ICANN81 | Reunión General Anual – Debate del GAC sobre la mitigación del uso indebido del DNS
Martes, 12 de noviembre de 2024 – 10:30 a 12:00 TRT

NICOLÁS CABALLERO: Señoras y señores, vamos a comenzar. Por favor, tomen asiento.

DANIEL GLUCK: Hola y bienvenidos a esta reunión el jueves, 12 de noviembre a las 7:30 UTC. Yo soy Dan Gluck, del equipo de apoyo para el desarrollo de políticas de la ICANN. Tengan en cuenta que esta sesión está siendo grabada y se rige por los estándares de comportamiento esperado de la ICANN y la política antiacoso de la ICANN. Durante la sesión solo se leerán en voz alta las preguntas y comentarios si se presentan en la ventana del chat.

La interpretación para esta sesión incluye los seis idiomas de Naciones Unidas más portugués. Si desean tomar la palabra durante la sesión, por favor levanten la mano en la sala de Zoom, indiquen su nombre, el idioma en el que van a hablar si es que no lo hacen en inglés y recuerden hablar a un ritmo razonable. Les recuerdo que hay mesas con micrófonos reservadas para los miembros del GAC, observadores e invitados. Ahora le doy la palabra al presidente del GAC, Nico Caballero.

NICOLÁS CABALLERO: Muchas gracias. Bienvenidos todos a la sesión sobre mitigación de uso indebido del DNS. Es un privilegio para nosotros tener a los responsables de áreas temáticas: Martina Barbero, de la Comisión Europea, Owen Fletcher, del gobierno de Estados Unidos, y Hajime Onga, de Japón. Espero estar pronunciando bien los nombres. También es un honor para nosotros tener a Mahmut Esat Yildirim, de la Autoridad TIC de Turquía, a Leticia Castillo, del equipo de cumplimiento contractual de la ICANN, Reg Levy, de Tucows, y Dennis Tan, de VeriSign, y Jeff Bedser, de CleanDNS.

Bienvenidos a todos. Sin más y por una cuestión de tiempo le voy a dar la palabra directamente al señor Hajime Onga, de Japón, quien nos va a explicar los detalles y matices de nuestras conversaciones para el día de hoy. Adelante.

HAJIME ONGA: Soy el nuevo representante del GAC de Japón. Esta sesión es una sesión con la Comisión Europea, Estados Unidos y Japón. Tendremos como invitados a miembros distinguidos del gobierno de Turquía, de la ICANN, de SSAC y de la Cámara de Partes Contratadas.

Esta es la agenda para el día de hoy. Después de esta breve introducción tendremos una presentación a cargo del país anfitrión. Luego el equipo de la ICANN nos dará una actualización sobre uso indebido del DNS después de la implementación del acuerdo de acreditación con los registradores y del acuerdo con los registros, RAA y RA. Luego tendremos una mesa redonda con Tucows, VeriSign y KINDNS. Luego tenemos un debate del GAC. Finalmente hablaremos

acerca de los próximos pasos hacia la reunión ICANN82 que tendrá lugar en Seattle. Hablaremos acerca del comunicado.

En primer lugar, la mitigación del uso indebido del DNS es un tema prioritario para el GAC. En Japón este problema atrajo mucha atención debido al phishing según lo que se define en los contratos de la ICANN para [inaudible] la piratería en el sentido más amplio. En segundo lugar, en función de los RA y los RAA actualizados, los registros y los registradores de TLD deben abordar el informe sobre uso indebido del DNS como obligación contractual.

En tercer lugar, en este acuerdo contractual se define el uso indebido del DNS como malware, botnets, phishing, pharming y en algunos casos también spam. Esta vez hablaremos acerca de las medidas que se están tomando, principalmente dentro del alcance del ámbito de la ICANN. En la próxima reunión hablaremos acerca del ecosistema en su totalidad. La siguiente diapositiva, por favor.

Aquí tenemos una descripción del alcance de la ICANN y de la mitigación del uso indebido del DNS. Ese rectángulo verde es la autoridad contractual de la ICANN como los RA y los RAA. Vemos que esa autoridad está limitada. Esta es una relación entre la ICANN, los registros y los registradores.

Tenemos distintos actores. Los registratarios y los registros de los gTLD que no están aquí. Hoy hablaremos acerca de la relación, el impacto y el efecto sobre este rectángulo verde. De hecho, las partes interesadas relacionadas con el uso indebido del DNS son más amplias que lo que vemos aquí. Tenemos muchos casos de uso indebido del DNS. Este

tema de uso indebido del DNS prevalece en la industria del DNS, que es el rectángulo azul. Además, hay personas que usan servicios como proveedores de hosting, CDN, que están representados en el rectángulo rojo.

Para mitigar el uso indebido del DNS tenemos que trabajar juntos en forma colaborativa. El mes pasado organizamos un seminario web, con Jeff, que va a estar hoy en el panel, donde hablamos acerca de SAC115 que se ocupa de las referencias más importantes en relación con los RA y los RAA actualizados. En la presentación, Jeff mencionó una serie de temas acerca del marco para la mitigación del uso indebido del DNS. Subrayó la importancia de la cooperación entre la comunidad del DNS más extendida. Hoy, en nuestra sesión, cubriremos los temas que vemos aquí, en este rectángulo rojo.

En primer lugar las autoridades de comunicación e información de Turquía hablarán acerca del abordaje que utilizan para el uso indebido del DNS. En el comunicado de Kigali se habló acerca de la importancia de considerar el uso indebido del DNS y tomar medidas adicionales. En esta presentación hablaremos acerca de las iniciativas turcas, incluida la cooperación con los administradores de ccTLD y otras organizaciones pertinentes. Perdón, la diapositiva anterior.

También hablaremos acerca de qué podemos hacer dentro de la ICANN. Hablaremos acerca de RA, el cumplimiento efectivo. Tenemos también un panel con las partes interesadas donde hablaremos acerca del efecto importante de los dominios públicos. Finalmente tendremos un debate en el GAC acerca de lo que podemos hacer con respecto a

este tema. Luego, en ICANN, hablaremos acerca de lo que podemos hacer en la comunidad más amplia o en el ecosistema.

Para finalizar, en la sesión de hoy hablaremos brevemente acerca de los próximos pasos luego de la reunión de la ICANN. Ustedes pueden ver que la agenda para el día de hoy es muy nutrida. Esperemos que todos respeten bien sus tiempos como los japoneses. Yo no soy un muy buen ejemplo hoy porque me estoy extendiendo un poco. Comencemos con la primera parte, que estará a cargo del país anfitrión. El señor Mahmut Esat Yildirim.

MAHMUT ESAT YILDIRIM: Muchas gracias. Hola a todos. Soy Mahmut Esat Yildirim. Encabezo el departamento de tecnologías de la comunicación y la información de Turquía. Voy a hablar acerca de los mecanismos de mitigación del uso indebido que estamos desarrollando en Turquía y en el ccTLD. Creo que están avanzando demasiado rápido. Pasemos a la siguiente, por favor.

NICOLÁS CABALLERO: Mahmut, ¿podría acercarse un poco al micrófono, por favor? Muchas gracias.

MAHMUT ESAT YILDIRIM: El CERT nacional turco y el ccTLD de Turquía están en el mismo departamento. TR-CERT es el centro de seguridad cibernética nacional. Su función principal es reconocer y mitigar las amenazas cibernéticas.

Como mencioné, trabajamos junto con el ccTLD, que es trABIS, y que forma parte del mismo departamento. Por eso podemos combinar dos facultades al mismo tiempo para combatir el uso indebido del DNS y otras amenazas cibernéticas.

Tenemos estrategias de seguridad cibernética a nivel nacional y también planes de acción. De hecho, tenemos cuatro. En estos planes hay algunos puntos en particular que apuntan a detectar los mecanismos de uso indebido y las amenazas cibernéticas. La última versión del plan de acción y estrategia de seguridad cibernética nacional tiene cuatro temas, seis objetivos estratégicos, 18 objetivos y 61 planes de acción.

Estos puntos están centrados en los seres humanos. Es un abordaje para la seguridad cibernética. Es la contribución a la seguridad cibernética. Defensa cibernética, disuasión, tecnologías nacionales para combatir las amenazas cibernéticas y, finalmente, la marca de Turquía en el área internacional. Todo esto forma parte de nuestra estrategia de seguridad nacional y nuestro plan de acción.

La base legal para mitigar las amenazas cibernéticas y el uso indebido del DNS se implementan de acuerdo con las cláusulas establecidas en los artículos de la Ley de comunicación de Turquía, la ley número 5809. En el artículo 60 sección 11 dice que la organización se encarga de tomar o de pedirle a alguien que tome todas las medidas necesarias para proteger y disuadir ataques cibernéticos a las organizaciones gubernamentales privadas y entidades reales. Como podrán ver, hay muchas responsabilidades que cubre el CERT nacional de Turquía para

tomar medidas contra las amenazas cibernéticas. La siguiente, por favor.

En el próximo párrafo o sección de la misma ley dice: “La organización puede recibir y evaluar información, documentos, datos y registros de lugares pertinentes dentro de su jurisdicción”. Con esta ley también podemos pedir datos e información para detectar ataques cibernéticos y podemos pedir estos datos a diferentes organizaciones o sistemas. La siguiente, por favor.

El fundamento legal de los ccTLD está dentro del marco de las reglamentaciones legales. El ccTLD .TR apoya el cumplimiento legal efectivo para combatir los delitos cibernéticos implementando medidas técnicas. Trabaja con las autoridades de aplicación de la ley, con los tribunales. Brindamos la información y los documentos solicitados por las autoridades. A veces también trabajamos en estrecho contacto con CERT y con las autoridades de aplicación de la ley en forma conjunta para detectar y disuadir estas actividades de uso indebido. La siguiente diapositiva, por favor.

¿Qué clase de actividades de uso indebido vemos todos los días? Phishing, distribución de malware, spam, secuestro de dominios, comando y control de botnets, materiales de explotación infantil, fraude, uso indebido del DNS, técnico como por ejemplo spoofing y hijacking del DNS. A veces violaciones de la privacidad.

Estamos tratando de detectar y disuadir todas estas categorías de uso indebido. Estamos utilizando determinadas herramientas y mecanismos para detectarlas. La primera de estas herramientas que

desarrollamos se denomina AZAD. Es un software que desarrollamos que utiliza el mecanismo de aprendizaje automático y de inteligencia artificial para detectar nombres de dominio de phishing. Por ejemplo, estamos recopilando todos los feeds de dominios recientemente generados. También otros feeds de otras fuentes. Estamos recopilando millones de nombres de dominio cada día utilizando la inteligencia artificial y el aprendizaje automático podemos reunir información sobre todos los nombres de dominio relacionados con el phishing, identificarlos entre todos estos millones de nombres de dominio. Hay operadores en el ccTLD que de esta forma pueden verificar en forma manual si ese nombre de dominio relacionado con phishing es realmente phishing.

Hasta el momento, este software ha tenido éxito en un [97%]. De esta forma se pueden detectar las direcciones de phishing y se las puede bloquear antes de que sean activas o en cuanto comienzan a trabajar activamente. Utilizamos toda esta potencia de CERT y de ccTLD para trabajar junto con los ISP de Turquía también de forma tal que podamos actuar muy rápidamente y mitigar estas actividades de phishing. Todos estos feeds, todos estos reclamos relacionados con uso indebido, se reúnen en un software especial que desarrollamos. Ahí recopilamos todas las notificaciones y las clasificamos en diferentes categorías.

Esta es la forma en que fluye el uso indebido en trABIS en general. Recibimos notificaciones de diferentes fuentes como los registratarios, los registros, los usuarios finales o AZAD. Recopilamos todas las notificaciones en una aplicación y luego enviamos esto a trABIS, que es

ccTLD. Allí se analizan todas las notificaciones utilizando inteligencia artificial y otras herramientas. De esa forma luego pueden suspender un nombre de dominio o pueden escalarlo y llevarlo a los ISP.

Tenemos algunos datos estadísticos con respecto a incidentes. Recibimos más de 13.000 reclamos. De estos 13.000 reclamos 8.000 fueron realmente incidentes. Esto significa que debimos verificar estas notificaciones para ver si eran actividades abusivas o no. De estos 8.000, 5.000 fueron de hecho actividades de uso indebido. En esos casos se canceló o se bloqueó el dominio. La siguiente, por favor.

Hasta ahora encontramos más de 900 sitios web de phishing, más de 300 eran bancarios, 3 centros de comando y control de malware y 26 nombres de malware. Todos estos los detectamos utilizando la herramienta con inteligencia artificial que desarrollamos nosotros. Hay algunos patrones comunes en la lista de nombres restringidos. En inglés quizá no tenga sentido pero hay implicancias de reclamos que utilizan préstamos en Turquía y que se utilizan para identificar robos. La cantidad de palabras que contienen el término banco o bancario no excede las 20. Utilizamos los nombres de bancos oficiales, los incluimos en las listas de nombres de dominios restringidos para que los actores ilegales no puedan registrar nombres de dominio que contengan términos bancarios. La siguiente, por favor.

En Turquía oportunidad, campaña, confianza. Estas palabras son palabras que se utilizan mucho en las actividades de phishing o en actividades relacionadas con uso indebido. Una vez más, quizá en inglés no tenga sentido para algunos de ustedes pero nosotros estamos creando y mejorando los mecanismos de inteligencia artificial

ampliando esta serie de palabras y todos los días le enseñamos nuevos mecanismos y palabras al sistema para mejorar el mecanismo de detección de actividades de uso indebido. La siguiente, por favor.

trABIS se creó en 2022 y hubo algunos puntos importantes después de 2022. Antes de trABIS todas las registraciones de nombres de dominio estaban basadas en documentos. Para com.tr, net.tr, org.tr había que proporcionar documentos oficiales pero después de trABIS se convirtió en el primero que lo pide, el primero que lo recibe. Por eso allí hubo un pico en las actividades de uso indebido. Por eso tuvimos que mejorar nuestros mecanismos de detección.

Después de 2023 comenzamos a utilizar las capacidades de CERT con trABIS para poder mitigar estas acciones más rápidamente. Nuestros métodos de reclamos pueden ser por mail, por medio de la página web o por medio de una línea telefónica. Nos pueden llamar y contarnos acerca de cualquier actividad abusiva. Si ustedes buscan usom.gov.tr, si van a ese sitio web, van a ver una lista negra con direcciones. Está a disposición de todo el mundo. Nosotros compartimos esta lista con todo el mundo para que puedan implementar esta lista negra con direcciones de dominio, de malware, de phishing y los puedan utilizar en sus propios proyectos, firewalls o listas negras.

Tenemos un trabajo de colaboración abierta con los miembros del GAC para encontrar las políticas más eficaces para mitigar el uso indebido del DNS. También nos interesaría aprender acerca de otras políticas de ccTLD en otros países. Queremos ver qué medidas toman, cómo hacen acciones de mitigación. Queremos compartir experiencias y esperamos que ustedes también puedan contribuir con sus experiencias para que

nosotros podamos incorporar esos mecanismos a nuestros procesos. Si tienen alguna pregunta, con todo gusto pueden hacerla. Muchas gracias.

NICOLÁS CABALLERO: Muchísimas gracias, Mahmut, por su presentación. Ahora vamos a recibir preguntas. Si alguien desea hacerle alguna pregunta a Mahmut. Yo tengo algunas preguntas con respecto a los tipos de técnicas que están utilizando para identificar anomalías en el tráfico del DNS o en las consultas al DNS o incluso spam en general. Están utilizando inteligencia artificial. ¿Cuáles son las técnicas más exitosas en su experiencia o bajo su punto de vista? Random forest, por ejemplo, aprendizaje profundo. En ese caso, ¿qué tipo de aprendizaje profundo utilizan? ¿Redes neurales? No quiero entrar en muchísimo detalle pero me interesa tener una idea y ver qué es lo que mejor funciona para ustedes y en su experiencia.

MAHMUT ESAT YILDIRIM: Muy buena pregunta. A mí me encanta toda la parte técnica. Tenemos dos aspectos de este aprendizaje automático. Por un lado, utilizamos los métodos del aprendizaje automático para detectar dominios recientemente registrados y ver las similitudes. Por ejemplo, yo registro mahmut.com y nuestro sistema, nuestros modelos de aprendizaje automático, ven si se trata de un sitio web que se utiliza para phishing o no.

NICOLÁS CABALLERO: Random forest, bosques aleatorios, ¿verdad?

MAHMUR ESAT YILDIRIM: Sí, en general. Por otro lado estamos trabajando con los ISP de manera tal que puedan utilizar sus propios sistemas de redes de ISP, que son muy amplios, para detectar otras instancias de uso indebido como secuestro de dominios o ataques a una red. Ellos utilizan otro tipo de métodos de aprendizaje automático para detectar ese flujo de paquetes. Nos lo informan. Cuando los ISP detectan estos ataques nos lo informan y entonces nosotros trabajamos con los expertos del ccTLD y los expertos del CERT para hacer una respuesta ante ese incidente y mitigar el ataque.

NICOLÁS CABALLERO: La Comisión Europea pide la palabra. Adelante, Comisión Europea.

GEMMA CAROLILLO: Gracias, Nico. Soy de la Comisión Europea. Muchas gracias al colega de Turquía por esta presentación tan interesante. Tengo algunas preguntas. Nosotros en la Unión Europea para .EU tenemos un enfoque muy similar. Utilizamos inteligencia artificial y aprendizaje automático para evitar o prevenir la registración de nombres de dominio maliciosos pero su enfoque parece incluso más interesante. Va mucho más allá porque usted integra esta inteligencia para detectar amenazas a nivel del CERT.

Quisiera que me cuente un poquito más al respecto. No sé si se puede compartir esta información. Nosotros hablamos mucho acerca de estas herramientas. Usted dice que esto se desarrolló internamente, que lo desarrolló su ccTLD. No sé si nos puede contar acerca del costo de este sistema y si este sistema podría estar disponible o podría ser integrado fácilmente a otros registros. Gracias.

MAHMUT ESAT YILDIRIM: Muchas gracias. Nuestros mecanismos de CERT en general funcionan con nuestros propios desarrolladores. Tenemos todas las actividades internas de investigación y desarrollo también. Nos tomó más o menos un año construir todo este mecanismo. Puede llevar menos tiempo pero a nosotros nos tomó más de un año porque queríamos enseñarles a los algoritmos de aprendizaje automático para que puedan crear los modelos. Antes de tener este software teníamos operadores que trabajan manualmente y lo que hacían era etiquetar a los nombres de dominio con phishing, malware u otro tipo de actividad maliciosa. Por eso tenemos una lista muy amplia de dominios que ya están etiquetados. Con esta línea creamos nuevos modelos y los estamos mejorando a diario. Por eso es tan exitoso.

Por otra parte, con respecto al mecanismo CERT, como usted dijo podemos directamente prevenir las actividades maliciosas. El ccTLD puede detectar la actividad maliciosa o alguien notifica al ccTLD y con el CERT trabajamos con los ISP en cooperación y en cinco minutos bloqueamos el acceso de este nombre de dominio. Cancelamos también nombres de dominio, los dejamos sin funcionamiento,

depende del caso. Por ejemplo, si es comando y control, directamente bloqueamos el dominio.

NICOLÁS CABALLERO: Muchas gracias, Mahmut. Dos preguntas más para Mahmut. No lo vamos a torturar con mil preguntas. Yo tengo muchísimas preguntas. Bangladesh y luego India piden la palabra. Bangladesh.

MUSTAFIZUR RAHMAN: Muchas gracias, Sr. Mahmut, por su excelente presentación. Después de verificar la documentación se redujo la cantidad de reclamos. Verificar documentos insume tiempo pero a la vez el cliente requiere un servicio con rapidez. ¿Cómo hacen para lograr un equilibrio entre ambas cosas?

MAHMUT ESAT YILDIRIM: Eso sucedía antes de trABIS. Hasta el 2022, como usted dijo, era un proceso lento, muy lento. Uno, por ejemplo, quería registrar un dominio COM.TR y presentaba sus documentos, cuatro o cinco páginas de documentos. Los operadores verificaban todo, verificaban la validez de la documentación, que fuese documentación auténtica y le otorgaban el dominio. Ahora, después del 2022, ya no lo hacemos así. Ahora se hace todo por orden de llegada. No pedimos documentación. Gracias.

NICOLÁS CABALLERO: Muchas gracias. Está sonando un teléfono en algún lugar de la sala. Ahora toma la palabra el representante de India.

T. SANTHOSH: Muchas gracias, señor Presidente. Muchas gracias, Mahmut, por su presentación. ¿.TR está abierto al mundo? De ser así, ¿cuáles son los procesos de verificación y validación que hacen para gente de otro país?

MAHMUT ESAT YILDIRIM: .TR está abierto a todo el mundo pero tenemos una serie de registradores permitidos en Turquía. Usted solo puede utilizar esos registradores para registrar su dominio en .TR. Tiene que tener datos de WHOIS correctos y tiene que brindarnos esos datos: número telefónico, dirección de correo electrónico, dirección física. Es similar a lo que sucede con .COM o lo que sucede en otros gTLD.

NICOLÁS CABALLERO: Esta es la única oportunidad que tengo de preguntar. Tengo que preguntar. ¿Qué hacen con el tunneling del DNS? ¿Qué funciona mejor, en su experiencia? ¿Una percepción multicapa para redes neurales? ¿Qué funciona mejor en su experiencia?

MAHMUT ESAT YILDIRIM: En cuanto a su pregunta, creo que podemos utilizar flujos de datos y redes neurales. Eso funcionaría mejor. No podemos estar seguros de cómo se implementan los mecanismos de tunneling en el DNS. No

podemos saber qué pasa a través de esos canales. Sí podemos obtener los paquetes, reunirlos y con redes neurales enseñarle al sistema a que detecte lo que sucede en el tunneling del DNS utilizando una serie de paquetes. Luego podemos analizar eso en detalle de manera manual.

NICOLÁS CABALLERO: Muchas gracias. Bangladesh. Luego le doy la palabra a Estados Unidos. Adelante, Bangladesh. Disculpen. Me confundí. Alguien estaba levantando la mano. ¿El representante de Libia? Adelante.

KHALED ALTARHUNI: Gracias, señor Presidente. Gracias, Mahmut, por su excelente presentación. ¿El sistema puede hacerse cargo o responder ante contenido ilegal?

MAHMUT ESAT YILDIRIM: Sí. De hecho, este software AZAD que desarrollamos verifica la similitud del nombre de dominio y el contenido del sitio web. En primer lugar emite una alerta cuando ve esa similitud. Si el 95 % indica que es un dominio que se utiliza para phishing, entonces recibimos una alerta. Si no vemos el contenido o no tiene contenido el sitio web, no podemos hacer nada. Supongamos que una persona está apuntando con un arma. No significa que le vaya a disparar a alguien. Tenemos que ver si realmente en el sitio web se está realizando actividad maliciosa. Los algoritmos de aprendizaje automático verifican si se actualiza o se renueva el contenido del sitio web y si

vemos que hay actividad o contenido malicioso, entonces sí tomamos acciones para mitigar esto.

NICOLÁS CABALLERO: Muchas gracias, Mahmut. Muchas gracias, Libia, por su pregunta. Ahora le doy la palabra a Owen Fletcher, del gobierno de los Estados Unidos.

OWEN FLETCHER: Creo que nos estamos atrasando un poquito en la sesión. Voy a ser muy breve y creo que el resto de los oradores saben que trataré de hablar rápidamente. Tenemos a Leticia Castillo, de cumplimiento contractual de la ICANN, que nos presentará las novedades en cuanto a las enmiendas contractuales en materia de uso indebido que el GAC recibió con agrado y que son de sumo interés para el GAC también. Le doy la palabra a Leticia.

LETICIA CASTILLO: Muchas gracias. Soy directora sénior de cumplimiento contractual de la ICANN. Como dijo Owen, les voy a contar qué pasó tras cumplirse seis meses de la aprobación de estas enmiendas contractuales en materia de uso indebido. La semana pasada publicamos un informe detallado sobre estos primeros seis meses de cumplimiento efectivo. Tiene 17 páginas. Tiene mucha información acerca de las investigaciones realizadas, resultados, conclusiones, respuestas. Los invito a que lean el informe si desean conocer más información acerca de las acciones de cumplimiento efectivo. Pasemos ahora a los datos, por favor, en la siguiente diapositiva.

Desde el 5 de abril de 2024 al 5 de octubre de 2024 iniciamos 192 investigaciones con registradores y registros por uso indebido del DNS. En estos casos al menos había un tipo de uso indebido del DNS que es phishing, pharming, malware, botnet o spam cuando se utiliza específicamente como vector de uno o más de los otros cuatro modos de uso indebido.

En dos casos hay una notificación de incumplimiento formal para un registrador y para un operador de registro porque no cumplieron con los requisitos en materia de uso indebido. Resolvimos 154 investigaciones con el proceso de resolución informal que tenemos. Este proceso nos permite resolver la mayoría de nuestros reclamos de toda índole. El registrador o registro demuestra que está cumpliendo con las normas o toma acciones de mitigación o de remediación antes de que se tenga que llegar a acciones mayores por incumplimiento.

En un caso puede estar involucrado un nombre de dominio o varios. A veces se descubre también que hay más dominios en una misma cuenta que están siendo utilizados maliciosamente. Estas 154 investigaciones resultaron en la suspensión de más de 2.700 nombres maliciosos y también se desactivaron más de 350 sitios web. En algunos casos el registrador también realizaba servicios de alojamiento web o web hosting.

Estos son los números, las cifras para los seis meses que van del 5 de abril al 5 de octubre de 2024. Tenemos múltiples investigaciones en curso. Algunas han sido cerradas, concluidas. No están incluidas aquí pero se las incluirá en la próxima actualización o el próximo informe. En estos seis meses también participamos en múltiples actividades de

difusión y comunicación para concientización a la comunidad acerca de estos nuevos requisitos.

En septiembre, por ejemplo, participamos en un taller con las partes contratadas en Pekín. Allí se habló acerca de los nuevos requisitos en materia de uso indebido del DNS. Lo mismo hicimos aquí el mes pasado, en Estambul. Trabajamos con nuestros colegas del departamento de [GSE] y GDS en sus actividades de capacitación como parte del enfoque multifacético de la ICANN para mitigar el uso indebido del DNS.

Hemos iniciado recientemente una auditoría para validar el cumplimiento del acuerdo de registro, no solo en cuanto a los requisitos en materia de uso indebido del DNS. En junio comenzamos a publicar informes mensuales acerca del cumplimiento efectivo de estos requisitos. Estos informes se clasifican según el tipo de uso indebido del DNS y las acciones pertinentes. Comenzamos con los datos de abril de 2024, y lo publicamos y actualizamos mes a mes.

El formato de los informes permite ver un panorama integral de todos estos casos. También lo complementamos con actualizaciones periódicas de distintos resultados, conclusiones, como las que les presenté previamente. También esto se ha publicado en un informe el 8 de noviembre. La idea es siempre seguir mejorando y actualizando estos informes. Recibimos con agrado los comentarios y las sugerencias de la comunidad. Ya les había mencionado el informe del 8 de noviembre. Pueden acceder mediante el enlace que está en la pantalla. Siguiente diapositiva, por favor.

También les mencionaba las 154 investigaciones de casos de uso indebido del DNS que hemos resuelto. Aquí vemos por qué fueron resueltas. Vemos también el número de registradores. En casi el 52 % de los casos el registrador tomó acciones. En el 21 % de los casos el registrador no encontró evidencias que justificaran el uso indebido del DNS. Nos dieron una razón o una explicación de lo que realizaron, de la investigación que realizaron y cómo llegaron a esa conclusión.

Por ejemplo, un registrador evaluó toda la información que tenía con respecto a un nombre de dominio, la información de la cuenta, las comunicaciones con el registratario y el titular de la cuenta y determinó que el registratario realmente había actuado con el conocimiento y consentimiento de la entidad que se creía que estaba realizando una actividad de phishing en un nombre de dominio.

También en casi el 12 % de los casos el registrador interrumpió el uso indebido del DNS. Por ejemplo, le informó al registratario, luego el registratario desactivó la URL donde se estaba cometiendo el uso indebido. En el 3 % de los casos aproximadamente el registrador tomó otras acciones para detener el uso indebido. Por ejemplo, sinkholing o redireccionar el tráfico de manera tal que quienes querían llegar al dominio malicioso eran redirigidos a un IP controlado por el registrador. En la próxima diapositiva vamos a hablar acerca de registros.

Resolvimos tres casos de uso indebido del DNS con operadores de registros. Todos los nombres de dominio se dieron de baja. Los dio de baja el registro. Estos son casos resueltos. Hay muchos otros que no. También tuvimos un caso que se limitó a problemas con el contacto de

uso indebido y este caso también se resolvió. La diferencia en las cantidades entre los casos resueltos con los registros y los registradores coincide con el hecho de que todos los reclamos recibidos en el 94 % se refiere a registradores y en todas las investigaciones iniciadas, el 97 % se refieren a registradores y el resto a registros.

No tenemos una cantidad mínima o máxima para iniciar o escalar una investigación. Esto lo prueba el hecho de que durante el mismo periodo emitimos una notificación de violación de contrato formal, pública, o un registro y un registrador. Estos son los números de los primeros seis meses. Estamos haciendo muchas cosas. Hay mucho que se resolvió después del 5 de octubre y pensamos continuar brindando actualizaciones y publicando informes con detalles. Voy a detenerme aquí para que haya tiempo para responder preguntas.

OWEN FLETCHER: Muchas gracias. Me resulta muy útil esa información. Seguramente a los demás también les pareció muy útil. Este es un tema importante para el GAC. Seguramente hay preguntas del público. Nico, ¿usted quiere comenzar?

NICOLÁS CABALLERO: Sí, tenemos tiempo para un par de preguntas. India.

T. SANTHOSH: Muchas gracias, señor Presidente. La presentación explica muy brevemente el papel de los registros y los registradores. En India, durante ese periodo, elevamos tres reclamos a través de este sitio web de reclamos contractuales pero no tenemos información con respecto al estado de esos reclamos, a la situación. Lo mismo ocurre con respecto al correo electrónico. ¿Cuál es el estado de los reclamos que planteamos? Esta información no queda reflejada. ¿Podría hablar sobre este tema? Gracias.

LETICIA CASTILLO: Gracias por la pregunta. Si entendí correctamente, usted presentó tres reclamos. Creo que dijo tres. No recibió información con respecto al estado de esos reclamos, a la situación. Creo que sé a qué reclamos se refiere. Creo que solicitamos cierta información y pedimos más tiempo. Estamos todavía esperando pero, si le parece, después podemos hablar sobre este tema, cuando termine la sesión, para ver si estamos hablando de los mismos reclamos.

Cuando se presenta un reclamo, hay una confirmación con una identificación de cada caso y luego hay comunicaciones adicionales que el procesador le envía a quien presenta el reclamo para solicitar información adicional. Esto suele ocurrir con frecuencia. Para hacer la revisión completa de un reclamo muchas veces necesitamos aclaraciones, evidencias. Enviamos esa solicitud, recibimos casos en los que muchas veces vamos y venimos pidiendo información. También a veces recibimos solicitudes de quienes presentan reclamos y cuando se resuelven los casos también reciben una información acerca de por qué se resolvió el caso y cómo contactarse con el

departamento de cumplimiento contractual en caso de que haya alguna pregunta con respecto a ese caso resuelto. Con todo gusto, si quiere, luego podemos hablar sobre este caso y darle más información sobre el estado de esos reclamos.

NICOLÁS CABALLERO: Tenemos Países Bajos y luego Estados Unidos. Por favor, traten de ser breves.

ALISA HEAVER: Gracias por la presentación. Me preguntaba cómo se comparan estos números con lo que ocurría hace medio año o hace un año antes de que se instauraran las nuevas medidas. Mi segunda pregunta es cuál es la duración promedio de una investigación antes de que un registrador tome algún tipo de medida. ¿En qué medida las investigaciones iniciadas están basadas en las nuevas medidas contractuales? Es decir, en qué medidas están relacionadas con las reglamentaciones anteriores.

LETICIA CASTILLO: Gracias. Con respecto a las cantidades a lo largo de los últimos años, incluso antes del 5 de abril, observamos un aumento en la cantidad de reclamos que recibimos, reclamos de uso indebido. En 2023 recibíamos en total en promedio 1.300 reclamos nuevos por mes que se sumaban a los casos existentes. De enero a septiembre de 2024 el promedio fue casi 2.000 reclamos nuevos por mes. Hubo un aumento. Incluso antes de abril de 2024.

Con respecto al tiempo que lleva una investigación, depende totalmente de la clase de investigación. Tenemos casos de uso indebido del DNS con un nombre de dominio. En ese caso contactamos al registrador. El registrador dice: “Sí, vamos a dar de baja ese nombre de dominio” y a veces se puede resolver en el mismo día, pero hay investigaciones que tienen miles de nombres de dominio donde la parte contratada solicita que no aborden ese caso de uso indebido pero también vemos patrones que indican que no hay un proceso instaurado para abordar el uso indebido del DNS. No se trata solamente de ese informe sino que esto puede afectar futuros informes y la forma de encarar el uso indebido del DNS en el futuro.

En esos casos pedimos que preparen un plan de remediación que nos indique cómo lo van a implementar, distintos hitos, fechas de implementación para asegurarnos de que implementen ese proceso y esperamos hasta que tienen ese proceso implementado y luego lo probamos y recién allí cerramos el monitoreo del caso porque si ocurren casos después de que se haya implementado todo eso, se debe aumentar o incrementar la medida de cumplimiento efectivo. Depende totalmente del caso.

NICOLÁS CABALLERO: Muchas gracias. Tengo un pedido más de palabra. Estados Unidos, Laureen.

LAUREEN KAPIN: Hablo como miembro del grupo de trabajo de seguridad pública. Quiero agradecer todo el trabajo que se está haciendo aquí y quiero decir también que es muy alentador ver estas respuestas tan específicas para mitigar el uso indebido del DNS. Es una señal de que estos son cambios bienvenidos y eficaces. Mi pregunta es la siguiente. En esta diapositiva hay una categoría que dice: "El registrador tomó una medida para alterar el uso indebido del DNS que es una categoría aparte de suspender el uso indebido". ¿Podría explicar cuál es la diferencia?

LETICIA CASTILLO: Gracias, Laureen. La obligación en el contrato implica llevar a cabo acciones de mitigación para detener o alterar esas acciones de uso indebido. Esas acciones dependen de las circunstancias específicas. En términos generales, un claro caso de uso indebido del DNS es un nombre de dominio que se registró para perpetrar uso indebido. Uso genera la suspensión del nombre de dominio.

Hay otros casos como por ejemplo… Estoy pensando en un caso en particular en el que fue un nombre de dominio comprometido. El registrador contactó al registratario, le informó acerca de lo que estaba pasando y le dijo: "Usted tiene que hacer esto y lo otro para que esto no siga ocurriendo". Esto fue un cambio, una alteración por parte del registrador. Se considera que en ese caso se cumplió con el acuerdo.

NICOLÁS CABALLERO: Gracias. Le doy la palabra a Owen.

OWEN FLETCHER: Gracias. Es muy bueno ver los indicadores relacionados con el cumplimiento efectivo de las enmiendas contractuales y ver los resultados que ustedes ya están informando. Ahora vamos a darles la palabra a los miembros del panel. Tenemos a Reg Levy, de Tucows, Dennis Tan, de VeriSign, y Jeff Bedser, de CleanDNS, y también de SSAC.

Ellos van a responder preguntas que van a estar en la próxima diapositiva. Hay una pregunta que solo es para Reg. Dice: "Como parte contratada, ¿qué hicieron ustedes desde las enmiendas? ¿Podría explicar esto?" Las preguntas dos y tres son para todos. ¿Cuáles han sido el impacto y las consecuencias de estas enmiendas en el campo? ¿Cuáles son las lecciones aprendidas en los primeros seis meses de la implementación de las enmiendas contractuales? Esto nos permitirá obtener más información acerca de lo que está ocurriendo con las enmiendas. Trataremos de darles tres minutos a cada uno. Les pido disculpas si los interrumpo pero voy a tratar de que podamos terminar a tiempo. ¿Podemos empezar con Reg?

REG LEVY: Reg Levy, de Tucows, registrador de nombres de dominio. Gracias, Owen. Tucows estuvo muy involucrado en la negociación de las enmiendas. Lo principal que voy a decir es que no hay demasiado que hayamos cambiado después de las enmiendas. Pensamos que comenzamos haciendo bien las cosas pero nos alegra mucho ver que ahora las enmiendas son parte de las obligaciones contractuales.

El equipo de siete profesionales que se dedican al uso indebido del DNS hace una revisión de todos los informes que llegan y confirman el supuesto uso indebido y toman medidas de mitigación. Una de las cosas que comenzamos a hacer y que cambió después de las enmiendas o que quizá se hace debido a las enmiendas es que empezamos a investigar en lugar de suspender a muchos de los dominios de phishing. Investigar significa que dirigimos los registros del DNS de un dominio en particular a un conjunto de servidores DNS en particular que son ejecutados por CleanDNS, que está aquí en el panel, para obtener información adicional acerca de las campañas de phishing, para que ellos puedan ver las tendencias en los distintos registradores. Nosotros vemos distintas cosas que ocurren en nuestro espacio de nombres pero un grupo como CleanDNS puede ver problemas más amplios que afectan a toda la industria y esperamos que esta información que les damos les ayude a ellos a identificar mejor las campañas que se producen en toda la industria.

OWEN FLETCHER: Muchas gracias, Reg. Muy bien. Estuvo por debajo de tres minutos su respuesta. Bien hecho. Dennis, ¿quiere tomar la palabra?

DENNIS TAN: Muchas gracias, Owen. No tengo mucho que agregar a lo que dijo Registración con respecto a las enmiendas en materia de uso indebido y su impacto. En cuanto a los operadores de registro, gran parte de la responsabilidad recae sobre el registrador que tiene relación con el registratario. Nosotros, los registros, nos ocupamos de los botnets, los

DGA y eso lo puede prevenir el registrador al momento de la registración. Esto requiere ingeniería reversa. No hay tanto que podamos hacer a nivel del registro.

Con respecto a los nombres de dominio en nuestro registro, se los referimos al registrador para que pueda mitigar o interrumpir el uso indebido del DNS que está sucediendo. Quiero decir en general que uno de los aspectos que tuvo, un aspecto positivo y práctico que tuvieron estas enmiendas para los registros, es mejorar el nivel de la calidad de los informes o las denuncias de uso indebido. Esto facilita evaluar y determinar cuál es el tipo de uso indebido y actuar en consecuencia.

Además, quiero decir que nosotros en la Cámara de Partes Contratadas venimos trabajando conjuntamente desde que se instituyeron estas enmiendas en materia de uso indebido. Siempre dijimos que sería el primer paso en una actividad múltiple para ayudar a mitigar el uso indebido del DNS. Venimos trabajando junto con otros grupos de la comunidad de la ICANN para entender problemáticas en común en las cuales podamos trabajar, generar mejores prácticas o también encontrar soluciones comunes a esos problemas.

Recientemente, algunos de ustedes habrán participado en una sesión con la NCSG para ver prácticas de mitigación del uso indebido del DNS desde la mirada de la evaluación humana de todos estos impactos. Creo que ahora me voy a detener en virtud del tiempo disponible. Le devuelvo la palabra, Owen.

OWEN FLETCHER: Muchas gracias, Dennis. Ahora pasamos a Jeff. Usted tiene algunas diapositivas, ¿verdad?

JEFF BEDSER: Muchas gracias. Las primeras diapositivas realmente repiten lo que ya se ha mencionado. Vamos a avanzar un poquito, por favor, en la presentación. Hasta aquí, muy bien. Quiero hacer alguna comparación de datos. Discúlpenme. No tengo muy buena voz. Voy a tratar de ser lo más claro posible. Quiero compartir algunos datos sobre grandes volúmenes de uso indebido del DNS para poder tener una perspectiva de los volúmenes acerca de los cuales estamos hablando.

Desde abril a junio procesamos 628.000 denuncias de uso indebido, que son casi 60.000 nombres de dominio únicos. El volumen mensual antes de este cambio en las obligaciones era de 225.000 por mes. Después de estas nuevas obligaciones vimos un incremento y llegamos casi a 240.000 informes o denuncias mensuales. Estoy hablando con registros, registradores y empresas que proveen servicios de hosting. Ellos ven este incremento porque ahora hay un cambio en las obligaciones y se están generando más informes.

Quizá un denunciante denuncie al mismo informe ante el registrador y el registro, por ejemplo, y ante la compañía de hosting. Eso genera tres informes. Aquí vemos los volúmenes de informes de phishing entre septiembre de 2024 y octubre de 2023. Los vemos de atrás hacia delante. Vemos que los promedios mensuales de informes han subido notoriamente en algunos casos pero en general el volumen de los informes se mantiene al mismo nivel en cuanto a phishing.

Esto me parece muy interesante. Tuvimos un informe de .TOP, de un registro. Esta es información pública. En julio se le notificó acerca de un incumplimiento. Había alrededor de 7.000 informes de uso indebido para .TOP. En agosto subió un poquito. En septiembre subió un poco más y en octubre llegó a los 13.000. Este es un ejemplo muy bueno de cumplimiento contractual de la ICANN porque a pesar de la notificación de incumplimiento, el volumen de los informes de incumplimiento en esa zona de ese TLD siguió incrementando. Lo que quiero decir es que cumplimiento contractual de la ICANN está realmente haciendo su trabajo y está ocupándose del uso indebido. Lo demuestran estos volúmenes que vemos en pantalla.

Lo que estamos midiendo es la cantidad total de informes procesados, la cantidad total de dominios involucrados. Puede ser una proporción de tres a uno, de dos a uno. La relación entre los informes y los dominios. Luego también la cantidad de acciones que implementa cumplimiento contractual por cada registro entre otras medidas.

¿Qué deberíamos medir? Hay que cambiar comportamientos para lograr la mitigación. Tenemos que ver cuántos informes realmente prueban efectivamente la mitigación y las acciones implementadas porque en la mitad de los casos no hay ninguna acción, no se toma ninguna acción. Los daños fueron mitigados antes de los informes. Tenemos que ver con esta nueva manera de obtener evidencias, tenemos que ver qué pasó realmente, cuánto duró el daño, el perjuicio. Obviamente si un nombre de dominio tiene un ciclo de vida más breve, entonces será menor el número de víctimas. Podemos usar aprendizaje automático e inteligencia artificial y podemos reducir todo

este tiempo desde la validación de un informe hasta la acción de mitigación.

Luego tenemos que ver algo en lo que también está trabajando la ICANN con Domain Metrica, su nuevo proyecto. Lo hace la oficina del director de Tecnologías. Tenemos que ver cuán efectiva fue la mitigación en cuanto a la reducción del volumen total. Tenemos que ver justamente qué pasa con la mitigación y con el comportamiento de los actores maliciosos. Luego tenemos que ver también cuánto esfuerzo se hizo para que una parte contratada que estaba en incumplimiento pudiera modificar su comportamiento.

OWEN FLETCHER: Jeff, le pido disculpas. Tiene que ir cerrando porque se nos está acabando el tiempo.

JEFF BEDSER: Esta es mi última diapositiva. Muy bien. El cambio en las obligaciones fue muy bueno. El cambio en los comportamientos está dando resultados. Vemos que las partes problemáticas que están fuera del ecosistema no están tomando acción y están siendo notificadas. Hay mucho más para decir aquí pero, para bien o para mal, las enmiendas están teniendo un impacto en el sistema y a los seis meses de su implementación creo que las conclusiones son positivas.

OWEN FLETCHER: Muchas gracias, Jeff. También tenemos una declaración de Mukesh Chulani, de la ICANN, que trabaja en Dominios Globales y Estrategia.

MUKESH CHULANI: Quiero resaltar que estamos viendo un impacto a nivel de casos. Un impacto que tienen estas enmiendas. Ya han pasado siete meses desde su implementación y hemos escuchado a las partes contratadas. Hemos visto informes consolidados del equipo de cumplimiento contractual. Vimos informes de terceros especialistas en métricas. Ya estamos viendo impactos positivos. Estas enmiendas, como mencionó Dennis, no fueron concebidas como una solución definitiva sino como un primer paso. Seguramente vamos a querer cambiar a futuro. Hay que continuar siguiendo todo esto muy de cerca. Hay que seguir dialogando.

Desde nuestro punto de vista cumplimiento contractual tiene que exigir el cumplimiento de las obligaciones contractuales. Tenemos datos que se enfocan específicamente en los casos existentes y hay que complementar esto con el punto de vista más amplio del mercado, y qué sucede con el uso indebido allí.

El equipo del director de Tecnologías de la ICANN tiene el proyecto Metrica, que es una plataforma para recopilar mediciones de datos. En los próximos días y meses tendremos más información y luego tenemos el proyecto INFERMAL que tiene que ver con las preferencias de los atacantes. Estamos trabajando así, internamente, y, como dijo Leticia, seguimos viendo las mejores maneras de intercambiar mejores

prácticas a través de plataformas como las que he mencionado. Muchas gracias por la invitación. Sigamos trabajando juntos.

OWEN FLETCHER: Muchas gracias, Mukesh. Creo que es muy beneficioso, muy positivo para nosotros recibir esta información de investigaciones y análisis de una amplia gama de actores de manera tal que el GAC tenga esta información que pueda nutrir sus debates acerca de los próximos pasos a seguir. Ahora tenemos un tiempo para preguntas y respuestas antes de pasar al debate del GAC. Nico, le doy la palabra.

NICOLÁS CABALLERO: Muchas gracias, Owen, Mukesh. Gracias a los panelistas también: Registración, Dennis y Jeff. Yo no veo que nadie en la sala de Zoom o aquí en la sala esté solicitando la palabra. Le doy la palabra a Martina, quien liderará este próximo bloque.

MARTINA BARBERO: Alguien solicita la palabra, la Comisión Europea.

NICOLÁS CABALLERO: Comisión Europea.

GEMMA CAROLILLO: Muchas gracias, Nico. Tengo una pregunta para la persona de VeriSign. Usted mencionó que están analizando un posible desarrollo de

políticas. Usted habló de su relacionamiento con la comunidad. Quiero saber si tiene ideas ya porque en el GAC estamos justamente analizando la misma idea.

DENNIS TAN: Muchas gracias por su pregunta. No necesariamente vamos a hacer un proceso de desarrollo de políticas porque la comunidad nos dijo que este proceso es muy engorroso, insume mucho tiempo y muchos recursos. Ahora se están concentrando en PDP más específicos y más acotados. Un PDP sería un posible curso de acción. Estamos hablando con la comunidad de la ICANN, lo estamos analizando. Queremos leer en mayor detalle el informe del proyecto INFERMAL que creo que será de mucha utilidad. Será un disparador para nuevas rondas de diálogo que, por supuesto, son bienvenidas.

NICOLÁS CABALLERO: Estados Unidos.

OWEN FLETCHER: Muchas gracias. Creo que la junta directiva ofreció hacer sesiones de escucha sobre el alcance de los posibles PDP a futuro para tener consideraciones con un poco más de matices con respecto a las enmiendas. Creo que esto sería muy interesante y podríamos seguir al respecto.

REG LEVY: Reg Levy, en representación del grupo reducido sobre uso indebido del DNS. Dennis y yo somos los copresidentes de este subgrupo o grupo reducido que está dentro de la Cámara de Partes Contratadas. Nosotros estuvimos en algunas sesiones de escucha que no son estas sesiones que ofreció la junta directiva. Hemos estado dialogando con distintos grupos de la comunidad, a ver qué es lo que ellos quieren que realicemos, qué les interesa y cómo nosotros, en tanto partes contratadas, podemos retomar esas iniciativas. Quizá no un PDP. Ya nos reunimos con el ALAC. Esperamos reunirnos con el SSAC para justamente dialogar de esta manera, individualmente con cada grupo de la comunidad para que cada grupo tenga la oportunidad de dialogar con nosotros.

NICOLÁS CABALLERO: Gracias a Estados Unidos. Gracias, Reg. No veo que nadie más que solicite la palabra. Le doy la palabra a Martina Barbero, de la Comisión Europea, que nos hablará acerca de los próximos pasos y las consideraciones para el comunicado del GAC.

MARTINA BARBERO: Tenemos dos partes de la agenda que tenemos que cubrir antes de dejarlos libres para ir a almorzar. Téngannos paciencia porque es importante. En primer lugar queremos abrir el espacio para hablar acerca de los temas que escuchamos hoy. Preparamos algunas preguntas para ver si ustedes quieren compartir algún aporte. Principalmente quisiéramos hablar dentro del GAC acerca de si tienen alguna opinión con respecto a lo que hablamos hoy acerca de la

implementación y los impactos de las enmiendas contractuales. Escuchamos muchas cosas interesantes. Queremos saber si tienen alguna reacción, algún comentario para compartir con nosotros. Este sería un buen momento para hacerlo.

También queremos saber si hay alguna otra lección que hayamos aprendido de la ronda anterior y que pudiera ayudarnos a prepararnos para la siguiente ronda en relación con la mitigación del uso indebido del DNS. Hablamos brevemente acerca de los PIC ayer con las partes contratadas pero también, si bien yo no estuve allí, hay un informe muy bueno sobre uso indebido del DNS de la ronda anterior que tiene algunas conclusiones que podríamos considerar al prepararnos para la siguiente ronda.

Finalmente, escuchamos una muy buena presentación de nuestros colegas de Turquía. Quisiera saber si hay alguna otra mejor práctica de ccTLD que podríamos considerar y que podría servirnos para pensar un poco más acerca del espacio de gTLD. Sería bueno compartir esa información. Antes de pasar a las consideraciones del comunicado quisiera abrir el espacio para preguntas y comentarios acerca de este punto y ver si algún miembro del GAC quiere comentar algo.

NICOLÁS CABALLERO: Gracias, Martina. Abrimos el espacio. Con todo gusto vamos a responder cualquier pregunta, comentario o cualquier cosa que quieran compartir con nosotros ahora. India pide la palabra. Adelante.

T. SANTHOSH: Muchas gracias. Durante la reunión 80 de la ICANN hubo una propuesta para la implementación del DNS que debía ser obligatoria, especialmente en los sectores financieros, salud, gobierno y telecomunicaciones. Esto estaría alineado con las medidas de seguridad global y permitiría proteger los intereses nacionales vitales. ¿Alguien tiene alguna opinión con respecto a la implementación de esto en relación con DNSSEC? Muchas gracias.

REG LEVY: Reg Levy, de Tucows. DNSSEC es una forma de asegurar los nombres de dominio. HTTPS es, al parecer, el protocolo actualmente adoptado por el mercado. El mercado decidió que esto es lo que quiere. Nosotros ofrecimos DNSSEC. Con todo gusto podemos asignar DNSSEC a cualquier nombre de dominio que nos adquieran. No es una opción muy popular. No es un punto de seguridad que interese al parecer a muchos de nuestros clientes o que aprovechen dado que HTTPS al parecer es más utilizado.

Hay muchos navegadores que ahora están pidiendo HTTPS, lo cual está generando un impulso. Yo creo que no hay ningún problema en pedirles a algunos actores o invitar a algunos sectores… Perdón, me piden que hable despacio. Para mí no hay ningún problema en pedir a determinados sectores que consideren vías adicionales de seguridad pero sí he visto que a la mayoría de los clientes no les interesa DNSSEC tal como nos interesa a nosotros en la ICANN.

NICOLÁS CABALLERO: Gracias, Reg. Reino Unido pide la palabra.

[CHRISTOPHER]: Es la primera vez que vengo a una reunión de la ICANN. Trabajo en el grupo de trabajo de seguridad pública en particular y quisiera hacer un comentario que tiene que ver con lo que señaló India. Desde una perspectiva más general creo que el viernes pasado la presidencia del consejo de seguridad de Naciones Unidas encabezó una sesión y hubo varios estados miembros que firmaron una declaración acerca del impacto sobre salud.

Especialmente hubo una conversación acerca de ransomware, que tiene mucho que ver con lo que estamos hablando aquí. Por lo tanto, hay un interés creciente en diferentes miembros de Naciones Unidas en este tema. Hay distintas iniciativas. Veo que ustedes trabajan activamente junto con Reino Unido y otros países representados aquí, en esta sala.

No es tanto una pregunta sino más bien un comentario. Hay otros organismos multilaterales en los que están involucrados algunos representantes de aquí que están impulsando estos temas en la agenda. Es muy pertinente que haya habido una reunión a nivel de Naciones Unidas. Estamos trabajando a través del grupo de trabajo de seguridad pública en estos temas. Estamos avanzando en este sentido. Gracias.

NICOLÁS CABALLERO: Gracias, Reino Unido. Estados Unidos pide la palabra.

OWEN FLETCHER: Gracias. Quería responder brevemente con respecto al tema de DNSSEC. Recuerdo que en la ICANN80 hubo un texto en el comunicado que tiene que ver con lo que solicitó Santhosh en su momento. Podemos hacer una revisión del texto pero yo diría que el texto en ese momento no impulsaba la promoción de la adopción de DNSSEC. No estoy muy seguro con respecto a la idea de que sea un requerimiento. Me parece que eso es algo que antes de considerarlo deberíamos recibir más información y tener más datos con respecto a las implicancias para saber si esta es una idea factible. También recordaba que SSAC señaló en su reunión bilateral con nosotros sobre estos temas algo parecido. Si determinamos que queremos buscar más información, esta sería una buena fuente. Muchas gracias.

NICOLÁS CABALLERO: Gracias, Estados Unidos. No veo que nadie más pida la palabra en forma presencial o virtual de modo que voy a volver a Martina Barbero, de la Comisión Europea, quien nos va a guiar a través de los próximos pasos y consideraciones relacionadas con el comunicado que debemos tener en cuenta.

MARTINA BARBERO: Gracias, Nico. Gracias a todos los miembros del GAC que intervinieron hoy. Christopher nos recordó correctamente que este es un tema que está subiendo en importancia en la agenda. Esperamos que lo tomen

en cuenta. Esto nos lleva a las consideraciones relacionadas con el comunicado. ¿Podríamos pasar a la siguiente diapositiva, por favor?

Los encargados de los temas incluyeron aquí algunos elementos a tener en cuenta pero ustedes también como miembros del GAC pueden hacer sus aportes. Como siempre, en el comunicado tenemos la posibilidad de agregar temas bajo cuestiones de importancia. Hay algunos temas que podríamos considerar incluir en el comunicado después de la presentación que tuvimos sobre la implementación de las enmiendas contractuales y la medición de su efectividad. Podríamos quizá sugerir que siga estando incluido en el comunicado. Creo que esto sería interesante.

Por supuesto, escuchamos hablar esta mañana acerca de estos temas. Recordemos que en la sección de comentarios públicos el GAC envió una respuesta que indicaba que había algunos temas que requerirían un trabajo adicional. Esto figura aquí, el monitoreo proactivo, transparencia, revisión periódica de la definición de uso indebido del DNS, abordar DNS dentro y fuera de la ICANN. Perdón, orientación sobre términos clave, consideraciones con respecto a cumplimiento contractual. Tiene razón. Estoy hablando demasiado rápido. Estaba tratando de terminar lo antes posible.

Estos son temas que fueron incluidos en la respuesta al periodo de consulta pública sobre enmiendas contractuales. Luego en Kigali y también ayer hablamos acerca de las consideraciones en cuanto a la preparación para la próxima ronda de TLD, que abrirá pronto. Estos son todos elementos entonces que podrían incorporarse al comunicado pero el objetivo de los siguientes ocho minutos es ver si

estos son puntos que ustedes consideran pertinentes, si hay algo más o si hay algún otro tema que quieran compartir antes de que pasemos a la parte de redacción del comunicado. Muchas gracias.

NICOLÁS CABALLERO: Gracias, Martina. Abrimos el espacio para preguntas o comentarios, ideas. Estados Unidos, adelante.

OWEN FLETCHER: Antes se mencionó el informe INFERMAL y alguien, creo que Jeff, mencionó también Metrica, la plataforma de OCTO. Tenemos distintas fuentes de información y de investigación que podrían servirnos para identificar trabajo futuro sobre enmiendas relacionadas con el uso indebido del DNS. También mencioné que hay sesiones de escucha y Reg también mencionó que las partes contratadas piden aportes y opiniones con respecto a este trabajo también.

NICOLÁS CABALLERO: Gracias, Estados Unidos. La Comisión Europea pide la palabra.

GEMMA CAROLILLO: Gracias. Quiero apoyar lo que decía Owen. Podemos pensar en las sesiones que tuvimos ayer y hoy. Creo que hay mucho interés en el GAC en el informe de SSAC, incluido el impacto de las nuevas tecnologías sobre el uso indebido del DNS. Hubo muchísimas preguntas y mucho interés en avanzar con este trabajo y también creo que la propuesta de ALAC para que ambos grupos trabajen juntos es una muy buena

propuesta, especialmente en torno a los nuevos dominios registrados de forma maliciosa pero creo que el tema en general es un tema que compartimos ALAC y GAC.

NICOLÁS CABALLERO: Gracias, Comisión Europea. ¿Algún otro comentario o pregunta? Adelante.

SAMANEH TAJALIZADEHKHOOB: Gracias por las presentaciones. Soy Samaneh, directora de investigación del equipo de SSR de la organización de la ICANN. Dado que surgió el nombre un par de veces quiero decir que nosotros somos los líderes del proyecto Metrica de la ICANN. También del proyecto INFERMAL. Quiero invitarlos a todos a la sesión que tendrá lugar mañana a las 13:15. En esa sesión hablaremos sobre los dos proyectos, la retroalimentación que recibimos y cuáles serán los próximos pasos. Gracias.

NICOLÁS CABALLERO: Gracias por la invitación. Lamentablemente el GAC tendrá una sesión al mismo tiempo. Vamos a estar redactando el comunicado mañana a las 13:15 pero, de todas formas, muchas gracias. Por supuesto, esto no impide que puedan asistir. Por supuesto. Muchísimas gracias. Reino Unido pide la palabra.

NIGEL HICKSON: Gracias, señor Presidente. Este es un diálogo realmente excelente. No vamos a tener tiempo de tocar este tema ahora. Es un tema nuevo pero en reuniones anteriores cuando hablamos acerca del RDRS también observamos el diálogo que había tenido lugar acerca de tener tantos PDP o micro PDP sobre aspectos específicos del uso indebido del DNS como phishing, malware.

En términos generales, los miembros del GAC consideran que esta es una buena idea. No se ha avanzado. Sé que todos tienen muchos temas en sus agendas y la gente de la GNSO también pero creo que es algo a lo que tenemos que volver porque claramente hay temas específicos con respecto a alguno de estos aspectos del uso indebido del DNS. Gracias.

NICOLÁS CABALLERO: Gracias, Reino Unido. Tomamos nota. ¿Algún otro comentario? No veo que nadie más pida la palabra en forma presencial o virtual de modo que vamos a darles a nuestros invitados la posibilidad de hacer algún comentario final. Les doy la palabra a los miembros del panel.

GEMMA CAROLILLO: Quiero agradecer a todos los delegados por haber participado en el debate hoy. Los colíderes del tema podrían sugerir texto para el comunicado. Quizá este es un tema que podría continuar estando en la sección de cuestiones de importancia del GAC. Por lo tanto, espero que consideren esto.

NICOLÁS CABALLERO: Gracias, Comisión Europea. ¿Algún otro comentario de nuestros distinguidos invitados?

DENNIS TAN: Gracias, Nico. Valoro esta invitación. Nos parece que es muy importante. Reg y yo estamos disponibles. Pueden contactarnos para hablar de cualquier cosa. Las enmiendas fueron el primer paso y ahora esperamos mantener las siguientes conversaciones, ya sea a través de un PDP u otra cosa. Queremos participar. Muchas gracias.

NICOLÁS CABALLERO: Muchas gracias, Jeff, Hajime. Adelante, Jeff.

JEFF BEDSER: Quiero aprovechar esta oportunidad para agradecerles por darme la oportunidad de hablar sobre este tema. Gracias por la invitación.

NICOLÁS CABALLERO: Muchas gracias. Mahmut, Hajime.

HAJIME ONGA: Muchas gracias por esta invitación. Gracias. Espero que podamos continuar hablando de este tema en la próxima sesión.

NICOLÁS CABALLERO: Gracias, Hajime. Mahmut.

MAHMUT ESAT YILDIRIM: Muchas gracias por darme la oportunidad de compartir nuestra experiencia con ustedes. Espero verlos aquí nuevamente para poder seguir intercambiando información y compartir nuestras experiencias.

NICOLÁS CABALLERO: Gracias, Mahmut. Nosotros esperamos poder volver pronto a Estambul. Colombia.

THIAGO DAL-TOE: Gracias, Nico. Quiero recordarles a todos que el uso indebido del DNS es uno de los temas que forman parte de nuestros objetivos estratégicos. De hecho es el objetivo número cuatro. Quiero agradecerles a los encargados de los temas por haber organizado esta sesión fantástica. Espero que podamos continuar trabajando muy bien sobre estos temas.

NICOLÁS CABALLERO: Muchas gracias a todos. Damos por finalizada la sesión. Volvemos a reunirnos a la 1:15 en punto para nuestra reunión con la junta directiva. Muchas gracias a todos. Disfruten el almuerzo.

[FIN DE LA TRANSCRIPCIÓN]