

---

ICANN74 | Foro de Políticas – Debate del GAC: uso indebido del DNS  
Martes, 14 de junio de 2022 – 15:00 a 16:00 AMS

MANAL ISMAIL:

Hola a todos. Por favor, tomen asiento porque vamos a comenzar a la brevedad. Veo que hemos regresado a tiempo. Buenos días, buenas tardes, buenas noches a todos quienes están aquí en la sala del GAC y también en Zoom. Bienvenidos a la sesión del GAC sobre uso indebido del DNS. Esta sesión tiene una duración programada de 60 minutos. En esta sesión continuaremos considerando las iniciativas de la organización y de la comunidad de la ICANN y también recibiremos información actualizada acerca de las novedades sobre este tema. Asimismo, continuaremos dialogando acerca de las posibilidades de que el GAC continúe trabajando con otras partes interesadas.

Como vemos en pantalla, tenemos un panel con distinguidos invitados. Tenemos oradores del grupo de trabajo sobre seguridad pública. Por ejemplo, Gabriel Andrews, de la Oficina Federal de Investigaciones; Cathrin Bauer Bulst, de la Comisión Europea y también copresidenta de nuestro PSWG; Lauree Kapin, de la Comisión Federal de Comercio de Estados Unidos, quien también es copresidenta de este grupo de trabajo, y por último Chris Lewis Evans, que también es copresidente de este

---

***Nota: El contenido de este documento es producto resultante de la transcripción de un archivo de audio a un archivo de texto. Si bien la transcripción es fiel al audio en su mayor proporción, en algunos casos puede hallarse incompleta o inexacta por falta de fidelidad del audio, como también puede haber sido corregida gramaticalmente para mejorar la calidad y comprensión del texto. Esta transcripción es proporcionada como material adicional al archivo, pero no debe ser considerada como registro autoritativo.***

---

grupo de trabajo y se desempeña en la Agencia Nacional de Lucha contra el Delito en el Reino Unido. El representante de Japón ante el GAC, Teruyuki se une a nosotros en forma remota. Le agradecemos mucho y esperamos que la zona horaria no sea un problema para usted en su país de origen. El señor Teruyuki trabaja en el Ministerio de Asuntos Internos y Comunicaciones.

Por último, pero no menos importante, por supuesto, tenemos a nuestro orador invitado, Graeme Bunton, del Instituto sobre Uso Indebido del DNS. Sin más, quiero darle la palabra a nuestro panel. Creo que Chris será quien comience.

CHRIS LEWIS-EVANS:

Muchas gracias, Manal. Hola a todos. Soy Chris Lewis Evans, de la Agencia Nacional de Lucha contra el Delito del Reino Unido. También soy copresidente del PSWG. Este tema del uso indebido del DNS es muy importante. Lo venimos tratando desde hace mucho tiempo y, como tenemos muy buenos oradores en el día de hoy, no quiero explayarme demasiado en aras del tiempo.

Quiero remarcar nuevamente la importancia de este tema para nosotros. Se ha hablado mucho acerca de las tendencias en lo que respecta al uso indebido del DNS. Vamos a tratar este tema y luego nuestro colega de Japón nos dará una presentación sobre el uso indebido del DNS en su país. Posteriormente tendremos

---

algunas perspectivas operativas y también se nos dará información acerca de iniciativas en curso y, por último, Graeme Bunton nos hablará acerca de una herramienta centralizada para el informe del uso indebido del DNS. También tendremos información acerca del rol de la ICANN y su comunidad. Ahora le doy la palabra a Lauren.

LAUREEN KAPIN:

Hola a todos. En esta oportunidad me pronuncio en mi carácter de uno de los copresidentes del grupo de trabajo sobre seguridad pública. Es un placer que estemos los tres copresidentes juntos en persona aquí hoy. Voy a comenzar con la pregunta de por qué es importante tratar este tema. Al hablar de la importancia de un tema a veces hay que comenzar con el qué de esta cuestión. El qué o el tema de fondo resultó ser algo que tiene muchas perspectivas. Sin embargo, hay definiciones de lo que constituye el uso indebido del sistema de nombres de dominio. El GAC compiló estas definiciones en un documento que es de suma utilidad. Tenemos una declaración del GAC sobre el uso indebido del DNS en la cual justamente recopilamos las distintas perspectivas de la comunidad.

Algunas de estas definiciones incluyen este concepto de amenazas a la seguridad que se originó con el asesoramiento sobre salvaguardas y medidas de protección que emitimos en

---

Pekín. Estas amenazas incluyen el phishing, el malware y los botnets. También se realizó la revisión de confianza, competencia y elección de los consumidores, y el equipo pertinente se centralizó en los problemas para los consumidores y trabajó con una definición en la cual el uso indebido del DNS está formado por actividades fraudulentas intencionales que son justamente perjudiciales para el DNS y sus usuarios.

También tenemos un informe con muy buena información acerca del uso indebido del DNS, su historia y demás información contextual. A veces creo que el concepto clave al hablar en el ecosistema de la ICANN es que todo trabajo que realicemos al respecto debe estar en consonancia con los estatutos de la organización. Con lo cual, el GAC se ha pronunciado en su declaración sobre uso indebido del DNS. Aquí tenemos enlaces para acceder a todos estos documentos que estoy mencionando.

Estas amenazas son amenazas que afectan al público, a los consumidores en línea como ustedes y como yo. Quizá todos nosotros. Afecta a nuestra confianza en el sistema de nombres de dominio. También afecta a las personas y a la infraestructura, a la resiliencia, a la seguridad y a la estabilidad de la infraestructura del DNS. Todo esto está plasmado en los

---

estatutos de la ICANN porque tiene que ver con el mandato de la ICANN.

Nosotros tenemos un grupo de trabajo sobre seguridad pública y allí tratamos este tema para ver el tema de la seguridad pública y tener un rol de asesoramiento al Comité Asesor Gubernamental para ser de ayuda en este tema. Con lo cual, en el 2015 creamos formalmente el PSWG y digo formalmente porque los encargados de cumplimiento de la ley y de protección al consumidor ya estaban trabajando sobre este tema pero creamos este grupo específico dentro del GAC para que se ocupara de estas cuestiones que son importantes.

No se trata solamente del GAC y del PSWG sino que también hay muchísimos grupos de partes interesadas en la comunidad de la ICANN para los cuales es prioritario combatir o mitigar el uso indebido del DNS. Quiero remarcar a los registros y a registradores en esta categoría también porque muchos de los actores, si no todos, entre las partes contratadas realmente se preocupan mucho acerca de su reputación, de sus clientes y por eso quieren trabajar y trabajan de forma voluntaria para mitigar esta cuestión.

Tenemos un alto grado de unanimidad y concordancia en tanto que podemos mejorar la manera en que gestionamos este problema. Esta mañana en el PSWG tuvimos una sesión con

---

algunos colegas de la ICANN y estos colegas reconocieron que los contratos que abordan esta cuestión son los cimientos o la base de nuestras expectativas en cuanto a las respuestas de las distintas entidades frente al uso indebido del DNS y por supuesto hay lugar para mejoras.

Este tema es objeto de mucha atención en este momento y hay mucho trabajo por hacer. El tema de los contratos específicamente es muy importante porque son las reglas del juego en el ecosistema de la ICANN en cuanto a lo que debe suceder y la junta directiva de la ICANN y el equipo de cumplimiento contractual de la ICANN reconocen que sí se pueden mejorar los contratos actualmente vigentes dado que no tienen la claridad suficiente y por lo tanto no generan obligaciones con el grado suficiente de exigibilidad.

Esto lo vemos en los distintos debates en la comunidad, en reuniones pasadas, en declaraciones también. Hay correspondencia de la junta directiva. Por ejemplo, del 12 de febrero de 2020 en la cual se reconocen brechas existentes en los contratos vigentes que generan inconvenientes para el equipo de cumplimiento contractual de la ICANN. Esto fue objeto por ejemplo del equipo de revisión del CCT, el equipo de revisión de WHOIS y también el equipo de revisión de seguridad y estabilidad. Además, también está dentro del alcance del PDP

---

sobre procedimientos posteriores a la introducción de nuevos gTLD.

Con esto les acabo de explicar a grandes rasgos por qué es importante este tema y también que la comunidad reconoce que hay trabajo por hacer. Además, hay distintos grupos de trabajo y equipos de revisión que también reconocen que hay cuestiones específicas o acciones específicas que se pueden implementar para incrementar la seguridad del sistema del DNS y que no sea objeto de uso indebido. Ahora lo que voy a hacer es pasarle la palabra a Gabe.

GABRIEL ANDREWS:

Hola. Soy Gabriel. Quiero seguir hablando acerca de la importancia de este tema para el GAC. El PSWG le ha informado al GAC previamente acerca de las formas más comunes de uso indebido del DNS como por ejemplo ransomware o correos electrónicos comprometidos y que esto comienza por el phishing, para captar a las víctimas. En otras palabras, lo que hacemos aquí para luchar contra el uso indebido del DNS, como por ejemplo el phishing o la diseminación de malware, esto ayuda a proteger a todos nuestros ciudadanos contra las características o las clases de delitos cibernéticos más comunes que existen hoy en día. Tenemos la herramienta de WHOIS, por ejemplo, que utilizamos cuando hay que vincular una

---

registración de nombre de dominio a un registratario. Esto existe debido a las políticas de la ICANN que son sostenibles a día de hoy.

Pasemos ahora a las novedades acerca del uso indebido del DNS y al informe sobre tendencias. Como muchos miembros del GAC sabrán, la organización de la ICANN publicó recientemente un informe que se llama: “Los últimos cuatro años en retrospectiva: Breve reseña de tendencias en el uso indebido del DNS”. Para hacer este informe, la ICANN tomó muchísimos dominios que están en listas de bloqueo de reputación en las cuales se incluyen los dominios maliciosos que por ejemplo utilizan spam, phishing, entregan malware o utilizan comando y control de botnets. Es decir, los malos actores.

La ICANN quiso ver cuáles son los dominios o la cantidad de dominios en esas categorías y ver si había alguna tendencia observable. Sí, la respuesta fue que sí y publicaron este informe. Nosotros leímos este informe con sumo interés porque para nosotros es realmente crítico entender todos estos hechos al hablar sobre uso indebido del DNS y obviamente vemos que los dominios dentro de la categoría de spam son mucho más que los dominios en las otras categorías.

Como sabemos, hubo una disminución de estos dominios a lo largo del tiempo. Desafortunadamente, dado el alto volumen de

---

spam a veces el ojo humano no puede discernir cuáles son las otras categorías y tendencias. Así que nosotros utilizamos distintos colores. Creo que el azul representa el phishing y el amarillo representa el malware. Es difícil visualmente ver las tendencias. No creo que podamos llegar a una conclusión solamente con esta información pero los autores de este informe fueron muy generosos y amables y se ofrecieron a compartir los datos que utilizaron para confeccionar este informe y así pudimos ver individualmente cada tendencia dentro de cada categoría para comparar phishing con malware, etc.

Esto es importante porque se utilizan estas acciones o actividades para comprometer distintos dominios. Por ejemplo, vemos el ransomware que utiliza phishing para captar a sus víctimas y luego pedir un rescate dinerario a cambio. Además, y por último, quiero decir que la ICANN en sus informes indica que intentará determinar las causas de las tendencias en estos dominios y en las categorías. Quizá esto lo incluyan en un próximo informe. Con esto lo que quiero decir es que no estamos listos todavía para llegar a una conclusión pero esperamos a futuro tener más detalles para interiorizarnos con este tema. Gracias.

---

LAUREEN KAPIN: Creo que ahora tiene la palabra nuestro colega de Japón. Vamos a darle la palabra. Vamos a colocar en pantalla su presentación para que él nos pueda dar su exposición en este momento.

TERUYUKI SHIBATA: ¿Puedo tomar la palabra?

MANAL ISMAIL: Sí, sí. Por favor, adelante.

TERUYUKI SHIBATA: Buenos días, buenas tardes, buenas noches. Soy Teruyuki Shibata, del Ministerio de Asuntos Internos y Comunicaciones de Japón. Quisiera expresar mi agradecimiento por esta oportunidad de poder compartir esta información de mi país, de Japón. En reuniones previas de la ICANN también hablamos acerca de problemas que afectan a los registradores y a otros actores en lo que respecta al uso indebido del DNS. Ahora quiero hablar acerca de las tendencias recientes y sobre todo en cuanto al incumplimiento de leyes de derecho, de propiedad intelectual.

Como podemos ver en este diagrama a la izquierda, más de la mitad de estos dominios tienen que ver con esta actividad maliciosa. Vemos que algunos dominios o sitios web fueron cerrados o dejaron de funcionar o se evitó que siguieran

---

funcionando. Luego, como vemos en el diagrama a la derecha, vemos que se concentra esta actividad maliciosa en unos pocos registradores. Tres de ellos.

Por ejemplo, tuvimos una reunión con un registrador y este registrador no estaba al tanto de que había actividad maliciosa en los dominios que estaban bajo su ámbito. Queremos proponer una sugerencia para abordar esta problemática y evitar o prevenir el uso indebido de nombres de dominio y registraciones.

Primero trabajar con la ICANN, con los registradores. Según el acuerdo de acreditación de registradores, es necesario tener el nombre, la dirección postal y el número telefónico de los registratarios. Los registradores también tienen que verificar si esta información es correcta. Por ejemplo, vemos que a veces hay que verificar la información de los registratarios. Como acción a largo plazo queremos...

*Los intérpretes pedimos disculpas pero por momentos el audio del orador no es lo suficientemente claro como para hacer una interpretación precisa.*

Además, queremos proponer que el equipo de cumplimiento contractual de la ICANN continúe realizando sus auditorías correspondientes. Es importante ver qué puede hacer la ICANN

---

para mejorar la situación en este ecosistema. Espero que continuemos tratando este tema en las reuniones del GAC. Siguiendo página, por favor. Siguiendo diapositiva, por favor. Gracias.

Nos gustaría compartir un concepto. Libre flujo de datos con confianza. Este concepto se creó en la reunión de Davos de 2019 y también en la reunión del G20 en Osaka. Es decir, libre flujo de datos facilitado por los actores pertinentes pero con confianza. Es decir, fortalecer la confianza abordando los desafíos en materia de privacidad, protección de datos, propiedad intelectual, derechos de propiedad intelectual para facilitar justamente el libre flujo de datos.

Queremos compartir este concepto y queremos compartir tres factores. Libertad de expresión, libre flujo de la información, confiar en la información, tener información confiable y tener una Internet global y segura. Esperamos que este concepto sea de su agrado también y con esto les agradezco mucho esta oportunidad de participar. Gracias.

CHRIS LEWIS-EVANS: Muchas gracias por su presentación. Si podemos pasar a la próxima diapositiva. Ahora vamos a hablar de algunas perspectivas operativas, algunas iniciativas que se están

---

realizando en la comunidad. La Comisión Europea nos dio la oportunidad de reunirnos con algunos colegas de organismos de cumplimiento, Europol, y esto fue muy útil. Tuvimos diálogos interesantes en relación con el uso indebido del DNS y los desafíos que enfrentan los organismos de cumplimiento en este tema, en este campo.

Los ítems que tratamos no tienen que ver solamente con interrumpir o desarmar las entidades delictivas que causan el uso indebido del DNS sino también se trata de identificar y proteger a las víctimas de los ciberdelitos, del fraude y de todo lo que se lleve a cabo dentro o a través de Internet, y que altera o modifica la confianza en Internet.

Después hablamos sobre las tendencias. Uno de los puntos mencionados en esa reunión es que la reducción en la cantidad de dominios no nos da una imagen realista de lo que está sucediendo en relación al uso indebido del DNS. Tendríamos que ver en realidad los daños causados, la cantidad de víctimas, la cantidad de informes sobre ciberdelitos. Esta es información que la ICANN puede recabar a través de sus métodos de conseguir información y esto se puede compartir con otras organizaciones.

Vamos a ver entonces cómo podríamos agregar información a las estadísticas sobre el uso indebido para ver en qué medida son efectivas las medidas que se han tomado o que se están

---

tomando, si pueden afectar el uso indebido del DNS y si contribuyen a la reducción de ese uso indebido.

No sé si los otros copresidentes del PSWG, si tienen buenas estadísticas o informes sobre organizaciones que recaban estos datos. Por supuesto, nos gustaría recibir esa información. Europol va a darnos su información sobre esto y otros países también me van a dar información sobre este punto. Presentaremos esta información en una próxima reunión de la ICANN.

Hablando ahora de iniciativas actuales y futuras, una de las iniciativas de la ICANN completada recientemente, y me cuestan las siglas así que voy a decir la palabra completa, es el Grupo de Análisis Técnico para Iniciativas de Facilitación de la Seguridad en el DNS, DSFI-TSG. Una de las cuestiones aquí importantes es la recomendación cinco que habla acerca de una plataforma para compartir información. Esto es algo que los grupos que trabajan en seguridad pública están acostumbrados a utilizar. Hay muy buenos ejemplos de esto en las instituciones financieras que tienen una muy buena plataforma para compartir información y centros de evaluación. Esto permite que se comparta información sobre las amenazas que se ven, sobre las tendencias que se observan, sobre las formas en que pueden abordar y reducir el uso indebido y también aquí se comparten

---

mejores prácticas. Creemos que esta recomendación es un buen paso adelante para crear una plataforma de ese tipo dentro de la ICANN con las partes contratadas y también para otras unidades constitutivas. Todos deberíamos trabajar juntos para abordar el uso indebido del DNS y creemos que esta es una de las principales recomendaciones surgidas de este informe del grupo para el análisis técnico que mencioné.

Graeme va a hablar sobre otra herramienta. No voy a hablar mucho de lo que él va a decir pero hay algunos marcos voluntarios muy buenos que se han desarrollado. Todos tendrán un impacto positivo en nuestra capacidad de reducir o abordar el uso indebido. Sin embargo, hay algunas limitaciones. No la de Graeme específicamente sino en general, todas tienen esta limitación, este limitante. No necesariamente se aplican a todas las partes contratadas. Todavía creemos que es necesario mejorar las cláusulas de los contratos y trabajar más en el tema de las políticas para que esto se aplique a todas las partes contratadas a fin de poder abordar efectivamente el uso indebido del DNS. Dicho esto, Graeme, le doy la palabra.

MANAL ISMAIL:

Veo que Kavouss levantó la mano en el chat. ¿Es un buen momento para hacer preguntas o comentarios? Kavouss, adelante.

**IRÁN:** Muchas gracias. En primer lugar quiero agradecer a la ICANN por el informe con respecto a este tema tan importante. Yo realmente aprecio todos los esfuerzos y toda la información que nos dieron. Señora Presidenta, le pido amablemente que tome este informe en cuenta para nuestras acciones futuras, en especial en lo que se refiere a todo asesoramiento futuro o seguimiento que se haga en relación a los asesoramientos del GAC sobre el uso indebido porque en este informe están algunas de las cuestiones que nos preocupan y no vamos a repetir lo que ya dijimos de esta manera. Ahora ya tenemos algunas respuestas. Creo que en gran medida este informe nos puede ser útil y le pido amablemente que tome en cuenta este informe cuando estemos redactando el comunicado o cuando definamos alguna acción de seguimiento en relación a un comunicado anterior. Muchas gracias.

**MANAL ISMAIL:** Muchas gracias, Kavouss. Tomo nota de esto. También quisiera pedirles a todos que se fijen en lo que se está escribiendo en el chat. Veo que alguien levantó la mano, una persona de Indonesia. Ashwin, le damos la palabra.

---

INDONESIA: Muchas gracias. Trabajo en el área de seguridad del DNS. Es muy importante este tema. Es cada vez más importante porque dependemos mucho más de la Internet por el problema del COVID-19. Mi comentario es el siguiente. ¿Sería posible que el equipo de seguridad de la ICANN o el grupo que trabaja en el uso indebido de DNS trabaje más en cooperación con la UIT? Como ustedes sabrán, la UIT también tiene una agenda sobre ciberseguridad global que preparó hace varios años.

IRÁN: ¿Está hablando usted de la pregunta 5 o de otra pregunta?

INDONESIA: No tiene exactamente que ver con la pregunta sino que es algo...

IRÁN: Señora Presidenta, todas las sugerencias me parecen bien pero...

MANAL ISMAIL: Kavouss, tiene la palabra la persona de Indonesia.

IRÁN: No he terminado. Perdón. ¿Me escucha, señora Presidenta?

---

MANAL ISMAIL: Por favor, Kavouss.

IRÁN: [inaudible].

MANAL ISMAIL: Le pedimos disculpas, Ashwin. Adelante.

INDONESIA: Quizá una mejor cooperación nos dé una mejor ciberseguridad porque la UIT también habla de una agenda global de ciberseguridad. Ya la preparó hace varios años. También se trató esto en una reunión en 2012 en Dubái y el objetivo es mejorar la gobernanza de Internet. Al mejorar la gobernanza, mejorará la ciberseguridad. Quizá, como ahora estamos más preocupados por la ciberseguridad, este tipo de cooperación que menciono podría volver a considerarse. Muchas gracias.

MANAL ISMAIL: Muchas gracias, Ashwin. Veo ahora una mano levantada del grupo de los Estados Unidos. Susan, le doy la palabra.

---

ESTADOS UNIDOS:

Gracias, señora Presidenta. Quiero agradecer a los copresidentes del grupo de trabajo para la seguridad pública por la maravillosa y completa presentación que han hecho. Nosotros creemos que las soluciones para abordar el uso indebido del DNS pueden tomar la forma de mejores y más exigentes requerimientos contractuales.

Chris mencionó que las iniciativas voluntarias son diferentes de los requerimientos de los contratos y de los programas de cumplimiento que se aplican a todos los registradores. También creemos que las soluciones pueden incluir los incentivos para lograr métricas antiabuso y procesos de desarrollo de políticas. Desde el punto de vista del USG y los debates que hemos tenido sobre el uso indebido del DNS, aparentemente hay una ecuación. A veces se compara o se considera que el uso indebido del DNS es todo lo que sea perjudicial en Internet o dañino en Internet pero las actividades dañinas e ilegales en relación al contenido están fuera del mandato de la ICANN. Sin embargo, creo que es un tema que debe ser abordado con urgencia a través de algún proceso específico, buscando soluciones colaborativas como por ejemplo las iniciativas que trabajan con notificadores de confianza. Muchas gracias.

---

MANAL ISMAIL: Muchas gracias, Estados Unidos. Veo otra mano levantada. Adelante, por favor.

PAÍSES BAJOS: Muchas gracias, señora Presidenta. Quiero decir algo con respecto a la agenda global de ciberseguridad. Lo que mencionó Ashwin antes sería bueno ver la posibilidad de trabajar juntos con otras organizaciones pero igual creo que debemos encontrar una solución aquí interna dentro del modelo de múltiples partes interesadas. Ya sé que se trató de este tema en 2012. Habría que ver qué pasó con esto y además esto fue hace 10 años. El mundo cambió mucho desde entonces. Gracias.

MANAL ISMAIL: Muchas gracias. No veo que nadie más haya pedido la palabra. Graeme, le doy nuevamente la palabra y me disculpo por haberlo interrumpido.

GRAEME BUNTON: Gracias, Manal. Gracias a todos por permitirme estar aquí hoy. Realmente estoy muy entusiasmado por poder hablar sobre el lanzamiento de NetBeacon. Tengo algunas diapositivas pero el mensaje clave es este. DNS Abuse Institute con el apoyo de CleanDNS y PIR ha lanzado un servicio centralizado de

---

notificación de uso indebido de DNS cuyo objetivo es simplificar el proceso de notificación del uso indebido del DNS y brindar valor a los registros y registradores para que sea más fácil para ellos actuar en los casos de uso indebido.

Ahora les voy a dar más información. El DNS Abuse Institute fue creado el año pasado. Tiene una misión sin fines de lucro. Ustedes saben que el uso indebido del DNS es un problema global complicado y que mitigarlo es difícil. Debemos trabajar en forma coordinada y centralizada para reducir el uso indebido del DNS. Por eso se creó este instituto, para combatir el problema, reducir el uso indebido y trabajar en forma coordinada dentro del DNS.

NetBeacon, el servicio centralizado de notificación del uso indebido, responde a una serie de actividades de la comunidad. SSR2, recomendación 13.1 habla de la creación de un portal centralizado para notificación. SSAC 115 también hace referencia a este tema. Incluso el informe CCTRT habla de un proyecto similar a este. El instituto consideró los problemas para resolverlos y tratamos de ver dónde podíamos hacer una diferencia.

Hay dos problemas fundamentales en la notificación de uso indebido, o había en el pasado. Notificar el abuso es difícil. Aquellos que trabajen en el área de ciberseguridad o en

---

organismos de cumplimiento de la ley saben que es muy difícil notificar el abuso en todo el ecosistema. Para los usuarios finales es muy difícil. Más difícil porque hace falta conocimientos técnicos, identificar un registrador, encontrar la página donde se informa el uso indebido. Hay que mandar las pruebas, la evidencia. Realmente es algo muy difícil.

Por otro lado, y algo que muchas veces no se toma en cuenta, es que los informes de uso indebido de los registros y registradores en general son complejos. No tienen una buena estructura, no tienen evidencia. A veces se da información sobre dominios que no pertenecen a ese registro o registrador. Muchas veces se crean tickets que tienen poco valor y la Internet no se vuelve más segura. Creíamos que había una solución para esto que podría estar en el medio para resolver los dos problemas al mismo tiempo. Esa solución es NetBeacon. La próxima diapositiva, por favor.

Es una herramienta gratuita. Es gratuita para enviar las notificaciones. Es gratuita para los registros y registradores. Acepta informes sobre uso indebido del DNS. En el caso de phishing, botnets, spam, toma esas notificaciones de uso indebido de manera estandarizada. Estandariza el formato. Enriquece los informes. No solamente tomamos lo que nos envían los usuarios finales sino que tomamos ese nombre de

---

dominio, esa URL, y lo verificamos con una serie de fuentes que dan inteligencia sobre dominios, a ver si averiguan más sobre el dominio, si también hay otros informes de que participen en actividades ilegales. Después agregamos esto a la notificación de uso indebido y esto es importante porque aquí hay un incentivo para que los registros y registradores utilicen esta herramienta porque ahora están recibiendo más información y parte del trabajo de investigación ahora la hace el servicio mismo. Reducimos la barrera para actuar que enfrentan los registros y registradores porque recibe notificaciones de uso indebido estandarizados. Todo lo que tienen que hacer en ese momento es decidir si es algo perjudicial o no y cómo responder. Otra funcionalidad clave es que distribuimos esta información en forma automática. El denunciante no tiene que averiguar adónde mandar el informe. Lo definimos nosotros y lo hacemos por el denunciante. La próxima diapositiva.

Esto es importante para entender la escala del problema que encaramos. Hay uso indebido del DNS. En toda la Internet se descubre parte de esto en las listas de bloqueo de reputación que se utilizan para medir el uso indebido del DNS pero hay un subgrupo de uso indebido informado en forma manual y esto es lo que lleva mucho tiempo y trabajo a los registros y registradores. Dedicar mucho tiempo a analizar todo esto y el valor no es muy grande. Tratamos de apuntar a este conjunto de

---

usos indebidos con nuestra herramienta NetBeacon. La próxima diapositiva, por favor.

Este es un ejemplo de un informe sobre phishing. Si entran a NetBeacon, pueden entrar a [netbeacon.org](http://netbeacon.org), y pueden crear un informe para un caso de uso indebido por phishing. Es muy fácil de utilizar. Es sencillo. Aquí se pide claramente la información. Creemos que la herramienta es muy buena y fácil de utilizar para la mayoría de los usuarios.

Aquí hay algo de fricción. A algunas personas no les gusta utilizar formularios pero lamentablemente el texto libre no sirve para trabajar en Internet. Los registros y los registradores necesitan información más estructurada para actuar correctamente. Además, necesitamos una dirección de correo electrónico que funcione. Tienen que ver que tienen una dirección de correo electrónico válida para enviar estos informes porque nosotros somos intermediarios. Estandarizamos la información y la mandamos a donde tiene que llegar. Si el registro o el registrador necesitan más información, tienen que poder ponerse en contacto con el denunciante. No pueden mandar denuncias de uso indebido en forma anónima. La próxima diapositiva, por favor.

Otras características. Hay una API para enviar los informes. Los organismos de ciberseguridad, las autoridades de aplicación de

---

la ley, los usuarios finales, todos pueden mandar estos informes. Todavía no tenemos claras las reglas ni la cantidad de información que se enviará pero queremos tener una buena calidad en las denuncias de uso indebido para que los registros y registradores la vean como una herramienta valiosa.

También hay una API para el consumo de informes, para que los registros y registradores puedan utilizar estos informes, no solamente por correo electrónico sino que los puedan subir a sus sistemas generales. Estos formularios son embebibles. Todo el mundo puede incluir estos formularios en sus sitios web, ver toda la información, aprovechar el valor de la información adicional que proveemos sin tener que volver a reprogramar y recrear todo. La próxima diapositiva, por favor.

Esto es importante porque debemos explicar qué es esta herramienta y qué no es. No es una herramienta de gestión de uso indebido. Los registros y registradores van a recibir estos informes en sus sistemas. Ya puede ser por correo electrónico, un sistema de tickets o una solución comercial. No es un lugar donde van a entrar para gestionar sus reclamos por uso indebido. Tampoco hace determinaciones. Siempre dependerá del registro o registrador que es el responsable de definir en última instancia si esto es uso indebido y cómo responder.

---

Tampoco estamos creando un depósito o repositorio de reclamos de uso indebido porque es un riesgo para el instituto y, además, a los registros y a los registradores no les gustaría que nosotros tengamos guardada su ropa sucia durante mucho tiempo. Tampoco estamos dando acceso a la información de los registratarios. Los registros en general ya tienen esta información. No la necesitan para mitigar el uso indebido. Estamos tratando de reducir el uso indebido. No estamos tratando de obtener acceso a información general.

Tenemos una agenda bastante ambiciosa para este servicio. Queremos crear una herramienta robusta, centralizada, que sea un bien público, que haga más segura la Internet. Esto debe ser útil para los ccTLD, los proveedores de servicios de correo electrónico, los proveedores de servicios generales. Queremos recibir la información y enviarla hacia donde debe llegar. De esta manera podremos tener vías de escalamiento. Esto puede ser informado a una empresa de hosting y después podemos mandarlo al registrador cuando corresponda. El mejor ejemplo de esto sería sitios web que han sido comprometidos. Ir en primer lugar a la capa de DNS no sirve. Mandamos esto primero al que tiene el hosting, a ver si el hosting hace algo y, si no, seguimos escalándolo.

---

La idea es llegar a la reputación del denunciante. Las personas que denuncian el uso indebido y lo hacen a nivel comercial y quieren demostrar que son buenos denunciando el uso indebido en NetBeacon hay un tercero objetivo que demuestra que son buenos denunciantes. Además, la idea es tener seguridad de que las personas que denuncian los usos indebidos lo hacen de buena fe y con un trabajo de calidad. Queremos llegar a esto también.

Algunas preguntas frecuentes. ¿Es fácil de utilizar esta herramienta para los usuarios finales? Sí. Probablemente tengamos que trabajar un poco más para mejorar la experiencia del usuario final pero creo que hoy por hoy casi todo el mundo puede usar esta herramienta. Hoy solo está en inglés. Deberemos mejorar un poco el texto y lo traduciremos para que esté disponible en todo el mundo.

Muchas veces me preguntan si vamos a publicar datos que pasan por el sistema, informes, por ejemplo. La respuesta breve es probablemente compartiremos estadísticas generales pero creemos que la adopción de esta herramienta es más importante que hacer pasar vergüenza a los registradores que reciben muchas denuncias por uso indebido. El DNS SI tiene una herramienta específica que será más robusta para responder a esta pregunta en particular.

---

Cierre y notificaciones. Nosotros no podemos cerrar los tickets de los registradores. Esto depende del registrador. Todavía se puede trabajar en cuanto a la gestión de expectativas en esta comunidad y espero que esto se trate.

Otra pregunta frecuente que hay que agregar aquí sería: ¿Los registradores deben inscribirse aquí? No. Los registradores están obligados a tener un contacto público para denuncia de uso indebido y ahí mandamos la información nosotros. Los registradores obtendrán más valor de este servicio si ellos crean una cuenta pero no es indispensable que lo hagan. La próxima diapositiva, por favor.

Esto también es una pregunta frecuente. ¿Por qué hacemos esto nosotros? Creo que es importante responder a esta pregunta. Cuando se considera el uso indebido y cómo se denuncia en Internet rápidamente se ve que para hacerlo de manera efectiva es necesario trabajar no solamente con los registros y los registratarios. Hay que trabajar con otros actores en la infraestructura de Internet. Esto va más allá del ámbito de acción de ICANN. Creemos entonces que siendo un miembro respetado de esta comunidad estamos muy bien preparados y posicionados para brindar este tipo de servicio.

Hay otro punto aquí con respecto a los registradores, registros y las empresas de hosting. Tienen muchos lugares donde se puede

---

denunciar el uso indebido. Si esto fuera una iniciativa de ICANN solamente, terminaríamos bifurcando los procesos de denuncia de uso indebido y esto crearía confusión para los usuarios finales y aquellos que denuncian el uso indebido.

Apoyar el trabajo. Antes di una definición de este proyecto. Trabajamos con el proyecto de jurisdicción de la Internet. Muchas gracias a ellos. También PIR ha apoyado al DNS Abuse Institute y CleanDNS ha sido un socio muy generoso. Han donado la tecnología y también las horas de desarrollo para personalizar todas estas herramientas. Gracias a todos ellos. La próxima diapositiva, por favor.

Esto está en vivo. Todo el mundo lo puede visitar. Ya pueden crear una cuenta. Si quieren denunciar un uso indebido, háganlo. Siempre me interesa ponerme en contacto con organizaciones que quieren reducir y eliminar el uso indebido del DNS. Muchas gracias. Si hay alguna pregunta, con mucho gusto les voy a responder. Muchas gracias por su tiempo.

MANAL ISMAIL:

Ya veo que alguien solicita la palabra en la sala de Zoom. Adelante, por favor. Disculpe si estoy pronunciando mal el nombre de la persona que solicita la palabra. Posteriormente Nigel, del Reino Unido.

ORADOR DESCONOCIDO: Hola. Soy del Reino Unido. Muchas gracias. Muy buena la presentación. Quisiera saber si los titulares de nombres de dominio pueden recibir informes de NetBeacon. Por ejemplo, nuestro dominio tiene mucho valor y es sujeto de muchos ataques. Para nosotros sería de utilidad ver cuáles son los dominios que están registrados con fines maliciosos. ¿Podría ser posible que nosotros tuviéramos información de lo que ustedes reciben en sus informes con respecto a nuestro nombre de dominio también?

GRAEME BUNTON: Muchas gracias. Su pregunta es muy interesante. No es muy frecuente. No tenemos esa funcionalidad todavía. Creo que es un problema interesante el que usted plantea. Necesitamos una herramienta un poco más sofisticada para cumplir con ese objetivo. Lo voy a agregar a la lista de herramientas a desarrollar y lo tendremos en cuenta. Muchas gracias.

MANAL ISMAIL: Adelante, Nigel, de Reino Unido. Tiene la palabra.

---

REINO UNIDO: Muchas gracias. Muchísimas gracias, Graeme, por esta presentación y gracias a todos los panelistas. Especialmente quiero agradecer a Graeme por este trabajo que realiza en esta institución, DNS Abuse Institute.

IRÁN: Disculpe, señora Presidenta. Tengo una propuesta.

MANAL ISMAIL: Kavouss, Kavouss, por favor, Kavouss. Kavouss, por favor, en este momento hay un colega que está tomando la palabra. Usted lo está interrumpiendo. Por favor, aguarde a que finalice Nigel y luego le daré la palabra a usted. Gracias. Disculpe, Nigel. Disculpe por la interrupción. Adelante.

REINO UNIDO: No, no. Por favor, por favor. No hay problema, Kavouss. Ahora perdí el hilo de lo que estaba diciendo pero quería agradecerle a Graeme por su trabajo con NetBeacon. Realmente es muy, muy positivo y lo digo de verdad. Contar con toda esta información realmente es algo muy, muy bueno.

Ahora tengo una pregunta. Creo que usted ya trató este tema en parte pero usted ha trabajado arduamente para analizar la información y lo que le indican al registrador correspondiente,

---

etc. Por supuesto, en última instancia hay que tomar una decisión acerca de qué hacer una vez que se recibe esa información. Nos intriga a nosotros como gobiernos también ver que haya un resultado positivo y creo que es un término un tanto subjetivo decir resultado positivo. Qué pasó con el dominio, si se lo dejó fuera de uso, etc.

GRAEME BUNTON:

Muchas gracias, Nigel. Agradezco sus palabras tan amables. Bien. Estamos tratando de hacer una medición de los resultados de los informes de uso indebido. Puede ser un tanto complejo. A lo mejor el informe era incorrecto o no era exacto. De todas maneras, lo estamos investigando en parte porque queremos demostrar que este servicio funciona y que facilita una Internet más segura. Eso es algo que estamos analizando.

MANAL ISMAIL:

Muchas gracias. Kavouss ha solicitado la palabra. Luego el representante de Ruanda y luego creo que tenemos que ir cerrando esta sesión porque se nos está acabando el tiempo. Kavouss, adelante, tiene la palabra. Por favor, les pido a todos que levanten la mano para ayudarme a identificar quiénes quieren tomar la palabra. Muchas gracias. Adelante, Kavouss.

---

Kavouss, ¿me puede oír? Bueno, entonces le doy la palabra al representante de Ruanda.

RUANDA:

Muchas gracias al representante del DNS Abuse Institute. Agradezco su presentación. Si me permite, necesito una aclaración. ¿Tiene alguna iniciativa para ayudar a los países en desarrollo a abordar el uso indebido del DNS? ¿Tienen iniciativas de capacitación? Como saben, muchos países no tienen DNSSEC en sus ccTLD. Creo que sería recomendable cooperar o que haya cooperación entre los registros de ccTLD para capacitar a los ingenieros y a los actores correspondientes para que implementen DNSSEC y de esa manera aumentar la seguridad del sistema de nombres de dominio. También tengo una pregunta acerca de la frecuencia de publicación. No sé si se trata de un informe anual o con qué frecuencia lo publican. Muchas gracias.

GRAEME BUNTON:

Muchas gracias por su pregunta. Con respecto a la capacitación, en nuestro instituto justamente difundimos mejores prácticas para registros y registradores, para usuarios finales, para que su sitio web sea seguro y para reducir el uso indebido del DNS. Tenemos iniciativas de capacitación y continuaremos

---

trabajando al respecto. Con todo gusto trabajaré con usted en estas iniciativas. También me había preguntado con respecto al informe. No sé qué tipo de informe vamos a publicar en NetBeacon pero espero que en agosto o septiembre ya empecemos con nuestras publicaciones y que sean mensuales.

MANAL ISMAIL:

Muchas gracias. Creo que la representante de Estados Unidos solicita la palabra y creo que nos quedan dos diapositivas todavía en la presentación. Le pido a la representante por favor que sea muy breve.

ESTADOS UNIDOS:

Gracias, señora Presidenta. Gracias, Graeme, por la presentación. Estados Unidos es consciente de la iniciativa de NetBeacon para informar acerca del uso indebido del DNS y queremos estar al tanto de mayores iniciativas en cuanto a NetBeacon y a su implementación para cuando lleguemos a la reunión ICANN75, específicamente sobre informes acerca de uso indebido del DNS porque para Estados Unidos es necesario tener mayor y más frecuente información con mayor nivel de detalle para ver cuáles son los tipos de uso indebido del DNS que se están midiendo y también tener datos sin procesar en todos estos informes. Muchas gracias.

---

**GRAEME BUNTON:** Muchas gracias por sus palabras. Usted es muy amable. Quiero mencionar que el servicio ya está operativo. Ya se ha informado acerca de un dominio malicioso y ese dominio ya no está funcionando en Internet. Vemos que esto es muy positivo. Tenemos esperanzas a futuro.

**MANAL ISMAIL:** Muchas gracias, Graeme. Cathrin, muchas gracias por su paciencia.

**CATHRIN BAUER-BULST:** Muchas gracias. También le agradecemos mucho a Graeme por su trabajo. Quiero decir que soy Cathrin Bauer Bulst. Soy de la Comisión Europea. Estoy muy contenta de estar aquí, con todos los colegas del GAC. Vamos a volver ahora al rol de la ICANN. ¿Cuál es el rol de la ICANN y cuál debería ser ese rol? Hemos avanzado mucho acerca de la transparencia en materia del uso indebido dentro y fuera de la ICANN. La ICANN tiene la iniciativa DNSTICR y la iniciativa DAAR. Vemos que hay que utilizar la tecnología, la automatización para que todo el ecosistema sea más eficiente en la lucha contra el uso indebido.

---

Volviendo a lo que ha dicho Lauren acerca de los contrato de la ICANN, hoy en día la ICANN fácilmente puede actuar cuando un registrador está incumpliendo su contrato. De esta manera puede contribuir a una infraestructura de Internet que sea más segura. Vemos que esto quizá no refleja plenamente la misión de la ICANN y vemos que la comunidad se hace eco de esta postura. Sabemos que es necesario trabajar aún más y con todo gusto le damos la bienvenida a estas iniciativas de la industria, más allá de la ICANN.

Tenemos que hablar acerca de la información y de la transparencia y de compartir la información, que es clave. Ahora entendemos mejor cuáles son los factores que impulsan a toda esta iniciativa para, de esta manera, poder apoyar a registros y registradores en sus acciones. Al mismo tiempo, las autoridades de seguridad pública y otros entes que realizan investigaciones tienen que tener en cuenta los impactos humanos y económicos del uso indebido del DNS. Esto está en consonancia con el rol de la ICANN definido en sus actas constitutivas y estatutos.

Podemos generar transparencia pero para eso necesitamos incentivos porque, en definitiva, actuar para combatir el uso indebido del DNS tiene un costo, incluso si se trata de una manera reactiva. Tenemos que pasar a ser proactivos. Siempre decimos que no siempre son las partes contratadas las que

---

contribuyen siempre con la ICANN las que menos participan. Vemos que muchas de las que contribuyen a la ICANN ya quieren hacer más todavía y participan activamente, pero qué pasa con las que no participan activamente, como lo ha demostrado nuestro colega de Japón. Por ejemplo, hay registradores que no están conscientes de tener un problema o de lo que podrían hacer. Por supuesto que necesitamos capacitación al respecto pero al mismo tiempo necesitamos incentivos. Tenemos que modificar los contratos también. Laureen ahora nos va a hablar acerca de las brechas existentes y de los posibles pasos que puede tomar el GAC. Muchas gracias.

LAUREEN KAPIN:

Muchas gracias. Última diapositiva. Soy consciente de que ya nos hemos excedido del tiempo programado para esta sesión. Muy bien. Vamos a ver ahora que si algo no está especificado en un contrato no se lo puede exigir. Tenemos que ver cuál es el contenido actual de los contratos y si se lo puede mejorar porque las facultades de cumplimiento contractual de la ICANN surgen de los contratos. Vemos que hay una disposición que tiene que ver con los compromisos en materia de interés público en el acuerdo base de registro-registrador. Vemos que esa disposición tiene que ver con la distribución de malware, con los botnets.

---

Vemos el texto en pantalla. Esto está tomado directamente de un contrato y uno quizá pueda pensar que todos estos comportamientos son prohibidos y, si sucede alguno de estos comportamientos, podemos actuar al respecto pero no. Esta prohibición no tiene esta naturaleza. Simplemente los registros tienen la obligación de decirles a los registradores que se tienen que asegurar de incluir esta prohibición en su contrato con los compradores finales. Vemos en esta relación contractual que la ICANN y los registros tienen una promesa mutua de plasmar este requisito en el contrato entre registrador y registratario pero el registro no tiene la obligación de cerciorarse de que el registrador cumpla con esta obligación o que tome tal o cual acción, con lo cual vemos que estos son temas que deben ser tratados en el marco de una pregunta que es cómo generar disposiciones de cumplimiento efectivo para mitigar el uso indebido del DNS.

Esto se tiene que conversar porque no depende solamente del Comité Asesor Gubernamental, de resolverlo de manera aislada. Ni tampoco depende de otro grupo en particular. Ya vemos cómo resolver al uso indebido del DNS y tenemos que ver cómo mejorar los contratos en esta materia. Esto se tiene que tratar en un diálogo, sobre todo con las partes contratadas que tienen su realidad comercial y empresarial. Ellos tienen una perspectiva

---

que nosotros no tenemos y viceversa. Tenemos que entablar una muy buena conversación para trabajar en conjunto.

Otro ejemplo en el cual podemos detectar una brecha contractual que tiene que ver con la obligación de los registros de hacer un análisis técnico para detectar amenazas a la seguridad. Sin embargo, los contratos no describen cuál es la acción a realizar después de detectarse esa amenaza a la seguridad.

Después tenemos el acuerdo de registrador en el cual hay que investigar y responder apropiadamente ante el uso indebido del DNS. La propia junta directiva reconoce que el acuerdo base de registrador no tiene el nivel suficiente de detalle para explicar qué significa esta cláusula. Sí, se habló al respecto. Hubo iniciativas por parte de los voluntarios. Se ha pensado mucho sobre el tema pero, aun así, necesitamos un diálogo sobre cómo informar, denunciar, cómo gestionar todas estas cuestiones de uso indebido del DNS y cómo se pueden modificar los términos y las condiciones contractuales para que podamos ser más efectivos. Dicho esto, quiero agradecerles porque nos han concedido un poco más de tiempo del que teníamos programado para esta sesión. Pido disculpas porque quizá no podamos responder a las preguntas.

---

MANAL ISMAIL: Es cierto. Es cierto. Muy bien. Muchas gracias a todos los panelistas, a los colegas del GAC, a quienes han participado en esta sesión. Les pido a los colegas del GAC que por favor regresen a las 16:30 hora local. Muchas gracias.

**[FIN DE LA TRANSCRIPCIÓN]**