ICANN85 Mumbai | Foro de la comunidad – GAC: debate sobre la mitigación del uso indebido del DNS
Lunes, 9 de marzo de 2026 – 16:30 a 17:30 IST

JULIA CHARVOLEN: Bienvenidos a la sesión del GAC sobre mitigación del uso indebido del DNS el lunes 9 a las 16:30 hora local. Esta sesión está siendo grabada y se rige por los estándares de comportamiento esperados, el código de conducta para los participantes en la comunidad de la ICANN y la política anti acoso de la ICANN. Por favor, digan su nombre para los registros y el idioma en el que va a hablar si hablan en un idioma que no sea el inglés. Hablen con claridad y a una velocidad razonable para permitir una interpretación correcta y, por favor, asegúrense de silenciar el resto de los dispositivos cuando se hace uso de la palabra. Le damos la palabra al presidente del GAC: Nico Caballero.

NICOLAS CABALLERO: Gracias, Julia. Bienvenidos a todos. Bienvenidos a la sesión del GAC sobre la mitigación del uso indebido del DNS. La verdad que tenemos acá unos oradores espectaculares porque tenemos a Martina Barbero, de la Comisión Europea; a Tomo Miyamoto, a mi derecha; Gabriel Andrews, del gobierno de Estados Unidos; y también el copresidente del Grupo de Trabajo de Seguridad Pública; y obviamente, Susan Chalmers, del Gobierno de los Estados Unidos. Y hoy tenemos dos oradores invitados que son

Devesh Tyagi, espero haber pronunciado bien el apellido, de los administradores ccTLD .in; y Manju Chen, de Trust Notifier Network. Tenemos una hora y espero que sea suficiente para también tener una mini sesión de preguntas y respuestas al final de las presentaciones. La idea es que sea un intercambio con todos ustedes e interactivo. Le doy la palabra a Susan.

SUSAN CHALMERS; Representante de Estados Unidos y, además, soy una de las corresponsables del tema de uso indebido del DNS junto con mis colegas de Japón y de la Comisión Europea. Esta es la sesión de GAC sobre uso indebido del Dans, que es un tema prioritario para el GAC, porque hay un gran impacto de lo que pueden ser ataques de phishing, malware y el Comité Asesor Gubernamental en su plan anual, bueno, se concentra en dos áreas de trabajo.

Tenemos el primero, que es hacer un seguimiento del trabajo que haga la política de la ICANN sobre el uso indebido del DNS antes de seguir delegando nuevos nombres de dominio, y tenemos también un área de trabajo de generación de capacidades, donde esto sirve para generar capacidad sobre el tema específico a los miembros del GAC. El uso indebido del DNS habla de actividades maliciosas que la mayor parte de los gobiernos considerarían ciberdelitos, por ejemplo, phishing, malware, botnet. Pero hay una definición muy específica en ICANN, porque uso debido del DNS en ICANN significa malware, botnet, phishing, pharming y el spam cuando se utiliza el

spam como un mecanismo de entrega de alguna de las otras cuatro categorías mencionadas.

Hay tres partes que tienen que ver con el servicio de nombres de dominio y que pueden ejecutar distintos tipos de ataques. Por ejemplo, tenemos los proveedores de internet, también los que brindan servicios de hosting, y en el GAC nos estamos centrando en el sistema de identificadores únicos y su seguridad y estabilidad, incluso el DNS. Eso es lo que estamos concentrando para las políticas, sobre todo los registros y los registradores que tienen un contrato firmado con la ICANN.

Estas partes contratadas pueden tomar medidas proactivamente para proteger a los nombres de dominios de que sean utilizados por actores maliciosos. En términos generales, los registros y registradores de gTLD deben responder a los usos indebidos del DNS. El Departamento de Cumplimiento de la ICANN es quien ejecuta y hace valer estas obligaciones contractuales. Y yo creo que son dos caras de la misma moneda. Siguiente imagen, por favor.

Estas obligaciones de uso indebido del DNS fueron establecidas específicamente por unas enmiendas a los contratos firmados entre ICANN y los registros y registrados de nombres de dominio en 2024. Acá tenemos un poco de historia, aunque no todas, y voy a hacer una pausa. ¿Hay algún…? Yo sé que tenemos 19, me parece, representantes nuevos ante el GAC. No sé si hay alguno de ellos presente en la sala. No tienen por qué ser tímidos.

NICOLAS CABALLERO: Los nuevos representantes ante el GAC, por favor, levanten la mano.

SUSAN CHALMERS: Bienvenidos. Ah, bueno, qué interesante. Bueno, quiero darles una... Quiero decirles algo, que es que, en general, hay documentos informativos que se distribuyen antes de la sesión y el personal de apoyo trata de poner todo lo que puede ser el historial, en este caso de uso indebido del DNS, en tan solo 15 páginas, y ahí pueden tener una idea general de cuál es la historia que tenemos con este tema. Pero acá tenemos nada más que los hitos, más allá de la enmienda del contrato y para los fines del GAC, uno de los hitos para nosotros en nuestro asesoramiento de la ICANN83, en Praga, que no lo voy a leer porque está en la pantalla, pero esto es lo que presentó el GAC el año pasado en Praga. Y más recientemente, y yo diría que, para nuestro beneplácito, se adoptó una nueva carta orgánica del PDP para lo que es la verificación de nombres de dominio asociados. Hay una parte de este programa donde mis colegas van a hablar de las actividades en curso en este PDP de ADC.

En lo que hace al programa, si podemos pasar a la agenda, antes y después de lo que está sucediendo en la ICANN, nosotros tuvimos el placer de recibir dos presentaciones diferentes que eran para entender distintos esfuerzos de política y operativos que no estaban dentro de la ICANN. Los colegas de India, de NIXI, quienes administran el ccTLD .IN, van a hacer una presentación para ver

cómo ellos manejan el tema de evitar el uso indebido. Y en la última sesión, en Dublín, durante la ICANN84, recibimos una presentación de Trusting Notifier Network, esta red de notificadores confiables. Y esto tiene que ver también con la generación de capacidades en el plan anual del GAC.

Esta red no sucede dentro de la ICANN, pero TNN, Trusting Notifier Network, es más que un programa. Y vamos a escuchar entonces hablar de lo que es la política y estructura a través de Manju Chen. Pero, sin más, le voy a dar entonces la palabra a Devesh Tyagi, de NIXI, que son los administradores del .IN. Le doy la palabra.

DEVESH TYAGI: Buenas tardes a todos. Nosotros hemos estado operando este ccTLD desde 2012. Nosotros hemos tomado algunas iniciativas que queremos compartir con ustedes y estas iniciativas se basan en las experiencias reales que hemos tenido con NIXI. Siguiente, por favor. Estas son las iniciativas que estamos implementando, que tienen que ver con la verificación de la clave de nombre del dominio, verificación de WHOIS, y también estamos haciendo la incorporación de las autoridades encargadas de aplicación de la ley indias, porque hubo ciertas conversaciones y recibimos varias sugerencias. Si bien a través de esas sugerencias lo que hicimos fue incorporar muchas de ellas para poder mitigar el uso indebido del DNS que estábamos observando.

Entonces, en primer lugar, empezamos con la verificación de los extranjeros que estaban incorporándose a nuestro registro .in.

Entonces, para poner esto en práctica, el registro .in verifica a los registratarios que utilizan documentos como puede ser el pasaporte o el documento nacional de identidad y otra identificación pertinente. Además, también, como tenemos un nuevo acuerdo de acreditación de registro, tenemos ahí una cláusula nueva, que es la 4.415, donde los solicitantes extranjeros que solicitan un dominio .in deben demostrar una conexión comercial legítima o un objetivo legítimo en India.

Estos son también algunos de los desafíos que nosotros enfrentamos con los dominios. Para estas otras iniciativas que estamos poniendo en la práctica y empezamos a hacerlo desde octubre del 2023, lo que hacemos es monitorear la registración de dominios. Para esto, hacemos un monitoreo mejorado, implementando medidas como pueden ser limitar palabras claves como pueden ser GOV, NIC, Bharat, para evitar el uso indebido de ellas. Vimos que el uso indebido también tenía que ver con nuevas iniciativas del gobierno y también en nombre de departamentos o ministerios del gobierno. Entonces, pusimos todos estos nombres en nuestra lista de monitoreo.

Cuando se registran estos dominios, entonces, en esos casos, hacemos una verificación de todos estos nombres de dominio. Desde mayo del 2024, implementamos un mecanismo en tiempo real para señalar registraciones de dominios en bloque que realizan los delincuentes repetitivamente utilizando correo electrónico indebidamente. Entonces, cuando tenemos un número de teléfono móvil, que es lo que sucede en los últimos años, así

como otros pedidos que pueden venir de un número móvil, entonces el sistema inmediatamente lo señala como para hacer una verificación adicional. Otra iniciativa tiene que ver con la verificación manual de los detalles de WHOIS y del nombre de dominio, porque nosotros sabemos que a veces tenemos dos registraciones diferentes dentro del WHOIS y a veces hay una representación que se da mal en esos campos.

No podemos tener todo, entonces empezamos a hacer una verificación manual cuando tenemos nombres de dominios sospechosos. Otra cosa que estamos haciendo es actuar sobre la lista de nombres de dominios recibidos de determinadas agencias como pueden ser CERT-in o el Centro de Coordinación de Ciberdelitos Indios y otras autoridades de aplicación de la ley. En la consulta que hicimos con ellos, también vimos que hay algunas listas reservadas y se encontró que se estaba generando un uso indebido a través de ellas. Y es por eso que están también en la lista de reserva y también las señalamos en tiempo real para nosotros. Siguiente imagen.

Entonces, el monitoreo periódico de las registraciones de dominio se da desde octubre del 2023, donde ahí entonces establecimos mecanismos de monitoreo periódico que verifican los dominios registrados diariamente y se verifican de manera sistemática. Esto tiene que ver con los ciberdelitos, actividades de phishing y un potencial daño a la reputación. También, debido a lo que nos dijeron tanto NIXI como MET IT y las autoridades encargadas de la aplicación de la ley, tenemos algunas cosas como puede ser

Reserve Banco India, o como dije yo, lugares donde puede haber registraciones que quieren tener el nombre del gobierno o pretenden tener el nombre del gobierno entre ellos.

Entonces, se señala cuáles son los contenidos, hay una alerta de esos contenidos, para ver cuál puede ser la amenaza potencial y se hace un informe a la institución en cuestión y también al centro de coordinación de ciberdelitos. También incluimos todos los dominios con palabras clave vinculadas con RBI y CBI porque muchos de ellos pueden ser utilizados para uso indebido.

Este es el mecanismo de implementación que estamos utilizando en tiempo real para obtener los números de móviles y las direcciones de email. Se utilizan los móviles y los mails para identificarlos y señalarlos en tiempo real. Entonces, a través de estas iniciativas, quiero compartir con ustedes las estadísticas para que vean cuáles son los números asociados con la prevención de actividades maliciosas. Las notificaciones de amenaza se reciben de los organismos de aplicación de la ley, del Centro de Coordinación del Ciberdelito de la India, CERT-In, y una verificación manual de eKYC y de CYC. Y a través de estas estadísticas en el 2024, estábamos recibiendo 78 notificaciones, pero en el 2025 esto se redujo a 23. Y ahora recibimos en el 2026 solamente uno. Entonces, la iniciativa está siendo exitosa.

A través del Centro de Coordinación de Ciberdelito de la India, que es uno de los principales en el país, vemos que ocurrió en el 2023, 2024, 2025, 2026, fue descendiendo la cantidad de 131, 211, 17 a 0

en este momento. También quisiera decir que teníamos 506 en el 2024 de las notificaciones de amenazas informadas por CERT-In que bajó a 177 en el 2025 y este año recibimos siete notificaciones. Entonces, ustedes pueden observar la cantidad de incidencias que se ha ido reduciendo a lo largo del tiempo.

Esta es una iniciativa importante que estamos implementando utilizando KYC manual y ahora KYC electrónica. Vemos que aproximadamente se registran unos 3.000 dominios por día, y a través de este proceso de verificación vemos que el 4% son los dominios que pudimos identificar como maliciosos. Y una vez que los ponemos en espera para demostrar si son realmente amenazas, solamente podemos hacer la verificación para un 4%, entonces pueden ver que el 96% de los dominios pueden haber sido creados para un uso indebido, pero todo esto se ha podido mitigar por nosotros. Estos son los números, aquí están las cifras, ustedes lo pueden ver por sí mismos. Y a través de esta iniciativa, en este momento estamos en el número de serie 58 y hemos avanzado muy bien. Tenemos este número de serie 58 de 4 millones de dominio, hemos identificado 2.276 como dominios con fines maliciosos, así que realmente hemos logrado un gran progreso.

Una vez más, comparto con ustedes que tenemos el acuerdo de acreditación de registradores y que hemos instruido a todos los registradores, incluso a los internacionales, que implementen requisitos obligatorios KYC. También se colabora con los organismos de aplicación de la ley durante los eventos internacionales principales, ocasiones sensibles, para asegurarse

de que haya una preparación de ciberseguridad. También desarrollamos procedimientos operativos estándar y buenas prácticas para .IN como registro y las presentamos a I4C. Con estas iniciativas hemos tenido muy buenos resultados.

El nuevo acuerdo de acreditación de registradores ha hecho que nuestro dominio .in sea más seguro, y vemos que tenemos la obligatoriedad de utilizar eKYC para todos los registratario, se mantienen los registros de transacciones financieras, el IP lo hacen los registradores, se establece un responsable de reclamaciones en cada registrador y también hay un representante local con una oficina registrada en India. Entonces, con todas estas medidas hemos podido mitigar la posibilidad de que se registren dominios con fines maliciosos. Quisiera compartir ahora los resultados también.

Incluso el alto tribunal de Delhi ha visto los beneficios de este proceso de verificación que hemos implementado con eKYC y ha dicho el honorable tribunal que esto ha aumentado la transparencia porque hay un proceso estructurado, implementado por NIXI y realmente esto es beneficioso para todos. Los organismos encargados de la aplicación de la ley de la India también valoran el apoyo que ofrece NIXI para poder frenar el ciberdelito en el país. Esto es lo que yo quería compartir con ustedes y les agradezco por la oportunidad de hablarles.

NICOLAS CABALLERO: Muchísimas gracias, Devesh. Tenemos tres a cinco minutos para preguntas. Por cuestiones de tiempo, le vamos a dar la prioridad a los gobiernos, y si no hay preguntas de los representantes de los gobiernos, podemos darles la posibilidad a otros participantes a hacer sus preguntas. Bueno, no veo ninguna mano en Zoom. Vamos a ver si hay preguntas aquí en la sala para el señor Devesh. Adelante.

ORADOR NO IDENTIFICADO: Soy representante de un registrador. Quería saber qué es lo que quieren decir cuando hablan de informes de amenazas.

DEVESH TYAGI: Informes de amenazas, básicamente, tienen que ver con que los organismos de aplicación de la ley con sus propias herramientas analizan los dominios en forma diaria. Los registros de .in comparten todos los dominios creados a todos los organismos de aplicación de la ley en el país y a través de esta herramienta analizan estos dominios creados y nos brindan un informe de amenazas.

NICOLAS CABALLERO: Gracias. Tengo al Taipei Chino.

PEI YING: Yo también trabajo con TwNIC, y quería pedirle que compartiera más su experiencia con respecto a las medidas que han

implementado, si son parte de las leyes nacionales o si son voluntarias para que las cumplan las organizaciones.

DEVESH TYAGU: Estamos, por supuesto, más que gustosos de compartir nuestras experiencias con ustedes. Nosotros nos guiamos por la legislación India, pero también por otras iniciativas, porque en años anteriores simplemente respondíamos a las amenazas. Ahora tratamos de hacer algo preventivo antes de que se produzcan las amenazas. Entonces, estos resultados que les compartí de los 3.000 dominios registrados, hemos identificado 4% como los maliciosos y un 4% de estos, solamente ese porcentaje puede justificar que un análisis más detallado de esas actividades.

NICOLAS CABALLERO: Bueno, gracias. Vamos a ver si hay alguna pregunta más. Recuerden que vamos a darle prioridad a los representantes de los gobiernos para que hagan sus preguntas primero.

BANGLADESH: Gracias. Soy representante de Bangladesh, del GAC. Tienen una muy buena iniciativa en India con el análisis de las amenazas dentro de la India. Ustedes obtienen información sobre el uso indebido del DNS y están tomando algunas medidas. ¿Qué pasa con el uso indebido del DNS por parte de registros que están más allá del .in? ¿Reciben también informes en forma periódica sobre ellos? ¿Y qué es lo que hacen? ¿Qué medidas toman?

DEVESH TYAGI: Hoy solamente estamos hablando estas modalidades con los niveles más altos. Estamos trabajando para mitigar también esas situaciones.

NICOLAS CABALLERO: Gracias, Bangladesh, por la pregunta. Veo una mano allí. Podemos tomar una pregunta más. Adelante.

MELANIE ALDONCE: Soy de Chile, para que conste los registros- Muchísimas gracias, Dr. Devesh, por su presentación. Quisiera consultarle si analizan dominios que están registrados, pero no activados de inmediato; es decir, que no se asignan a un host, porque se sabe que muchos de los dominios que terminan haciendo uso indebido están registrados y permanecen inactivos durante mucho tiempo. Gracias.

DEVESH TYAGI: Es una pregunta muy clara la que me está haciendo, estamos muy al tanto de esta situación. Hoy compartí un proceso y este proceso se ha automatizado. Todos los meses tenemos, con la herramienta que hemos creado, la posibilidad de ejecutar esa herramienta para analizar todos los dominios que tiene el registro, y se genera un informe que también se comparte con los organismos de aplicación de la ley, porque sabemos que hay algunos dominios que pueden volverse activos después de un tiempo. Entonces,

todos los días o todos los meses analizamos estos dominios que se han creado utilizando herramientas automatizadas, los identificamos y los reportamos a los organismos de la aplicación de la ley.

NICOLAS CABALLERO: Muchas gracias. Julia.

JULIA CHARVOLEN: No tengo una pregunta, pero sí voy a leer una pregunta del chat de Jorge Cancio, el vicepresidente: ¿Cuántos registradores están comercializando el ccTLD .in? ¿Y ven registraciones maliciosas relacionadas con una amplia gama de registradores o solo de unos pocos?

DEVESH TYAGI: ¿Puede repetir, por favor?

JULIA CHARVOLEN: Tal vez lei muy rápido. ¿Cuántos registradoes están comercializando el ccTLD .in? ¿Y observan registraciones maliciosas relacionadas con una amplia gama de registradores o solo de unos pocos?

DEVESH TYAGI: Básicamente, cada registrador está teniendo algunas actividades a través de los dominios que se registran a través de ellos. Entonces,

para los registradores extranjeros, vemos cuál es la filiación con .in. Y para todos los demás registradores indios, no vamos a esos detalles. Cada vez que hay una registración con un registratario, un registrador de la India, y ellos utilizan su dominio en particular con KYC, que es el requisito que habíamos establecido.

NICOLAS CABALLERO: Muy bien, continuamos. Y en este momento le voy a dar la palabra a Martina Barbero, de la Comisión Europea, y a Gabe Andrews, del FBI, quienes nos van a presentar un informe sobre los debates de política del uso indebido al DNS. Adelante, Martina.

MARTINA BARBERO: Les mando saludos desde Bruselas. Lamento no estar para ustedes. En la próxima ronda, tanto Gabriel como yo vamos a hablar de qué es lo que estamos haciendo en las deliberaciones de PDP. Siguiente imagen, por favor. Desde que se lanzó el PDP, como indicó Susan en la parte de introducción de esta sesión, empezamos a formalizar la forma en la que trabaja el GAC, estableciendo un grupo reducido específico para el uso indebido del DNS, que es la forma en la que nos preparamos para las deliberaciones del PDP. Las ideas para formalizar este grupo también seguían todo lo que tenía que ver con los datos de registración, para ver si había alguna falsificación, y nosotros lo hacemos de manera periódica también con los representantes del PDP del GAC, tanto Gabriel como yo llevamos esta posición al PDP. Y va a haber muchísimo trabajo con este PDP sobre el uso indebido

del DNS y establecimos este grupo que nos pareció una buena idea para ver de qué manera los intereses del GAC podían estar presentes en la discusión, pero no utilizar toda la lista de distribución del GAC, que quizás sería un poco abrumador para algunos.

Entonces, ahora tenemos en el GAC 17 participantes, el grupo, obviamente, está abierto para quienes quieran participar y están interesados en el uso indebidos en el DNS. Si son miembros nuevos y quieren unirse, pueden enviar una nota al equipo de apoyo del GAC diciendo que quieren participar en el grupo. Es bueno ver caras nuevas, así como caras que ya hace más tiempo están trabajando eso. Como mencionó Susan, el lanzamiento del PDP fue decidido por el Consejo de la GNSO en diciembre y la primera reunión del grupo, del PDP, se realizó hace dos días y hoy es la primera vez que se reúne y lo hace acá en la ICANN85. Está el PDP 1 vinculado con las verificaciones de dominios asociados que tiene que ver con el informe presentado el verano pasado; y el segundo PDP habla de las medidas de protección para acceso a las API a los nuevos clientes. Y no sabemos cuándo va a ser iniciado este segundo PDP. Para el primer PDP tenemos una delegación que tiene dos miembros completos del GAC, que somos quien les habla y Gabriel, que viene de la Comisión Europea y del FBI, pero también somos como presidentes del PSWG. Y después también tenemos a Wolfgang, de Alemania, que es un participante. Wolfgang puede intervenir en las discusiones, pero no tiene derecho a votar, él proviene de la policía. Y después también tenemos de la policía en

Grecia, pero en este caso es un suplente, en caso de que no estemos presentes ni Gabriel ni yo. Entonces, en realidad, en este momento actúan como suplentes, entonces no tienen ni voz ni voto. Es un grupo bastante fuerte, tiene muchos participantes que son observadores del GAC y esto realmente resulta muy útil. Las primeras reuniones se realizaron hace dos días atrás y hoy en la siguiente imagen les voy a decir brevemente qué es lo que discutimos en estas dos primeras sesiones.

Bueno, primero, obviamente hubo una reunión de apertura en la ICANN85 y la idea era recibir información sobre los plazos que teníamos para este trabajo. Acá pueden ver que tenemos los principales hitos del plan en este momento. El informe inicial del PDP, esperamos que esté listo para febrero del 2027 y el informe final en septiembre del 2027. Y que después el consejo de la GNSO haga la consideración de este informe entre octubre y noviembre del 2027. Hoy lo que vimos en la tercera reunión es que recibimos la presentación de los expertos del tema sobre cómo hacer las verificaciones de dominios asociados y cuáles pueden ser las mejores prácticas.

Lo más importante que deben mantener presente de esta imagen es que nosotros vamos a tener que dar una contribución temprana, que es el 20 de marzo. La verdad que esto está muy cerca, sobre todo considerando esta reunión y hay que preparar, entonces, preguntas de la carta orgánica. Nosotros tenemos un documento en Google que fue formado por varias personas y vamos a seguir contribuyendo dentro de este grupo reducido para poder cumplir

con los plazos fijados. Ahora le voy a dar la palabra a Gabe, que va a hablar más en detalle de los próximos pasos.

GABRIEL ANDREWS: Gracias. ¿Podemos pasar a la siguiente imagen, por favor? Ah, no, perdón. Para que ustedes sepan, estas son las preguntas que están en la carta orgánica del PDP. Y nosotros tenemos que responder a estas preguntas. Como acaba de decir Martina, tenemos que dar estos comentarios o respuestas el viernes de la semana que viene. Esa es la fecha límite. Este PDP se está moviendo muy rápidamente, y veo que está el presidente del PDP, quien nos exige que vayamos muy rápido. Entonces tenemos que dar respuestas rápidas, pero quiero alertarlos a todos ustedes que estamos anticipando brindar respuestas preliminares la semana que viene. Pero quizás esto no permite un gran periodo de revisión como el que ustedes están acostumbrados; es decir, si están muy interesados en estos temas, como dijo Martina, les pido que sean parte del equipo reducido, porque entonces ayuda también a redactar las respuestas a estas preguntas.

Mirando hacia el futuro, ella señaló que el próximo PDP que nosotros prevemos va a tener que ver con el acceso de API. Algunos quizás se acuerdan que cuando se presentó el informe INFERMAL de la ICANN, que asociaba distintos atributos de la registración de dominios con el uso indebido observado, el utilizo de acceso a través de API tenía una gran correlación a esas amenazas. Es por eso que es muy importante para nosotros. Esperamos realmente

que en ese trabajo podamos participar y haga parte de lo que acabamos de decir.

El GAC también, en sus conversaciones y en documentos pasados, también dio otras ideas para áreas potenciales que podían tener que ver con acotar el alcance del PDP, donde habla de monitoreo proactivo como parte de las medidas preventivas, abordar el tema de la exactitud en los datos de registración, una mayor transparencia en las obligaciones de informes, la política por conceso en el uso indebido del subdominio, porque a veces el subdominio es lo que genera el phishing y entonces, como el dominio puede tener distintos subclientes, este puede ser un problema. Y también mecanismo de coordinación centralizado para lo que tiene que ver con DGA, que es el algoritmo de generación de dominios. Entonces, estos son también algunos temas que mencionaron los miembros del GAC y que los vamos a explorar en el futuro.

NICOLAS CABALLERO: Perdón, antes de pasar al siguiente orador, yo preguntaría si hay alguna respuesta o comentario. Veo que Gema de la Comisión Europea pide la palabra. Adelante.

GEMMA CAROLILLO: Muchísimas gracias, Nico. No quiero tomar mucho tiempo, pero sí, en primer lugar, felicitar a todos nuestros colegas del GAC que realmente están brindando aportes importantes y significativos en este proceso. Realmente creo que empezamos con el pie derecho. Y también quiero señalar, ya que utilizando el beneficio de la

información de los colegas del GAC y también la presencia del presidente del PDP en esta sala, nosotros le pedimos al grupo del PDP que revise los requisitos de la carta orgánica para tratar de reducir el plazo fijado ahí, porque nos parece que un año y medio, que sería el final de este proceso, pero incluso para el informe final, estamos hablando de reuniones semanales y trabajos de preparación. Esto realmente va a necesitar de muchos recursos de varias partes de la comunidad de partes interesadas y los profesionales que participen, y me parece que el alcance de esta cuestión es bastante acotado. Entonces, no hay mucha controversia, sino que hay mucho consenso. Es por eso que instamos a que revisen esta carta orgánica como para reducir el plazo.

Y el otro punto que quiero señalar es que es alentador escuchar de la GNSO que las otras cuestiones de importancia consideradas en nuestro informe van a ser consideradas sobre la base de la metodología y lo que ya presentó Gabriel son realmente prioridades importantes para nosotros.

También quiero señalar en particular el tema que tiene que ver con abordar el tema de la exactitud de los datos de registración y la mayor transparencia en las obligaciones de presentación de informes.

NICOLAS CABALLERO: Gracias, Comisión Europea. Tengo a India ahora.

SUSHIL PAL: Quiero felicitar realmente a las autoridades del GAC por llevar adelante todo eso y también señalar la importancia que tiene esto en otras áreas y que también está en la lista de cuestiones prioritarias. Creo que nosotros nos tenemos que concentrar en las medidas de implementación, porque es muy importante poner en práctica esto en simultaneidad con la validación de los datos de los registratarios cuando se hace la registración. Esto es muy importante y hay que entender que hay algunas inquietudes que también conocen en la GNSO y nosotros también tratamos de hablar sobre este proceso, y además de lo que tiene que ver con el informe del año que viene, pero los ciberdelincuentes en realidad se basan en la anonimidad. Entonces, tenemos que apuntar a eso.

También vimos lo que compartió el señor Tyagi sobre la metodología que ellos utilizan y también como nuestro colega preguntó qué es lo que podemos hacer respecto de los registratarios que están por fuera del dominio. Querría aclarar que hay una obligatoriedad en esto. Estamos hablando de un periodo de 30 días para validación y verificación y ese no es el problema. Quizás nuestro pedido es instar al GAC para que dé un asesoramiento, no para un PDP, pero sí un asesoramiento del GAC a la Junta Directiva para acelerar este proceso y que también esto sea parte del contrato con los registradores por algún medio posible. Gracias.

NICOLAS CABALLERO: Gracias, India. Vamos a avanzar entonces. Creo que ahora le tengo que dar la palabra a Tomori Miyamoto. Él hablar de lo que es la presentación de Trusted Notifier Network junto con Manju Chen. Le doy la palabra, Tomo.

TOMORY MIYAMOTO: Gracias. Vamos a pasar a la siguiente imagen. En primer lugar, acá lo que estamos haciendo es hablar de nuestro plan anual y del comunicado que fue presentado en la ICANN84. Y una de las cosas que proponemos ahí es realizar un PDP, como señaló Martina, y lo otro tiene que ver con la generación de capacidades. La generación de capacidades incluye capacitación para los nuevos miembros del GAC, que están cerca de los 20 en este momento. No solo eso, sino que también hablamos de lo que son las mejores prácticas y que pueden contribuir a mitigar el uso indebido del DNS. Como podemos ver ahí en el 4.7, estamos hablando de darle a los miembros algunos ejemplos. Siguiente imagen, por favor.

Creo que pueden reconocer acá que el alcance del contrato y la autoridad contractual de la ICANN es muy limitado, como ustedes pueden ver acá en la imagen. El casillero verde es lo que representa contratos con la ICANN y es muy limitado. Entonces, la definición del uso indebido del DNC también es otro limitante, porque estamos hablando de botware, malware, spams. Pero ustedes pueden ver que esto abarca un poco más lo que puede ser también una violación en algunos datos que tienen que ver con Japón. Y hay cosas que se pueden hacer por fuera de los contratos de la ICANN.

Siguiente imagen, por favor. Acá le voy a dar la palabra entonces a Manju, que va a hacer la presentación de Trusted Notifiers Network.

MANJU CHEN: Muchas gracias, Tomo. Hola a todos. Soy Manchu Chen, directora de Trusted Notifier Network. Esta es una breve introducción. Tomo ya presentó de qué se trata, así que por cuestiones de tiempo voy a avanzar a la siguiente diapositiva porque quiero dejar tiempo para un intercambio. En Dublín, Edmund y Jo Fan de TWNIC y de .asia, hubo presentaciones, allí se habló de los notificadores confiables, pero nosotros somos diferentes en el sentido de que utilizamos el mismo concepto, pero tenemos la idea de que los acuerdos bilaterales son un poco lentos. Entonces, tenemos una red. Cuando uno se incorpora a la red de notificadores confiables, ya las notificaciones son confiables para todos los que participan en la red y todas las notificaciones que reciben también son de entidades que ya son confiables y no tenemos limitaciones a los ccTLD. Muchos ccTLD en APAC estaban muy interesados y ya están indicando que quieren sumarse. Y hablamos también con muchos registros de gTLD a nivel global y muchos están mostrando un gran interés.

Entonces, una de las principales diferencias entre .asia y TWNIC como iniciativas es que los registros y los registradores ya están mostrándose interesados en sumarse. Cubrimos, o tenemos la intención de cubrir más de 200 TLD. con el interés que estamos

viendo ahora, esto representa por lo menos el 60, que son los dominios actuales, y estamos también recibiendo mucha atención de aquellos que quieren convertirse en notificadores confiables. Pero por el momento nos estamos concentrando en incorporar a los registros y registradores porque, si no tenemos los intermediarios, ¿a quiénes le van a enviar notificaciones? Entonces ese es nuestro foco en este momento.

¿Cuál es el problema? Hay una transferencia de costos que es injusta. Las empresas, las marcas se ven afectadas por ciberataques, ataques de phishing y no tienen el tiempo o el conocimiento para lidiar con ellos, entonces lo tercerizan a alguien que está en el mercado con proveedores de servicios de retiro. Los servicios de retiro para las marcas no tienen la autoridad en realidad de retirar ningún dominio porque no son ni los registros ni los registradores. Entonces, lo que hacen es enviar notificaciones libremente a los intermediarios. Y como es libre, envían tantos como quieren. Se les paga por enviar notificaciones. No se les paga por decir por qué algo está bien, no para aprobar nada.

Entonces, a su vez, los intermediarios están frente a este concepto de responsabilidad social. Si ellos retiran ese dominio según este pedido, a veces tienen que rendir cuentas ante la sociedad civil o a los clientes. Entonces, para reducir todos estos costos hay que hacer criterios y requisitos más estrictos para reducir los costos y nosotros lo que vemos es que esto hace que todos estén desconformes porque es injusto este sistema. Creo que la mayoría de ustedes se pueden sentir identificados con esta situación, están

repletos de ataques a los ciudadanos, sienten que no están haciendo lo suficiente, que habría que trabajar de manera más rápida. Pero bueno, esta es una imagen generada por inteligencia artificial, no pertenece a ningún país en particular, pero los gobiernos también se sienten presionados. Y si no se cubren sus necesidades, sienten que tienen que aprobar nuevas reglamentaciones para lidiar con esto. Por lo tanto, todos se culpan a todos.

Nuestra solución, queremos reducir el costo y el riesgo para los intermediarios de internet para que se sientan más cómodos y más seguros al hacer un retiro de un dominio por pedido. ¿Cómo lo hacemos? Para eso necesitamos mejorar la detección y los retiros. Tenemos que mejorar la calidad y la exactitud de las solicitudes. Entonces, de esta manera se puede desarrollar la competencia necesaria. También hay que involucrar a los gobiernos, porque ustedes son importantes, es por eso que estoy aquí. Les agradezco por invitarnos aquí, pero tenemos que trabajar juntos.

Y también quiero señalar, las políticas de nuestra red apuntan a llevarnos a un proceso que se pueda multiplicar, queremos que todos comenten si están interesados, puedo compartirles la política, el documento de política, y ustedes nos pueden dar su opinión.

Y, por último, en lugar, pero no en importancia, sabemos que esto no solamente ocurre a nivel del Dans, en la ICANN tenemos un alcance muy limitado centrado en el Dans, pero en realidad esto

ocurre en todas partes, y para combatir el uso indebido en el mundo en línea necesitamos la cooperación en todos los niveles de la industria.

Entonces, estos son los objetivos que queremos cumplir, que los notificadores tengan que verificar sus notificaciones antes de enviarlas a la siguiente entidad y luego a los intermediarios. Queremos que los notificadores estén autenticados para que sean confiables. Una vez que consiguen ese estado de confiable, tenemos criterios para establecer eso, pero podemos hablar en mayor detalle cuando tengamos más tiempo. Queremos también reducir el riesgo, los riesgos legales, sobre todo para los intermediarios, para que se sientan más seguros al actuar, al manejar las solicitudes de retiro. Entonces queremos tener un contrato que permita que los intermediarios puedan tener esta seguridad de que pueden actuar. Y para eso tendríamos una cadena de contratos.

Los notificadores confiables tienen que aprobar una serie de requisitos, y sus notificaciones se envían a TNN con determinados criterios que deben cumplirse según la sigla DINA. No es lo que más me gusta, pero es lo que se aplica. Tienen que estar verificados, tienen que estar no automatizados, ser indemnes y exactos. Esta es la descripción que utilizamos. Hay que seguir el proceso debido para verificar las solicitudes, y es por eso que confiamos en esta solicitud y va a haber confianza entre los notificadores y los intermediarios.

En la próxima diapositiva les voy a explicar más. Todas las notificaciones van a estar estandarizadas y codificadas para facilitarle las cosas a todos, para que no tengamos inconvenientes con no contar con evidencias o no saber cuál es la solicitud, y debido a esta cadena de contratos, esta cadena de confianza, los notificadores van a poder verificar esas notificaciones que reciben. En realidad, aquí la intención es invertir la transferencia de costos y les voy a explicar cómo se aplica esto a los organismos de aplicación de la ley. Siguiente.

Los organismos de aplicación de la ley nosotros los vemos desde otra óptica, porque los requisitos para los notificadores confiables podrían ser difíciles de cumplir para estos organismos. Conocemos algunos organismos, tal vez no podamos tener contacto con todos. Entonces, todos los organismos oficiales de aplicación de la ley son considerados notificadores confiables, pero hay que verificar las solicitudes que se reciben de estos organismos. Por cuestiones de tiempo, tal vez no pueda explicarles cómo hacemos la revisión de estas notificaciones, pero hay dos condiciones. Si uno quiere incorporarse, estos organismos de la aplicación de la ley deben reconocer que las notificaciones tienen que seguir las normas de la industria para garantizar la diligencia del procedimiento, y a su vez tienen que dar una condición de indemnes a TNN y a los intermediarios cuando se suman a nuestra organización.

Esto es lo que Tomo ya les describió. Tenemos que involucrar a todos en esta red, pero la ICANN tiene un alcance limitado. Nosotros comenzamos con la ICANN, pero en el futuro esperamos

poder expandirnos a otros actores, al mundo real, a las empresas de telecomunicaciones, las de web, las que se ocupan de nombres, de números y ciberseguridad. Con esto finalizo mi presentación y quedo a disposición para sus preguntas.

NICOLAS CABALLERO: Lamentablemente, no tenemos tiempo para un intercambio. Les pido disculpas, pero pueden ponerse en contacto con Manju y su equipo más adelante directamente. Ahora le quiero dar la palabra a Tomo para algunos comentarios finales relacionados con el comunicado del GAC y algunas sugerencias.

TOMORU MIYAMOTO: Muchas gracias. Quisiera darle ese micrófono tan pronto como sea posible, pero tenemos aquí tres PDP o tres temas para considerar aquí de importancia. El desarrollo de la política de verificación de dominios asociados, el futuro desarrollo de políticas sobre el uso indebido del DNS. Tenemos ya el PDP 1 y ahora un plazo para el PDP 2. Hay otras brechas que se han identificado y también tenemos que considerar las posibilidades para futuras iniciativas y colaboraciones para trabajar en el ámbito del uso individual de ANS. Así que dejo abierto el micrófono para escuchar sus sugerencias. Gracias.

NICOLAS CABALLERO: India ha solicitado la palabra.

SUSHIL PAL: Era un comentario, pero como hay una diapositiva específica sobre el comunicado, Quisiera saber si podemos incluir este aspecto del mecanismo de prevención respecto del periodo para la registración.

SUSAN CHALMERS: Creo que, respecto a esta sugerencia, el PDP actual y los futuros PDP podrían dar cabida a esta sugerencia. Creo que había un punto en el informe de cuestiones al respecto. Se hablaba de una metodología para priorizar distintas áreas para el trabajo futuro. Entonces, tal vez allí podría tener cabida, pero, sin duda, vamos a pasar por un proceso para compartir el texto correspondiente a estos temas de importancia.

SUSHIL PAL: Gracias, Susan. Esto entendemos que se ha mencionado, pero también surgió como una de las cuestiones de importancia antes, por lo menos en otras sesiones de reacción de comunicado, entonces creo que esto es algo que es tangible. Estamos tratando de hacer más expeditivo el proceso de desarrollo de políticas para la verificación de nombres de dominio asociados, resultado que estamos esperando desde hace un año. Esta medida preventiva va a tener un impacto mucho mayor que lo que podríamos tener con el proceso de PDP relacionado con los nombres de dominio asociados. Creo que esta medida preventiva debería transmitirse a

la Junta Directiva como asesoramiento para que encuentren las modificaciones contractuales necesarias a través del medio que haga falta.

NICOLAS CABALLERO: Gracias, India. Lo trataremos en una de las sesiones de redacción de comunicado. Nos hemos quedado sin tiempo. No sé si tienen algún comentario final Susan o los demás oradores.

SUSAN CHALMERS: Desde hace varias reuniones, los responsables de los temas del GAC han invitado a la mayoría de los países que tienen ccTLD a hacer su presentación. Tenemos .rw para Rwanda, como lo vimos en Kigali y ahora en este caso, pero para quienes son nuevos en este tema hay un proceso de política de ccTLD y también tenemos el espacio gTLD, que son muy diferentes y muy exclusivos en la ICANN. Hay un proceso de múltiples partes interesadas que puede obtener información a partir de las prácticas nacionales, pero son procesos singulares, separados, y al final de cuentas se necesita el consenso de la comunidad y de todos los involucrados. Quería resaltar que, para quienes son nuevos, estos son dos espacios de política separados. Eso es todo lo que quería decir y les quiero agradecer a todos por su participación en este proceso.

NICOLAS CABALLERO: Gracias, Estados Unidos. India, ¿volvió a pedir la palabra? Muy bien, doy por finalizada la sesión. Muchas gracias Devesh, Gabe, Manju,

Tomo y Susan, por supuesto. Muchas gracias a todos. Nos volvemos a ver mañana a las 9:00 AM para la reunión con el ALAC. Muchas gracias. Disfruten de la merienda, los tragos o la cena. Gracias.

[FIN DE LA TRANSCRIPCIÓN]