que uno puede pensar y solo uno tiene el efecto deseado. Entonces este punto primario tiene que ver con crear un solo lugar para que todos los pedidos vayan ahí y tener, obviamente, el punto de contacto correcto para llegar a la resolución.

Después tenemos los caminos de escalamiento, en el sentido de que, uno quiere ir al punto que tenga una relación directa con la entidad que está generando este uso indebido, a veces no responden, entonces tenemos estos caminos para ir escalando en la jerarquía y poder ver entonces cómo elevar este pedido para llegar a quien corresponda y obtener una respuesta.

Obviamente también hay un cronograma vinculado con este camino y también sé que algunos miembros del SSAC no estuvieron de acuerdo con algunas de las propuestas realizadas en el SSAC 115.

Uno tuvo que ver con esto, con los caminos de escalonamiento, cuáles eran los períodos que se daban para pasar de un escalón al otro, muchos pensaron que no era la velocidad adecuada. Esto es algo que se planteó.

Pero bueno, creo que para empezar es mucho mejor de lo que podríamos haber esperado, las autoridades lo que quieren hacer es garantizar que tenemos unas normas también porque piensan que es bueno tener normas, que las cosas estén normalizadas con estándares, que hablen de distintos rangos de gente que participan, como ver cuáles son los que manejan el tema de uso indebido del DNS y reducir así la carga de algunas otras entidades que reciben solicitudes todos los días.

Después el tema de la terminología de la evidencia y las normas, que también tiene que ver con los caminos mencionados anteriormente, cómo se hace esta elevación del pedido.

Y algo que creo que también abarca varios puntos, tiene que ver con la disponibilidad y la calidad de la información del contacto, esta información a quién hay que dirigirlo, si realmente vamos a obtener el resultado que queremos dirigiéndonos a ese contacto, entonces también se habló de esto, tenemos que pensar en los revendedores, por un lado.

Y hay otro aspecto, que son los datos reales que se reciben para ver si estos datos son correctos o no y permiten entonces tomar las acciones más adecuadas y convenientes.

Esto se centra entonces en respaldar todo lo propuesto, pero obviamente creo que lo más importante es el tema del contacto y estos caminos de escalonamiento. Siguiente diapositiva, por favor.

Dentro del SSAC 155 surge con estas recomendaciones de múltiples partes que, se necesita un poco de consideración de que el uso indebido del DNS no está limitado a la comunidad de la ICANN, cómo la ICANN puede comenzar una conversación y mostrar en la industria cuáles son las mejores prácticas porque tenemos que tener en cuenta que son varios los actores que intervienen.

Como mencioné, en el PSWG la propuesta es tener un facilitador común del uso indebido, como se llama acá, para dar respuesta a los pedidos para que entonces empiece esta persona a iniciar la conversación y ver cómo se puede implementar, hemos tenido diálogo con varias partes y todos dicen que sería bueno tener estas conversaciones con una persona y me gustaría ver esto en el futuro.

Sabemos que el GAC ha visto esto como algo a lo que podemos respaldar y realmente realizar aportes sobre cómo podría funcionar dentro de cada una de las distintas jurisdicciones. Tenemos que tener presente entonces todo esto y le voy a dar la palabra a Gabe, gracias.

GABRIEL ANDREWS: Yo le voy a dedicar 10 minutos a hablar del marco de los DGA y lo que tiene que ver con el software malicioso y botnets. Esto es un proyecto entre el grupo de trabajo de seguridad pública y el de registros,

realmente hemos hablado y también le dimos la oportunidad a este otro grupo de definir.

Cuando decimos DGA esto es algo técnico y tiene que ver con los botnets y los botnets son redes que lo que hacen es comprometer a los dispositivos que están controlados por delincuentes, algunos de los más grandes con los que tuvimos que ver en el pasado tiene que ver con conficker y Avalanche.

Si están controlados por los malos, utilizan estos algoritmos que generan dominios, los DGA. Estos algoritmos son un código, una herramienta que se puede utilizar para ingresar una fecha y tiempo específico y sacar un nombre de dominio para ese momento específico.

La acción que han tomado las autoridades contra estos DGA, contra los botnets, es algo que tiene que ver con que son bajos en frecuencias, pero su impacto es alto, es decir, que pueden dar una acción muy amplia de todos los dominios vinculados con los botnets que tienen estos DGA.

Puede tener un impacto administrativo, tanto en los registros con los que participamos como en las autoridades con las que participamos, por ejemplo, si tenemos cientos de miles de dominios vinculados con este output o salida del DGA, las autoridades antes tenían que ir a los tribunales una vez al año para actualizar cuáles eran los dominios vinculados con ese DGA.

Y realmente esto se hace año tras año, los tribunales tienen que investigarlos, los registros realmente no querrían ir a ICANN como para

solicitar dispensas por las solicitudes realizadas a los tribunales por las autoridades.

Entonces dentro de este marco se dio la posibilidad de hacer una derivación de estos DGA para uno solo, esto es una acción perenne, sería una acción que perdure durante toda la vida del botnets, toda la vida del DGA y no tener que hacer los registros todos los años, una nueva solicitud para esta dispensa en la ICANN. Este marco en realidad es voluntario, no es vinculante.

El grupo de partes interesadas de registros y de seguridad pública quieren que los entendimientos a los que llegamos comunes, sean útiles para establecer el proceso futuro de todas las partes, los registros, las autoridades… Todos los que tienen que tomar una acción responsable para evitar estos DGA en los botnets.

Habiendo dicho esto, quisiera pedirle a James Galvin… Para saber si él quiere decir algo dentro de su representación en el grupo de registros.

JAMES GALVIN: Bueno, yo quería hablar acá que el marco de uso indebido del DNS es importante, yo sé que no es… Perdón, esta es la imagen que quería mostrar, no la anterior porque no están en secuencia.

El marco de uso indebido del DNS es algo que abarca muchas cosas y tienen que ver con el SSAC 115, como habló Chris, el marco como el que habló Gabriel. Entonces este marco habla del ecosistema legal al que hace referencia el SSAC 115 y podemos ver acá a la derecha que el

sistema de registración, donde tenemos registros y registradores, son una parte pequeña de este ecosistema.

Estas son las cosas sobre las que podemos actuar, entonces lo que hace el marco es tener una definición del uso indebido del DNS y esto significa que los registros y los registradores pueden directamente accionar dentro de este marco, mientras que el DGA es nada más que un subgrupo, es una pieza nada más de la cantidad de cosas que son directamente aplicables a los registros en particular.

Este es el espacio en el que nosotros podemos actuar directamente y rápidamente para solucionar este tipo de inquietudes, pero como lo dice el SSAC 115, el marco, cuando fue completado hace un par de años, desde ese momento ha sido adoptado por distintas partes contratadas y también haber sido reconocido para ambos grupos de partes interesadas.

Si bien es voluntario, también dice que hay muchas personas que son parte del ecosistema, pero no están presentes, si pensamos en el SSAC 115 nosotros hablamos de las acciones, del tiempo necesario, pero la idea es ver cómo hacemos que todo esto funcione dentro de los registros y dentro de los registradores.

El problema es mucho más amplio de lo que nosotros podemos hacer en nuestro espacio y existe la necesidad de tener un facilitador, que es el que nombra el SSAC 115, porque hay muchos otros actores que están por fuera del sistema de registros que no son parte de este debate y ellos también tienen un rol que cumplir, son parte de esto también.

Muchas de las acciones y de los programas… Por ejemplo, cuando hablamos de SSAC 115 y cómo tener un facilitador para respuesta es útil, tiene que ver si vamos a la persona correcta en el momento correcto, los registros tienen algunas acciones que pueden tomar en algunas circunstancias.

Nosotros como registradores somos parte y tenemos que hacer la derivación a las partes adecuadas, pero quizás sería más fácil si directamente se va, se dirigen los pedidos a esas partes que tienen que decirlo. Esta demora entonces en responder al uso indebido, la acción que tiene que tomarse, todo tiene que ver con que las partes correctas sean las contactadas.

Yo hablo en nombre del grupo de la cámara de partes contratadas, igualmente los registros están trabajando directamente con el PSWG y el grupo de partes interesadas del registro, el PSWG es parte de todos ellos, nosotros estamos contentos de trabajar con ellos y con ICANN para generar otro marco voluntario para quienes quieran realmente mitigar el uso indebido del DNS.

Nosotros esperamos hacer nuestra parte para poder enfrentar este uso indebido creciente que está en el DNS. Muchísimas gracias por su atención.

GABRIEL ANDREWS: Gracias, James. Y quería remarcar algo, hay una oportunidad de acción colaborativa, así que invitamos a las distintas Unidades Constitutivas,

socias del GAC, a que participen y si tienen áreas de acciones viables, las marquen porque siempre hay espacio para ello. Muchas gracias.

LAUREEN KAPIN: Muchísimas gracias a nuestro invitado James y a Gabe por su presentación. Ahora vamos a cambiar de tema, pasaremos a algo que ya ha sido abordado cuando Chris habló del SSAC 115 y es el tiempo para obtener las respuestas a las solicitudes de datos del WHOIS.

Es un tema que se está discutiendo, se está debatiendo en este momento en el equipo de revisión de la implementación de la fase 1, les doy un poco de contexto.

Las solicitudes urgentes son muy limitadas y se restringen aquellas circunstancias que representan una amenaza inminente a la vida, lesiones físicas graves, daños a la infraestructura crítica o explotación infantil, en casos en que su divulgación es necesaria, para luchar contra esta amenaza o para lidiar con ella.

O sea, es una categoría muy estrecha de solicitudes que típicamente no se formulan y los representantes del GAC ante este equipo, solicitan que se responda dentro de las 24 horas y esto se compara con el tiempo de respuesta de solicitudes no urgentes, que es de 30 días.

Sobre la base de las recomendaciones se contempla específicamente que el plazo para las solicitudes urgentes sea determinado por el equipo de revisión de la implementación, que no sea algo determinado por la política y esto lo queremos señalar para su atención porque lo que se discute en este momento es esta comparación, este período de 24

horas, algo que, para los expertos en la aplicación de la ley, a veces puede ser demasiado extenso.

Hay un argumento que se lleva en realidad hasta tres días hábiles responder estas solicitudes, cuando algo pasa, un día hábil (las 24 horas), es una situación posible de que ocurra algo malo durante un fin de semana y se concreta este período tres días hábiles o de tres días consecutivos cuando hay fines de semanas y en una amenaza muy urgente.

Cuando hay una amenaza a la vida o lesiones físicas, daños a la infraestructura, estos períodos pueden sumarse hasta seis días, o sea es una categoría muy estrecha de solicitudes que requieren una respuesta muy rápida para que los organismos de aplicación de la ley puedan trabajar para proteger al público. La siguiente, por favor.

Este tema también está relacionado con los datos de registración y es algo muy importante para luchar contra el uso indebido del DNS, y se relaciona con una diapositiva que presentó James, cuando habló de los actores claves que están presentes en este ecosistema, además, de los registradores y los registros están los revendedores.

Este tema fue tratado en la revisión de CCT en la recomendación 17 y de alguna manera cierra esta brecha que existe cuando los registradores publican los datos y los registros, hacen una solicitud de información de registración y a veces no es el registrador el que tiene esta información, sino una parte relacionada con el registrador, es decir, un revendedor.

O sea, es una recomendación muy sencilla que hizo el equipo de revisión de CCT, que la ICANN recopile los datos y dé a conocer la cadena de partes responsables por las registraciones.

La Junta Directiva aceptó esta recomendación e indicó que ya se está poniendo en práctica, pero el problema aquí es que, aunque a veces esta información está en el registro público de datos de registración, no existe la obligación de que esté y queríamos señalar este tema porque sigue requiriendo una acción adicional para que sea aceptada plenamente.

Nosotros creemos que la Junta Directiva apuntaba a la aceptación plena de esta recomendación, pero esto requiere la recopilación y divulgación de la cadena de partes, tales como los revendedores que son responsables para las registraciones. La razón por la cual esto es importante es porque les permite a los organismos de la aplicación de la ley que ahorren tiempo, no tener que ir a cada una de las partes que tienen la información.

En algunos casos, hay derivaciones entre dos o tres partes porque puede haber varias partes involucradas. Nosotros creemos que esto es de fácil resolución y esperamos ver algún tipo de medida que cierre esta brecha y que haga que la situación o la posibilidad de obtener información para proteger al público sea un proceso más sencillo. La próxima diapositiva, por favor.

Ahora, vamos a recibir una presentación que se refiere también al acceso a los datos de registración de nombres de dominios y tiene que ver con un estudio reciente del grupo de trabajo sobre la lucha contra el

uso indebido en mensajería malware y dispositivos móviles, y el grupo de trabajo contra phishing dieron a conocer, nos van a contar un poquito más al respecto. En esencia, para darles un adelanto.

Se trata de un relevamiento que hicieron los investigadores en el área cibernética y los proveedores de servicio contra el uso indebido, esta encuesta tenía como propósito entender de qué manera la aplicación por parte de la ICANN, del GDBR, de la Unión Europea, ha impactado en el servicio del WHOIS y el trabajo contra el uso indebido.

Y discute específicamente la especificación temporaria sobre el acceso por parte de los actores que trabajan contra el uso indebido y el uso de la información de registración de nombres de dominios, que es esencial, es central para diferentes investigaciones. En ese sentido, le pasaré la palabra a mis colegas, les agradezco por adelantado por brindarnos esta actualización.

LAURIN WEISSINGER: Muchas gracias, Laureen. Veo que las diapositivas ya están en pantalla, pasemos a la primera diapositiva.

Como decía Laureen, esta es una encuesta que hicieron en conjunto el grupo anti-phishing y el MAAWG. Los investigadores principales están en pantalla, quien les habla, Dave Piscitello, quienes muchos de ustedes conocen y también Bill Wilson que está con nosotros en esta llamada y va a hablar, quien es un asesor senior del MAAWG. La siguiente, por favor.

Rápidamente para que todos en esta llamada sepan qué es MAAWG, el MAAWG fue creado en el año 2004, es el grupo de trabajo que lucha contra el uso indebido en el área de mensajería malware y dispositivos móviles, es el más grande de la industria, incorpora todas las partes interesadas que les interesa el tema de abordajes cooperativos para luchar contra el uso indebido de manera cooperativa.

Nosotros hacemos dos cosas, por un lado, desarrollamos y publicamos documentos de mejores prácticas, declaraciones de posición, capacitación, etc., para ayudar a la comunidad en línea a luchar contra el uso indebido.

Y también hacemos acciones de incidencia de política pública, no es lobbying, para dar orientación técnica y operativa a los gobiernos y a los organismos de política pública de internet para desarrollar políticas sin legislación. La siguiente.

Para este estudio obtuvimos 277 respuestas de distintos contactos a través de listas de correos, las respuestas fueron proporcionadas por organismos que trabajan en ciberseguridad, aplicación de la ley, seguridad pública, etc., o sea para un grupo específico.

También quiero señalar que los usuarios fueron muy diversos, es algo que nuestro estudio quiere resaltar, cómo se acceden a los registros, qué propiedades son necesarias, por ejemplo, hay una gran diferencia entre quienes utilizan los datos para hacer análisis beta, quienes tienen accesos infrecuentes o los organismos de aplicación de la ley para sus investigaciones.

GULTEN TEPE: Voy a pedirle al orador que hable un poquito más despacio, por favor.

LAURIN WEISSINGER: Por supuesto, disculpas. Entonces veamos a los encuestados, vemos que la mayoría son profesionales de ciberseguridad, un 40%, seguidos por un 25% de personales jurídicos, también la comunidad académica, empresas, ISP y seguridad pública.

Aquí estamos comparando un estudio de datos del WHOIS, un estudio del 2018 y uno de este año, estudio que hizo el MAAWG también. La siguiente diapositiva.

Es importante señalar que, incluso dentro de esta muestra tan particular, es decir, no demasiadas personas, uno de cada 10 encuestados hacen más de 10 mil consultas por día y más de 2/3 están por debajo de las 100 consultas.

Más allá de estos números, lo que las solicitudes comprenden y cómo se utilizan los registros es variable. La siguiente por favor. Aquí lo que vemos es que, comparando la encuesta del 2018; que en ese momento lo que se estudió fue el uso combinado, podemos ver que, en general, se da una disminución en términos de volumen de consultas, con muy poquitos aumentos.

Y el grupo más grande, como pueden ver, es el de datos técnicos, es decir, elementos que no están expurgados. En el 2021 el volumen de

consulta es aproximadamente el mismo, un poco más del 50% de los encuestados. La siguiente, por favor.

El acceso al WHOIS está reflejado en los números que vieron antes, aquí ven que más del 36% lo utiliza para hacer consultas en la web del WHOIS con distintas tecnologías al resto. La siguiente. Hay mucha más información en el informe que les invito a leer, esto es solo un pantallazo general, veamos el efecto de la especificación temporaria según nuestros encuestados.

Casi el 71% dicen que el tiempo para mitigar las amenazas excede el umbral aceptable, o sea esto es un gran problema obviamente, es decir, la especificación temporaria tiene un efecto en especial con respecto a la oportunidad.

Luego, menos del 10% dice que las investigaciones no se ven afectadas y un poquito más del 20% dice que sí se ven afectadas, pero pueden seguir manejándolas dentro de un tiempo aceptable. La siguiente por favor.

Y si esto lo comparamos ahora con el 2018, vemos que hay un leve aumento de las personas que dicen que el tiempo para mitigar excede el umbral aceptable, del 65.6% al 70.9% o sea, un poquito peor. La siguiente, por favor.

Como pueden ver; y no es de sorprender, más del 80% nos dice que el tiempo para manejar las actividades maliciosas en línea ha crecido y también para manejar los dominios maliciosos, hay que tener en cuenta que esto ya lo escuchamos varias veces, pero vale la pena volver a

decirlo. Es necesario actuar, la mayoría de las actividades criminales que tienen lugar es para obtener algún tipo de lucro, tratemos de resumir entonces las cuestiones. Si quieren más detalles lo encontraran en el informe, es un tema de interés con muchos más gráficos y mucha más explicación.

Solo 1/4 de los encuestados pudieron encontrar fuentes de datos alternativas, la atribución se ve perjudicada en gran medida; no es de sorprender, y aquí 9 de 10 encuestados informan problemas en este sentido, debido al hecho de que los datos están siendo expurgados.

Más del 50% consideran que la expurgación de los datos de personas jurídicas y no europeas es excesiva, y solo el 2.2% considera que la especificación temporaria funciona. La siguiente.

Entonces una de las maneras que nosotros tenemos para manejar los datos expurgados del WHOIS es enviar una solicitud para lograr obtener los datos que están expurgados u ocultos. El 34.4% de nuestros encuestados nos dijeron que no lo hacen porque lo consideran demasiado laborioso.

Un poquito menos de 1/4 sí lo hacen y fíjense que el resto está dividido entre que, pensaban que no estaba disponible o que no sabían cómo hacerlo y quiénes no responden o consideran que no es parte de sus casos y usos. La siguiente, por favor.

Aquí vemos, nuevamente, que en comparación con el 2018, los tiempos de respuestas experimentados por los encuestados en promedio han aumentado, en particular; y algo que creo es interesante, este período

de más de 7 días del que hablábamos, una semana en promedio en comparación con el 2018, hubo un aumento del 60%, es decir, que es un largo tiempo de espera para obtener la respuesta a la consulta. La siguiente, por favor.

¿Este plazo de 30 días es aceptable para nuestros encuestados, para la divulgación de los datos expurgados? Bueno, como pueden ver, en general la respuesta es no, los investigadores, el 50%, consideran que está bien en 30 días, en el área de marcas comerciales y propiedad intelectual para un poquito más de un 1/4 está bien, pero para los demás necesitan períodos de respuestas más rápidos.

Spam 10%, pero, en general, no es considerado aceptable por los encuestados, propiedad intelectual, marcas comerciales. Propiedad intelectual es gente que por ahora estaría conforme. La siguiente, por favor.

Y aquí es donde vemos lo que podría ser considerado como aceptable por los encuestados, vemos que, para malware, phishing, botnets, etc. Tenemos un promedio inferior a la base del marco para spam, por debajo de 4, para cuestiones de propiedad intelectual. En promedio, la gente estaría conforme con 5.5, 5.3 y los investigadores con un 10. La siguiente, por favor.

Con la divulgación, aquí lo que queremos es garantizar que las respuestas sean informadas, sean claras, pero son dispares. A veces se recibe una acuse de recibo, pero no se reciben los datos, a veces se reciben datos incorrectos, o sea que no son viables.

También evaluamos los sistemas de divulgación que la ICANN está considerando, y tengan en cuenta que estos datos son de hace unos meses atrás, así que probablemente deba ser actualizado. Se habla de un sistema de pago y el 61% de los encuestados informaron que no tienen ni la capacidad o los recursos para pagar un sistema de esta naturaleza.

El 39% indicaron que sí estaban dispuestos a pagar una tarifa, el 78% estaría dispuesto a pagar una tasa de acreditación razonable y el 61% aceptaría un sistema en niveles o precios por volúmenes. La mayoría de los encuestados también indicaron que un sistema sí es totalmente inapropiado tener que pagar para esta información. Siguiente diapositiva, por favor.

Y, por último, aunque no lo menos importante de lo que quiero contarles los reclamos ante la ICANN, ¿cuán satisfecho se sienten cuando se ha presentado un reclamo ante cumplimiento de la ICANN con el manejo que se ha hecho, un reclamo sobre las solicitudes de datos de registración. Vemos que la situación no es demasiada positiva, el 45% está muy insatisfecho, un 35,9% dijeron que están algo insatisfechos.

Y con esto me gustaría pasarle la palabra a Bill Wilson, quien les va a presentar un resumen de esta presentación. La siguiente diapositiva, por favor.

BILL WILSON: Hola a todos, espero que me escuchen bien. Hay cuatro observaciones que, creo que nosotros podemos sacar de todo esto, uno es que todos estamos de acuerdo en que necesitamos que todos los datos relativos que sean posibles; y obviamente seguimos protegiendo la privacidad de las personas naturales, tendrían que estar disponibles. Las respuestas a la encuesta muestran que lo que está debatiendo la ICANN no va a cumplir con la necesidad de las autoridades o los actores en el ámbito de la ciberseguridad.

El tercero es que, nosotros o la ICANN debe establecer un sistema funcional que le permita que los datos de los registratarios puedan ser accedidos por las partes acreditadas, es necesario que exista un sistema tanto para los profesionales de ciberseguridad, como para las autoridades encargadas de la aplicación de la ley, pero tienen que funcionar de una forma que elimine parte de estas demoras en el tiempo y, obviamente, también tiene que incluir controles estrictos de privacidad y controles de seguridad, tiene que haber algún método o algún sistema para rendir cuentas al respecto.

El cuarto de los puntos que se señala acá dice que, como se mencionó anteriormente, hay dos tipos de usuarios, unos que son los que realmente lo usan muchísimo y otros que son los menos, los que lo usan una vez cada tanto o con un volumen muy inferior. El sistema debe ser capaz entonces de manejar ambos tipos de abusadores. Siguiente imagen, por favor.

Entonces los tres puntos acá que resumimos es que, la especificación temporaria para el sistema de acceso mostró que aumenta la cantidad

de tiempo como para abordar todas estas cosas y entonces la oportunidad del acceso es un desafío realmente para una gran cantidad de personas. La otra es que, el sistema no es uniforme dentro de toso los registros, entonces cuando uno obtiene cierta información de determinada manera de uno, pero no de los otros.

Y esto, obviamente, genera otro tipo de dificultades. Tiene que existir un sistema de pedidos formales para poder acceder a los datos expurgados, en comparación con los otros porque en realidad esto fracasa habitualmente porque a veces son ignorados, son rechazados, lleva demasiado tiempo la respuesta, entonces lo que sucede es que, tarda tanto la respuesta que ya carece de valor.

Y lo otro, que son los procesos de cumplimiento contractual de la ICANN, fueron descritos como muy largos y deficientes, y que con frecuencia no brindan una solución o un recurso. Esperamos entonces poder cambiar esta situación en el futuro, siguiente imagen por favor.

Si tienen alguna por pregunta por fuera de lo que es este formulario ahora, les pedimos que nos envíen un correo electrónico a la dirección que figura en pantalla para poder respondérselo, con suerte, con mayor velocidad de la que estuvimos hablando en esta conversación. Gracias.

LAUREEN KAPIN: Gracias, Bill, gracias, Laurin, por esta presentación tan interesante con realmente ejemplos concretos de la vida real, algunos de los desafíos que experimentan los profesionales de la ciberseguridad, así como las autoridades de la ley. Realmente esto nos permite seguir pensando en

los desafíos que tenemos por delante, cómo trabajar y cómo equilibrar adecuadamente el tema de datos bien protegidos, pero, por otro lado, prestarle atención a lo que es la seguridad pública.

Ahora vamos a cambiar de tema por completo, en este caso, nuestro colega de Japón, Shinya Tahata, que va a hacer una presentación, así que le voy a dar la palabra. Gracias.

SHINYA TAHATA: Gracias, Laureen. Hola a todos.

En primer lugar, quiero agradecer realmente a los copresidentes del PSWG por darme esta oportunidad de hablar. Hoy tengo algunas actualizaciones porque hubo una propuesta realizada en marzo en la ICANN70, entonces yo querría presentar información junto con estas ideas, al mismo tiempo que podemos hablar de medidas concretas para fortalecer lo que es el cumplimiento contractual de los registros y los registradores.

En la ICANN70 nosotros llegamos al entendimiento de que había algunos casos que tenían conflicto con el RAA, por ejemplo, que no se exigía la información de estos registratarios y que era necesario que estos registratarios tenían que saber cuáles eran los datos exactos que estaban en el WHOIS.

Como se mencionó, el uso indebido de los dominios tenía que ver con algunos registros y registratarios, no con todos, según el grupo de estudios hubo 15 nombres de dominios maliciosos registrados por un solo registratario y no seguían con las disposiciones del RAA, pidiéndole

la información de los registratarios, por lo tanto, si se garantiza el cumplimiento y hay empresas que no cumplen, puede ser una de las medidas eficaces contra el uso indebido del DNS.

Quiero hablar de tres puntos que tienen que ver con el cumplimiento del RAA, en primer lugar, hay que recopilar información correcta de los registratarios cuando hacen la registración del dominio, según lo plantea el RAA, los registradores deben recopilar la información de los registratarios como la dirección postal, número de teléfono y también los que tienen que ver con las normas de la ICANN y hay algunos que no la siguen.

Es por eso que no podemos disminuir este uso indebido, tiene que haber auditorías de parte de cumplimiento contractual de la ICANN para verificar que esto se cumple. En segundo lugar, verificar la identidad de los registratarios, según lo dice el RAA, estos registratarios tienen que cumplir con ciertas medidas, si no lo hacen podemos tener lo que es la suspensión del número de dominio por una cantidad de días.

Y verificar, también, que los datos sean correctos, por lo tanto, se puede suspender el nombre de dominio a los registratarios basándose en esta disposición, también tienen que tener la verificación del número de teléfono para verificar identidad. En tercer lugar, también tiene que haber una respuesta estricta a lo que son los informes de uso indebido de parte de cumplimiento contractual de la ICANN, tiene que haber un programa de cumplimiento del registratario.

Y es importante pedir pruebas para demostrar que estos nombres de dominios no son abusivos, también hay que ver cómo se manejan estos temas de uso indebido. Esto es muy importante.

Tiene que haber normas específicas, así como establecer normas para mitigar el uso indebido y normas que se basen en el contrato RAA. Además de estos tres puntos podemos hablar de las listas de bloqueo y su eficacia en el futuro para que los registros y los registradores tomen las medidas adecuadas. Es esencial que los registradores respondan a este uso indebido, verifiquen la identidad de los registratarios sobre la base del RAA.

Esto sirve para garantizar el uso del internet, entonces podemos seguir hablando en estas reuniones de la ICANN sobre los temas que tienen que ver con el uso indebido del DNS y que son de suma importancia para todos nosotros usuarios de internet. Muchas gracias por su atención.

LAUREEN KAPIN: Muchísimas gracias porque, además, en su presentación usted presentó propuestas precisas, así que muchas gracias por ese aporte.

Tenemos distintos sabores dentro de nuestro menú de uso indebido del DNS, brevemente yo voy a hablar de los próximos pasos, cosas que pueden ser posibles y después voy a dejar un tiempo para preguntas. Yo sé que esta diapositiva tiene que ver con disposiciones contractuales específicas más allá del tema general, pero esto es algo que armó nuestro colega de Japón y que realmente es muy útil para tener a mano.

Ahora, en lo que respecta a los pasos futuros hubo muchas propuestas que tenían que ver con cómo mitigar el uso indebido del DNS y el uso indebido del DNS en sí mismo, el Proceso de Desarrollo de Políticas de los procedimientos posteriores, que es un grupo específico de la GNSO indicaron que el uso indebido del DNS tiene que hacerse valer respecto de todos los gTLD y no solo los nuevos gTLD, es algo, en otras palabras, que tenemos que manejar de manera holística. No solamente vinculado con la próxima ronda de gTLD.

Hay algo que tenemos que tener en cuenta y es que, en la primera ronda de los nuevos gTLD, de hecho, esto actuó como una oportunidad, como un incentivo para levantar la vara y entonces hacer que las disposiciones contractuales fueran mucho más poderosas para evitar el uso indebido.

Entonces los contratos para estos nuevos gTLD incluyen ese tipo de disposiciones y eso fue un avance positivo. Podemos tener algo similar o incluso un elemento mejorado para esta nueva ronda de gTLD porque, de hecho, hemos aprendido de la experiencia para los contratos del programa de nuevos gTLD. Si bien, son más sólidos sigue habiendo algunos vacíos de los que hablamos en reuniones anteriores, que podemos enfrentar y podemos solucionar en la nueva ronda de gTLD.

Creo que es la oportunidad que tenemos de hacerlo para cundo esta se dé, es por eso que lo mencionamos como un próximo paso, más allá de que sé que existe un debate sobre este tema. Y bueno, sabemos que la perfección es a enemiga de lo bueno, pero tenemos que tratar siempre de mejorar, tenemos que hacer lo que podemos hacer en el momento

en el que podemos hacerlo para poder enfrentar este problema, más temprano que tarde.

Tenemos que seguir debatiendo esto sobre el uso indebido del DNS y cuál es la definición de uso indebido del DNS, nosotros hemos escuchado que hay mucho desacuerdo al respecto, pero, de hecho, también hay un área en común. El GAC hizo una declaración muy concreta en septiembre del 2019 sobre el uso indebido del DNS, hizo hincapié en estos aspectos comunes, que hay un texto contractual que tiene que ver con los gTLD anteriores y que hay trabajo de la comunidad anterior también al respecto.

También se señaló para nuestros colegas de toda la comunidad de múltiples partes interesadas cada uno ha propuesto una definición y realmente ha habido esfuerzos voluntarios muy importantes al respecto, y esto también tiene aspectos comunes que tenemos que tener en cuenta. Siguiente diapositiva, por favor.

Yo querría hacer referencia… Yo quiero dejar tiempo para las preguntas, pero quería hacer referencia, igualmente, a las distintas definiciones que existen del uso indebido del DNS, que también están mencionados en el trabajo que dije del GAC. El equipo de revisión de ccTLD preparó una definición amplia que decía que era actividades no solicitadas con connivencia o engañosas que hacen un uso activo del DNS o de sus procedimientos utilizados para registrar nombres de dominios.

Y el uso indebido de la seguridad del DNS hace referencia a formas más técnicas de una actividad maliciosa como el software malicioso, phishing, etc. Después tenemos los contratos de la ICANN que tienen su

propio texto y también es amplio porque hablan de prohibiciones generalizadas sobre distribuir software malicioso, los botnets que operan abusivamente, phishing, piratería, una violación a los derechos de propiedad intelectual o marcas comerciales.

Entonces utilizando también estas definiciones nos brinda un campo bastante amplio para poder mitigar estas conductas abusivas. Yo quería recordarles entonces el hecho de que nosotros sí contamos con definiciones sobre las que podemos basarnos y que, obviamente, podemos seguir trabajando a futuro sobre estos temas, pero tenemos un cimiento sólido.

Cuando hablamos de próximos pasos; y sé que esto es a muy alto nivel, nosotros estamos alentando al GAC a cuando está trabajando toda la comunidad sobre la definición de uso indebido del DNS, mejoras en las disposiciones contractuales y hacer educación pública, como lo mencionamos acá y en otras reuniones, hay algo que nos emparenta con ALAC y el tener que hablar de esta educación, de hablar con todo el mundo porque si uno lo identifica lo puede señalar y lo puede evitar.

Entonces es muy importante trabajar sobre este último aspecto y creo que el GAC también puede unir fuerzas con otros miembros de la comunidad para trabajar sobre este punto. Le voy a pedir a Manal si quizás podemos dar 5 minutos para las preguntas o, de lo contrario, quizás podamos dar esta oportunidad para otra sesión donde tengamos más tiempo, pero bueno, yo sé que queremos hacer muchas cosas en poco tiempo; que es el que tenemos disponible.

Le doy la palabra nuevamente a Manal y bueno, usted dirá cómo seguimos.

MANAL ISMAIL, GAC CHAIR: Sí, entiendo plenamente que son muchas cosas las que hay que abarcar en esta sesión. Vamos a continuar entonces con las preguntas, yo sé que la idea es revisar rápidamente el comunicado en la media hora que nos queda, pero podemos tratar al menos de reprogramarlo para mañana porque hay otra oportunidad en el día de mañana, me parece que es una sobre el WHOIS y el EPDP.

Esto creo que nos va a permitir hacer algunas preguntas ahora, yo veo muchas preguntas en el chat, pero también veo que la mano de Olivier está levantada, así que, Olivier, por favor le doy la palabra y quienes quieran hacer preguntas del GAC lo pueden hacer obviamente oralmente, ahora le doy la palabra a Olivier.

OLIVIER CRÉPIN-LEBLOND: Muchas gracias a todos. En primer lugar, querría felicitar al trabajo del PSWG porque realmente en esta sesión hemos podido apreciar el trabajo realizado por este grupo, creo que realmente es un tema muy importante el del uso indebido del DNS y también quiero apoyar las propuestas realizadas por Shinya, de Japón, creo que, en definitiva, muchos de los problemas que estamos evaluando acá pueden solucionarse a través del cumplimiento de las obligaciones contractuales, haciendo valer estas obligaciones contractuales, ejecutándolas es algo que se dijo en varios informes.

Obviamente nosotros tratamos de mejorar estas disposiciones, pero me parece que hoy por hoy el cumplimiento estricto de estas disposiciones son herramientas que no permiten, como decía Shinya, nos permite enfrentar a los delincuentes. Muchas de las partes contractuales cumplen con estas obligaciones contractuales, pero hay algunos nada más que no lo hacen y entonces necesitamos concentrarnos en esos, y solucionar esos problemas.

Y también el tema de la exactitud de los datos de registración, esa es otra cosa que resulta muy importante cuando estamos hablando del uso indebido del DNS. Me interesó mucho el informe de Laurin y me gustaría confirmar el tema del acceso a los datos de registración porque obviamente es algo muy importante para las autoridades, hay varios expertos en leyes y Francia ha estado tratando también de promocionar este tema dentro del GAC.

En cuanto al informe del SSAC, el SAC 115, la verdad que las recomendaciones que incluyen son muy útiles y aportan más apoyo sobre todo en nuestro debate que tengamos mañana con la Junta Directiva, qué opinan ellos de eso y cuáles son los próximos pasos sobre este informe también. Muchísimas gracias, Manal.

MANAL ISMAIL, GAC CHAIR: Muchísimas gracias, Olivier. Veo también muchos comentarios en el chat, gracias, dice India, al PSWG por sus esfuerzos incansables de volver sobre este tema con el GAC.

Veo un comentario también de India en el chat que dice: “La educación a los usuarios finales sobre el uso indebido del DNS y la exactitud de los datos del WHOIS ayudarán a mitigar el uso indebido del DNS. La falta de conciencia sobre el uso indebido del DNS en los usuarios de internet debe ser enfrentada por el contenido en diferentes idiomas, para hacerlo debe formarse un grupo sobre los contenidos del curso y también los países interesados deberían participar en el desarrollo de estos cursos en los idiomas regionales”.

Veo que también se hace referencia y se incluyeron enlaces en el chat a distintos materiales que están circulando, también entiendo que vamos a hablar de este tema con ALAC cuando tengamos la sesión bilateral. Me voy a detener acá y lo que quiero hacer es ver si algunos de los disertantes tienen algo que decir.

LAUREEN KAPIN: Creo que hay un interés real de ALAC y del grupo de trabajo de seguridad pública de trabajar juntos sobre estos temas, también sé que nuestros colegas de las partes contratadas están pensando en este tema, han desarrollado material y podemos poner toda esta energía, estos conocimientos y creo que es algo que entonces va a valer la pena.

La idea es también que este material sea traducido a varios idiomas para que el público pueda beneficiarse de este material, de este tema y de estos conocimientos, es una buena oportunidad para esta colaboración.

MANAL ISMAIL, GAC CHAIR: Muchísimas gracias, Laureen. No veo ninguna otra mano levantada, así que si no veo más preguntas espero no haberme perdido ninguna, de lo contrario, les pido que levanten la mano o que la vuelvan a escribir en el chat. Veo sí una pregunta de Dinamarca que dice: "Como la organización de la ICANN está tomando la posición de que no es el responsable o corresponsable de los datos y no pueden hacer valer algunos de los requisitos específicos. ¿Cómo puede cumplimiento contractual de la ICANN cumplir con lo propuesto por Japón?"

LAUREEN KAPIN: Difícil responder a esta pregunta. Yo creo que hay ciertas posiciones tomadas respecto del rol de responsabilidad sobre los datos de la ICANN, y me incluyo, no creo que sea necesario mencionarlas, pero hay que reflexionar sobre estos temas. Aclaro que las cuestiones y exactitud son importantes, y que el hecho de que WHOIS se apropie de la responsabilidad sobre esto es importante.

La disposición del contrato es necesario que tenga obligaciones directas sobre la exactitud y un cumplimiento robusto de las disposiciones existentes sería de beneficio, pero hay trabajo por hacer tal como todos sabemos, existen estas disposiciones contractuales y, sin embargo, hay un problema de exactitud, por eso precisamente se ha señalado la necesidad de trabajar a futuro, lo ha dicho la GNSO, y este grupo está más que dispuesto a participar, así que esperamos arribar a algo positivo.

MANAL ISMAIL, GAC CHAIR: Gracias, Laureen. Chris, adelante.

CHRIS LEWIS-EVANS: Quería agregar simplemente que lamentablemente hay una sección en el RAA que cubre los datos del WHOIS, pero algunas disposiciones del GDPR son levemente distintas, entonces como Laureen lo remarcó, esto requiere que se siga trabajando en la comunidad, sé que el GAC ha ofrecido su ayuda para el trabajo de la GNSO.

MANAL ISMAIL, GAC CHAIR: Gracias, Chris. Sí, precisamente es muy bueno y es necesario pensarse que la pregunta ha sido difícil.

Y la propuesta de Japón me permite insertar una pregunta yo, ¿existe experiencia para demostrar que los nombres de dominios no son abusivos, creo que esto precisamente fue uno de los puntos que se plantearon en la presentación. Entonces si aquí hay experiencia de mejores prácticas sería muy útil poder compartirlas. Mientras tanto, continúo con el resto de las preguntas. Veo una pregunta de Reg Levy de Tucows que dice que Laureen hizo referencia a una definición propuesta por el GAC de uso indebido del DNS.

Creo, Laureen, que usted ya habló al respecto, ¿no?

CHRIS LEWIS-EVANS: Disculpas, Manal. Laureen hizo referencia a la declaración del GAC sobre el uso indebido del DNS y puse una copia del vínculo en el chat.

MANAL ISMAIL, GAC CHAIR: Así es, gracias. Bueno, esto ya está entonces.

Vi otra pregunta de Susan Payne: "Laureen, ¿de qué manera la imposición de nuevas obligaciones sobre los TLD que no existen todavía tendrá un impacto en aquellos que sí existen? Los TLD que ya tienen un contrato no tendrán incentivo para adoptar disposiciones diferentes, debemos recordar que en volumen la vasta mayoría del uso indebido se da en los TLD heredados, entonces, ¿por qué no se aplica aquí el foco de atención?"

LAUREEN KAPIN: Son puntos válidos la observación de que, el gran volumen del uso indebido y es exacto, se da en los TLD heredados, es así, y es por tamaño no en proporción. Creo que la respuesta a esta pregunta; y digo que estas observaciones son muy válidas, es que, hacemos lo que podemos y cuando podemos.

Los contratos con los TLD heredados en este momento no se están negociando, tenemos esta oportunidad dorada con los nuevos gTLD porque no tienen contrato todavía, está por desarrollarse, entonces es la oportunidad de mejorar esas disposiciones. Ahora, ¿esto tendrá un efecto de derrame sobre los TLD de la primera ronda o con el contrato con .COM? Debo decir que se adoptaron algunas de las medidas de protección en el contrato con .COM, así que, diría que sí que existe este potencial de que se dé un impacto posible, positivo.

Pero tenemos que tomar las oportunidades que se nos presentan, me encantaría realmente que estas disposiciones contra el uso indebido del DNS se dieran para todos los TLD, pero tenemos que ser realistas y aprovechar las oportunidades que tenemos, y a veces el trabajo incremental logra un efecto de cascada. Esa es mi expectativa.

Y este efecto de cascada en mi expectativa es que, logre mejoras en la situación actual y eso viene a través de la nueva ronda de gTLD.

MANAL ISMAIL, GAC CHAIR: Muchas gracias, Laureen, y disculpas si pasé por alto alguna pregunta. Espero a determinar si hay más preguntas, mientras tanto, quiero agradecer por el vínculo a la encuesta en el chat, lo considero muy interesante e informativo. Quería saber si hay alguna pregunta sobre soluciones posibles, aquellos que expresaron su insatisfacción me pregunto si expresaron también alguna solución posible.

LAURIN WEISSINGER: Muchas gracias. Está por venir el MAAWG con la colaboración del PSWG, va a trabajar en el análisis de soluciones posibles, incluyendo a otras partes interesadas. Así que tendremos que volver con esa respuesta a finales de este año con un segundo documento.

Hemos recopilado los datos como primera etapa, luego veremos la política, haremos una observación de lo que dicen los datos y las preguntas nos dan cierta información, pero el reporte es distinto, el reporte de las preguntas es algo diferente de encontrar soluciones. Esperemos darlo para finales de año.

MANAL ISMAIL, GAC CHAIR: Muchas gracias, Laurin y gracias a los otros oradores. El PSWG de Japón, del MAAWG, una sesión muy informativa y con esto concluye nuestra sesión de discusión de medidas de mitigación del uso indebido, les pedimos a los miembros del GAC que permanezcan en la sala porque vamos a aprovechar estos minutos que nos quedan para hacer una revisión muy rápida de la redacción del comunicado.

Muchas gracias a todos y por favor háganme saber cuándo podemos comenzar con esta rápida discusión del comunicado.

GULTEN TEPE: Voy a pedir pongamos a Benedetta también como anfitriona. Gracias, Manal.

[FIN DE LA TRANSCRIPCIÓN]