ICANN85 Mumbai | Foro de la comunidad – Plenario de At-Large: avances en la agenda de mitigación del uso indebido del DNS
Martes, 10 de marzo de 2026 – 10:30 a 12:00 IST

MICHELLE DESMYTER: Hola, bienvenidos a la plenaria de At-Large, cómo avanzar la agenda de mitigación del uso indebido del DNS. Yo soy Michelle DeSmyter y coordinaré la facilitación. Esta reunión será regida por los estándares de comportamiento y la política antiacoso de la comunidad de la ICANN, durante la sesión las preguntas o comentarios serán leídos en voz alta solo si se presentan en el panel de preguntas. Tendremos interpretación de inglés, francés y español.

Si desean tomar la palabra, por favor, levanten la mano en Zoom y cuando digan su nombre se permitirá la participación virtual, y el participante podrá abrir su micrófono. Por favor, digan su nombre para el registro, en qué idioma hablarán, si no es inglés, y, por favor, hablen a una velocidad razonable. Con esto le paso la palabra a Justine Chew.

JUSTINE CHEW: Gracias, Michelle. Sean todos bienvenidos, los que están presentes y los que están en línea, queremos tener la mayor cantidad posible de participantes porque tendremos una interacción al final.

Yo soy Justine Chew, moderadora de la sesión, y en nombre del ALAC quiero agradecer a todos los panelistas que están aquí, quiero señalar que hemos recibido disculpas de algunos de los panelistas que fueron invitados, por eso verán las diapositivas, no tendremos a nadie del grupo de registros ni de registradores y el GAC lamentablemente tuvo que cancelar a último minuto, pero está bien, podemos seguir y conversar, de todas maneras, porque no vamos a decidir nada.

¿Podemos mostrar la agenda, Michelle, por favor? En este breve tiempo trataremos de abordar tres temas, la primera parte de la agenda es una reflexión de nuestros panelistas, algunos de ellos son participantes o miembro del Proceso de Desarrollo de Políticas, uno sobre las verificaciones de dominios asociados, entonces tendremos una serie de cuatro sesiones sobre este PDP y ahí voy a invitar a algunos de los panelistas a que compartan sus reflexiones, qué funciona bien, etc.

Luego destinaremos un poco más de tiempo al segundo tema que tiene que ver con los algoritmos de generación de dominios y, en este caso, tenemos el privilegio de recibir la presentación de una persona del GAC, del grupo de seguridad pública, que hablará del marco existente y después vamos a ver cómo avanzar. Tendremos comentarios de John y Mukesh, se suponía que iba a ser Teresa, así que, él se va a hacer pasar por ella hoy.

Luego hablaremos de cuáles son las otras líneas del GAC en relación con las brechas de mitigación del uso indebido del DNS,

sabemos que hay un aporte al proceso del consejo de la GNSO en la identificación de procesos acerca de cuáles son las brechas que hay que abordar, ya tenemos una serie de tres, el primero ya está siendo tratado por el PDP 1, el segundo será manejado por el PDP 2, que vendrá después.

El tercero es esto que estamos hablando aquí, los algoritmos de generación de dominios, y todavía no hay indicación si se va a manejar dentro de un PDP o por fuera de las comunidades de PDP, me gustaría hablar al respecto, si es necesario que piensan ir por un proceso de PDP, o no.

Con respecto a la participación del público, tendremos una encuesta para arribar a una impresión de lo que piensan sobre esta agenda de uso indebido del DNS, o sea cuál debiera ser esta cuarta brecha. Entonces si les parece, comencemos.

Vamos a ir a la primera parte de la agenda y las preguntas son: ¿Qué piensan sobre lo que está pasando con el PDP 1? Vamos a empezar, obviamente, con los panelistas y si alguien del público quiere intervenir, por favor, indíquenlo y yo me voy a ocupar de que no nos quedemos sin tiempo, vamos a ser estrictos.

Voy a ir en el orden que vemos en pantalla. Si los oradores no están listos, simplemente díganlo y los ponemos al final de la lista. Entonces ese es el grupo de partes interesadas comerciales y el panelista es Ching Chiao, le voy a dar la palabra.

CHING CHIAO

Gracias, Justine. Soy Ching Chiao, represento la BC del CSG, gracias por recibirme. Como dijo Justine, yo soy uno de los miembros, así que, solo podré hablar en nombre de la BC y el CSG, sé que hay otros miembros de ese grupo en la sala, así que, por favor, no duden en intervenir, si así lo considera.

Respondamos esta pregunta. La impresión general que nosotros tenemos, por lo menos desde el punto de vista de la BC, es que fue muy bueno el arranque de este grupo, muy constructivo, muchas participaciones pensadas en el grupo, la mitigación del uso indebido del DNS sigue siendo, claramente, una prioridad de la comunidad. Habiendo dicho esto, el segundo punto que quiero transmitir es que nosotros ya reconocemos la fatiga que experimenta esta comunidad de tener que hablar y trabajar sobre el uso indebido del DNS y las políticas, pero también quiero reconocer que esta fatiga está fuera de la comunidad, los ataques sobre las organizaciones y muchos de los profesionales de ciberseguridad, con los cuales yo trabajo en mi cotidianidad, bueno, esa fatiga está ahí, por estas causas continuas de tener que lidiar con el uso indebido del DNS, eso lo tendremos que considerar.

Otra reflexión que quiero compartir sobre las declaraciones es que, el BC y el CSG siguen preocupados por los tiempos, por el cronograma y los desafíos que estamos manejando, por un lado, tiene que ver con el proceso del PDP; que ya lo ha señalado el personal, que este PDP en particular podría terminar a finales del 2027, pero la realidad es que no sabemos cuánto durará porque el

paisaje del uso indebido del DNS seguramente cambiará para el 2027, entonces quizás se necesite uno o dos años más para que se pueda implementar el cambio de política, estamos hablando del 2029 para que se implemente este PDP.

Entonces sabiendo que las campañas de uso indebido del DNS funcionan no en días, sino en horas, esto hay que señalarlo. También en la lista de trabajo tenemos, por un lado, con los ADC, la mitigación es una cosa y la detección es otra. Entre la mitigación y la detección hay una brecha, entonces tuvimos que señalar estos hechos en este ecosistema en particular, que en este mismo momento requiere hacer una limpieza de los actores que utilizan estos ADC y que hacen estos manejos de las conductas de las brechas.

Ahora quiero señalar otras cuestiones, algo que, probablemente, no sé si surgirá, pero es para que entiendan mejor. En el caso de este PDP, tiene un alcance muy estrecho, estamos hablando solamente de los registradores y los ADC, no estamos hablando de múltiples registradores y múltiples ADC, vamos a manejar uno por vez.

Ahora quisiera concluir mi participación diciendo que para CSG, en particular, es un trabajo sobre una consolidación de las ideas del uso indebido del DNS, nos tenemos que asegurar de que la ICANN sea la fuente del DNS, aunque en los últimos años y en los años futuros el uso indebido del DNS no desaparecerá, de hecho, se va a intensificar en los próximos años, pero bueno, el CSG está aquí

para trabajar con todos ustedes en la resolución de este problema, queremos trabajar con el grupo y con todos y cada uno de ustedes en la sala, eso es todo lo que tengo para decir.

JUSTINE CHEW: Gracias, Ching, por tu presentación. Espero que hayan prestado atención porque tendremos una sección de preguntas y respuestas después de los presentadores. Vamos a darles cinco minutos a cada orador, si les parece. Nuestra siguiente oradora es Michaela del NCSG.

MICHAELA SHAPIRO: Quiero agradecer la invitación, soy del grupo de partes interesadas no comerciales. Ching ya mencionó algunos temas, ustedes ya tienen una idea, recién comenzamos a trabajar, así que, estamos muy optimistas. Queríamos decir que hay una discusión, que es sustancial, y es sobre la carta, ayer iniciamos una discusión sobre la primera pregunta de la carta orgánica que debiera disparar verificación de un dominio asociado, todavía no se ha definido nada, incluso el cronograma se está discutiendo.

Como dijo Ching, el uso indebido del DNS es una situación que va cambiando, entonces tenemos preocupaciones de seguridad reales que queremos que se aborden. También queremos asegurarnos de que se haga bien, no queremos que se apure, las soluciones deben ser equilibradas para las partes interesadas de los usuarios finales y los registratarios.

El NCSG está muy contento de ver que los Derechos Humanos y sus evaluaciones se integren en el proceso desde el comienzo y, como dijo Justine, no estamos tratando aquí de manejar todos los tipos de uso indebido del DNS, queremos desarrollar un proceso y un marco que pueda aplicarse entre distintos tipos, entonces la idea es que sea a prueba del futuro, es un proceso que puede utilizarse con la evolución de la situación.

Me gusta ver que el alcance del PDP es como es y recordarles que es limitado, como la carta lo marca, por una razón, es para dar un marco y acordamos deliberadamente esto con el consejo, así que, queremos hacer énfasis en el hecho de que el cronograma es clave. Seguramente hay mucho más por decir, pero quizás deba hacer una pausa en este momento. Gracias.

JUSTINE CHEW

Gracias, Michaela. Tal como usted lo dijo y lo puso Michele en el chat, el uso indebido del DNS, como lo define la ICANN, es en lo que estamos trabajando, son cinco cosas, en realidad, no es general. Ahora pasamos al GAC, al grupo de trabajo de seguridad pública, del Comité Asesor Gubernamental.

Yo no sé si Janos y Wolfgang quieren hablar por separado, o si será uno solo.

JANOS DRIENYOVSZKI

Buenos días, yo voy a hablar en nombre del GAC. Como dice Michaela, estamos en la fase inicial del PDP 1, de hecho, de las

cuatro sesiones solo una se ocupó de la sustancia del PDP, así que, el grupo de trabajo de seguridad pública comparte este optimismo.

Estamos contribuyendo activamente a tener un resultado rápido del PDP, que debiera ser muy focalizado, y por esa razón esperamos un cronograma que se acuerde y que se maneje, de manera que refleje adecuadamente esta naturaleza focalizada del PDP, es decir, este enfoque estrecho del alcance aborda un tema específico, que son las verificaciones de los dominios asociados, esperamos que este PDP sea uno de los primeros ejemplos de eficiencia.

Sobre lo que mencionó Ching sobre las brechas, creo que, abordar la brecha entre detección y mitigación es un buen punto y también creemos que las acciones que se tomen en virtud de esta nueva política, posiblemente, también aborden la evolución y que se pueda disparar una vez que se consiga o haya disponible evidencia sobre la cual se pueda actuar.

El tiempo de reacción, la responsabilidad y la aplicación debieran poder monitorearse, tiene que ser una política que aborde el uso indebido del DNS, pero también que nos dé feedback sobre cómo puede mitigarse este tipo de uso indebido para tener un buen sentido de en qué funcionan las operaciones y, por supuesto, que tenga una suficiente aplicación efectiva, que sea una herramienta significativa, básicamente para evitar este abordaje generalizado del uso indebido del DNS, que es la situación actual, un bordaje coordinado, que la comunidad que yo represento le sea de utilidad

y también a las partes contratadas les permita ahorrar tiempo y esfuerzo. Gracias.

JUSTINE CHEW Gracias, Janos. Ahora pasemos a mis colegas Steinar o Khatleen, ¿quién va a tomar la palabra?

STEINAR GRØTTERØD Hola, soy Steinar Grøtterød de At-Large. En primer lugar, estoy de acuerdo que fue un muy buen comienzo y es muy interesante ver los distintos abordajes de las distintas partes, desde la perspectiva de At-Large no hay nada escrito que esté fijo, no estoy seguro de si vamos a tener algo ya cerrado, pero entiendo, y después de haber hablado con distintos registradores, creo que, es importante tratar de llegar a una política de consenso.

Para ser franco, sería obligar a los malos registradores a hacer algo porque la mayoría de los registradores ya están haciendo algo, esta política es también una responsabilidad del área de cumplimiento de la ICANN y tener una herramienta para ser policía… No sé si sea una buena palabra decir que es algo malo, pero bueno, es interesante tener un abordaje proactivo de discusión del uso indebido del DNS y su mitigación, es lo que hay que hacer.

Entonces esperemos que sea rápido el resultado, algunos rumores dicen que puede hacerse en un mes, no estoy seguro, pero bueno, podemos ser optimistas. No sé, Khatleen, si quieres decir algo.

JUSTINE CHEW

Gracias, Steinar. Voy a recibir algunos comentarios, no tenemos demasiado tiempo, pero sí tenemos participantes en línea que hacen comentarios en relación al impacto de este tema sobre los Derechos Humanos, esos son la mayoría de los comentarios recibidos, no sé si alguno de los panelistas quiere responder. Veo que Volker solicita la palabra.

Si alguno de los panelistas quiere hablar acerca del impacto que este tema tiene sobre los Derechos Humanos en el chat, por favor, levanten la mano y, mientras tanto, le doy la palabra a Volker.

VOLKER GREIMANN

Estoy en el grupo de partes interesadas de registradores. Yo pienso que, al haber considerado este tema con tanto nivel de detalle, obtenemos una mirada muy acotada, no se trata solamente de los registradores, quizás los miembros de la BC podrían hacer mucho más para combatir el uso indebido, tienen mucho poder dentro de su alcance, pueden hacer muchísimas actividades, pueden identificar a los malos actores que están obteniendo rédito a partir del uso indebido.

Hay partes contratadas que están obteniendo muchísimas ganancias a través de esta acción y, sin embargo, nada se hace al respecto, hay actores maliciosos que no pueden seguir operando; por las partes contratadas que se lo impiden, pero aparecen en otros ámbitos, esto sucede una y otra vez en distintos mercados

porque no hay mecanismos apropiados para hacer frente a esta situación.

Por ejemplo, si yo en mi registrador dejo sin efecto, o le doy de baja a un actor malicioso, ese actor malicioso se va al registro de otro colega, creo que, estamos teniendo una visión muy acotada y debemos ampliar la visión desde la mirada de un ecosistema amplio, que va más allá de las partes contratadas, tienen que participar mucho más los organismos de orden público, tienen que arrestar a estos malos actores y me estoy cuidando para no usar un vocabulario vulgar porque si estos malos actores quedan fuera de circulación, de todas maneras, van a seguir actuando.

Nosotros en la cámara de partes contratadas tenemos un pequeño ecosistema y tenemos una acción muy acotada, pero estos actores maliciosos van más allá de la industria, son trasversales en la industria, operan en distintos registradores, por ejemplo, hay campañas a través de un registrador, un revendedor, luego hay otro registrador, hay un vendedor de dominio; que es minorista, y veo que el mismo actor malicioso está utilizando más de un canal.

Entonces ahí sé a ciencia cierta que son activos en el espacio de más de un registrador, incluso si yo actúo inmediatamente se van a pasar a otro registrador que active su dominio malicioso y tenemos que adoptar una perspectiva mucho más amplia, eso no quita que nosotros debamos actuar y tomar medidas, lo que digo es que tenemos que tener una visión más amplia para poder avanzar en este tema.

JUSTINE CHEW

Muchas gracias, Volker, por compartir su perspectiva, creo que, en la comunidad vamos a estar de acuerdo con lo que usted plantea, el tema es, ¿cómo lo logramos? No vi que se haya respondido al tema de los Derechos Humanos planteados en el chat. Michele, usted había solicitado la palabra, pero antes quiero pronunciarme en mi capacidad como coordinadora de enlace entre el ALAC y la GNSO.

Hay un impacto sobre los Derechos Humanos que está evaluado en este PDP, entonces tenemos que generar procesos que estén de cara al público, eso es lo que no hicimos en otros PDP, necesitamos fortalecer algunas funcionalidades cuando hablamos del interés público global, de la infraestructura global, entre otros temas.

Entonces el PDP está estructurado de manera tal de tener en cuenta consideraciones amplias del uso indebido del DNS en este momento. Michele, le doy un minuto porque debemos avanzar.

MICHELE NEYLON

Me parece cómico que me dé un minuto. Volker ya abarcó gran parte de lo que yo quería decir. Con respecto a los Derechos Humanos tenemos que ser muy conscientes de que quizás corremos el riesgo de que haya reacciones impulsivas y quizás es muy fácil para los pequeños registradores que no están al tanto de la situación general, corremos el riesgo de que estos registradores, al ver una política, la cumplan en exceso.

Por ejemplo, lo vimos en las enmiendas contractuales recientes que tienen que ver con el uso indebido del DNS, capaz hay un usuario anónimo aleatorio en una red social y a raíz de ese caso queda sin efecto la actividad del registrador. Por ejemplo, tenemos que ver a qué registro contactar, tenemos que ver de quién es el dominio, tenemos que convencer al registro de que vuelva a activar ese dominio que había quedado fuera de funcionamiento, esto es muy problemático porque estas políticas pueden parecer, de alguna manera, limpiar internet, pero, por otro lado, también sirven para que haya competencia entre distintas empresas y hay actores maliciosos que utilizan estas políticas en contra nuestra. Gracias.

JUSTINE CHEW

Gracias, Michele, tomamos nota de su intervención y sí, los registradores siempre nos recuerdan esta situación que usted ha planteado. Quiero pasar al segundo tema de la sesión del día de hoy, avancemos, por favor.

Ahora tenemos el privilegio de poder ver mejor o en más detalle cuál es el marco existente para dar respuesta a los algoritmos que generan nombres de dominios, estamos hablando de software malicioso que genera cientos, o incluso miles, de nombres de dominios que son utilizados por los actores maliciosos para perpetrar sus acciones, esta es una explicación muy simple.

Ahora le voy a dar la palabra a Janos para que hable en mayor detalle acerca de este tema y luego veremos cuáles son nuestros posibles pasos a seguir como comunidad. Tiene la palabra, Janos.

JANOS DRIENYOVSZKI

Muchas gracias. Gabe y Andrews, mi buen colega y amigo del grupo de trabajo sobre seguridad pública del GAC fue quien estuvo detrás de toda esta presentación, yo voy a hacer lo mejor posible para estar a la altura. Mi presentación sobre los algoritmos que generan dominios se centra principalmente en la dificultad que generan para los organismos de cumplimiento de la ley y cómo estos organismos pueden actuar de manera responsable frente a esta situación.

Básicamente este marco es de carácter voluntario, no tiene carácter vinculante, fue diseñado por el grupo de partes interesadas de registros y el grupo de trabajo de seguridad pública del GAC, y no es vinculante.

Dicho esto, como dijo Justine, estos algoritmos que generan nombres de dominios son utilizados por delincuentes para perpetrar sus actividades, sus actos ilegítimos, esos algoritmos utilizan una cantidad aleatoria de números y letras, por eso los ciberdelincuentes pueden ir de un dominio a otro y continuar con sus actividades maliciosas como la distribución de malware. Tenemos que tener medidas de seguridad a nivel nacional, por ejemplo, bloquear un dominio dentro de una red, estas actividades

tienen consecuencias significativas para las víctimas y se realizan por lo general, a gran escala.

Aquí vemos las principales características de estos algoritmos que generan dominios y también vemos el impacto de su utilización, se generan miles de dominios a través de los algoritmos, como dije, es muy fácil para los ciberdelincuentes registrar un dominio y mantener el control en una red de bots para distribuir software malicioso e incluso después de que se tome una medida, estos algoritmos siguen generando dominios.

Entonces como esta generación de dominios es continua los organismos de orden público de cumplimiento de la ley tienen que recurrir al poder judicial para que ordene el cese de estas actividades y esto también puede ser sumamente costoso, este es un ciclo que se perpetúa y se permite.

¿Por qué es importante una cooperación más eficiente entre los registros y los organismos de cumplimiento de la ley? Este marco abarca a las partes interesadas que utilizan el nombre de dominio, usan infraestructuras de botnets y diseminan software malicioso, especialmente a través de estos DGA, entonces este marco quizás también pueda ser utilizado para hacer frente a grandes listas de dominios generadas por estos algoritmos que utilizan redes de bots para perpetrar sus actividades maliciosas.

Ahora bien, con respecto a reservar un dominio, el registro lo coloca en su lista de nombres reservados, entonces no se puede registrar el dominio que está en esta lista, ¿por qué es eficiente esta

medida? Porque evita las registraciones ilegítimas de estos dominios que fueron generados, entonces no se puede utilizar para cometer uso indebido del DNS.

Esto no requiere ninguna información de la ICANN, el registro puede actuar de manera inmediata, pero tiene algunas limitaciones también porque no permite sinkholing, que se utilizan para identificar máquinas que están infectadas con virus, y tampoco se puede notificar a las víctimas, con lo cual esta medida es apropiada cuando no hace falta recurrir al sinkholing de dominios.

Sinkholing significa redireccionar el servidor de nombre de un dominio para que los organismos de cumplimiento de la ley puedan identificar a las víctimas, o a aquellas máquinas que diseminan el malware, además, se puede crear un registro de dominios creados por algoritmos que redirija, o haga el sinkholing del dominio, de manera tal que todo ese tráfico de botnets quede capturado allí y pueda ser analizado.

Entonces se puede reservar el dominio, se hace el sinkholing, se identifican las máquinas infectadas y se identifican a las víctimas, esto sirve para notificar a las víctimas y también para tomar medidas de remediación. Ahora bien, esto requiere de ciertas medidas, o características, se requieren algunas restricciones contractuales de la ICANN, ahí se mencionan las secciones correspondientes del acuerdo de registro, también se necesita el

permiso que obtenga el registro y, además, se pueden cobrar tarifas.

Ahora bien, también necesitamos una manera expeditiva y una vía expeditiva de cursar estas solicitudes para los registros y esto se plasma en las obligaciones contractuales, de manera tal que los registros puedan pasarse en estas medidas cada vez que un dominio es creado de esta manera.

El objetivo del marco es generar un entendimiento en común de los problemas que enfrentan los organismos de cumplimiento de la ley para combatir el malware y los botnets a gran escala derivados de estos dominios generados por algoritmos, también pretende explicar cómo se pueden utilizar estos DGA para justamente generar malware y botnets, y cuáles son las medidas de remediación.

Tenemos cuatro pilares sobre los cuales se basa este marco orientativo para los organismos de cumplimiento de la ley para que generen información oportuna, de manera tal de que tengan el tiempo suficiente para actuar, tomar las medidas correspondientes y tener una solución a largo plazo, básicamente que eviten que estos organismos de cumplimiento de la ley tengan que obtener, por ejemplo, la renovación de una orden judicial año tras año, para poder seguir dando respuesta a estos dominios generados por algoritmos o DGA.

Los invito a leer el documento completo, no es un documento muy extenso, al final tiene un anexo con plantillas donde se les explica

cómo presentar una solitud para ERSR, para esa solicitud de seguridad expeditiva para los registros y espero que esto sea inspirador, que pueda ser replicado en otras áreas y que todos podamos ver esta situación a través de esta perspectiva. Todo esto lo hicimos con casos claves, casos reales y a través de esos casos pudimos encontrar esta solución, esto es algo no vinculante, pero permite que los registros y los organismos de cumplimiento de la ley actúen de manera coordinada para ahorrar tiempo, esfuerzo, dinero y tener una medida de remediación sostenible para dar o hacer frente a estos dominios generados por algoritmos.

Les agradezco su atención y estoy abierto a sus preguntas.

JUSTINE CHEW: Muchas gracias, Janos, por respetar el tiempo que le otorgamos para su presentación. Volker, adelante.

VOLKER GREIMANN: Tengo una pregunta porque hay algo que no entiendo, vemos que los DGA son herramientas, como podrían ser los algoritmos, es decir, se les puede utilizar con cualquier finalidad, ya sea buena o mala, entonces, ¿cómo se diferencia a los DGA que se utilizan con fines legítimos, ilegítimos o neutrales? ¿Cómo podemos hacer esto para tener un discernimiento y no ponernos a todos en la misma categoría?

JUSTINE CHEW Naoum, ¿quiere responder?

NAOUM MENGOUDIS Muchas gracias. Cuando nosotros hablamos de los algoritmos DGA, de estos dominios generados por algoritmos, queremos ver para qué se lo utilizan y cómo fue su ingeniería, entonces ahí podemos diferenciar si se trata de un dominio malicioso, o no, entonces hacemos ese discernimiento y utilizamos este marco de manera expeditiva.

JUSTINE CHEW Muchas gracias. Volvamos a la agenda. Ahora pasamos a la discusión, pero antes de abrir el piso a los panelistas, al público aquí y en la sala de Zoom quiero invitar a John, primero, para que nos cuente sobre lo que se habló y también las preguntas que tenemos para usted, ¿qué rol podría la organización de la ICANN desempeñar en esta área? En especial a la hora de coordinar.

JOHN CRANE Una cosa que la ICANN, tradicionalmente, hizo en este ámbito porque obviamente tenemos 15 años de experiencia trabajando con personas que están tanto dentro como fuera de la comunidad en los DGA, lo que deberíamos hacer, en realidad, depende de cómo se determine la política y los contratos, no quiero ser demasiado crítico al respecto, pero necesariamente el personal de la ICANN necesita esa política para diseñar su propio trabajo.

Escuché hablar de compartir la información y escuché lo que ustedes hablaron, en una discusión en 2010 nosotros recomendamos tener una solución centralizada para compartir la información y en aquella época eso vino del personal, hubo conversaciones que no anduvieron muy bien y era necesario mejorarlas, ahora lo miro con nostalgia, incluso en el 2010 cuando hicimos la propuesta, no era necesario que la ICANN hiciera este trabajo, pero había una necesidad de tener algún tipo de coordinación.

Fue una discusión interesante, esa discusión surgió en parte por lo que la ICANN estaba haciendo a finales de los años 2000 hasta el 2010 sobre los DGA, en ese momento había un malware particularmente malicioso que comenzaba a usar esta tecnología con frecuencia, el más famoso, probablemente, sea Conficker.

Entonces durante ya una década hemos trabajado y ahora se entiende la metodología, en aquella época trabajamos con la comunidad de aplicación de la ley, los grupos de seguridad pública y los científicos para tratar de determinar de qué se trataba esta metodología. Una vez que se hizo la ingeniería inversa de los DGA uno no alcanzó con hacer una lista, los colegas de aplicación de la ley lo saben, que es mucho trabajo, hay mucho por hacer para que no haya víctimas de los DGA, es una metodología que requiere mirar todos los nombres, decidir si un nombre debiera crearse o bloquearse, o reservarse. Esa era la terminología que se utilizó en el nuevo marco.

Hemos trabajado extensamente en los últimos 15 años con la comunidad de aplicación de la ley y la gente de seguridad operativa de la comunidad para entender cómo funciona el sistema de nombres, cómo se registra, cómo se bloquea un nombre, muchísimas conversaciones sinkholing, cómo funcionaría, hablamos mucho acerca del parking de páginas y tratamos de trabajar con las personas que intentan luchar contra el uso indebido.

Creo que, el resultado que todos queremos es tener una mejor seguridad pública, ya no tenemos estas conversaciones porque la gente ya entiende la metodología, en la medida en que evolucione no hay inconveniente en continuar teniendo esta interacción si la comunidad arriba a soluciones que requieren una política, la vamos a implementar, si hay un PDP su resultado, el que fuere, lo vamos a implementar.

Ahora bien, si el resultado de este PDP es muy extenso… Porque yo no creo que configurar algún tipo de esfuerzo de coordinación para pasar datos sea algo sencillo en verdad, entonces no somos la única industria que se ocupa de este tema, compartir inteligencia, compartir datos muchos lo hacen, cómo se hace de manera segura o cómo se hace de manera adecuada es un proyecto de múltiples años. Eso significa que, para nosotros, no está presupuestado, pero, sin duda, tenemos un rol que desempeñar aquí.

Escuché este comentario del ERSR, tuvimos muchas respuestas a estas solicitudes a lo largo de los años y mi colega Mukesh hablará

un poquito al respecto acerca de cómo esto evolucionó, no sé de cuándo es el ERSR, ¿2009? Mukesh, quizás sea tu turno de tomar la palabra.

MUKESH CHULANI El ERSR era un servicio diseñado específicamente para brindar servicio a los operadores de registros, vimos una presentación en un marco de cuatro puntos que lo incluía como último punto, pero nosotros observamos; y esto es lo que decía John, que la evolución de los procesos actuales también iba a ocurrir porque la industria avanza y eso nosotros lo notamos, de hecho, nos lo hicieron notar los registros, no eran los únicos que requerían los ERSR porque los registradores también eran parte en causas judiciales, por ejemplo, entonces había que tomar medidas.

El ERSR fue la manera en que manejamos las tarifas de la ICANN para que no existieran, pero el resultado fue que el tratamiento fue desigual y los rectificamos en 2021, ya no se lo conoce como extensión de respuesta de seguridad porque no es solo para registros, las actividades maliciosas que involucran en el DNS son de tal escala y gravedad que requiere seguridad, estabilidad y resiliencia sistemáticas porque existe el potencial de una amenaza tanto temporaria como a largo plazo, entonces el registro o el registrador tienen que tomar medidas.

Estas son las reglas básicas, pero, como todos vimos, se necesita evolución.

JUSTINE CHEW

Gracias, Mukesh. Algo que quisiera ver y vamos a asignar un poco de tiempo para hablar al respecto, pero antes le voy a pedir a Wolfgang, a Naoum o a Janos que respondan la pregunta en el chat de Steinar, lo agradeceríamos, simplemente respondan en el chat de Zoom.

Y en el tiempo que queda quisiera hablar del siguiente tema, una reseña muy general del marco, nosotros sabemos que hay alguna terminología que se actualizó, ya hace tiempo que existe, entonces la pregunta… Vamos a dar prioridad a los panelistas, la pregunta es: ¿Cómo hacemos para que esto avance? ¿Cómo tomamos esta información y avanzamos? Porque necesitamos un PDP, es mejor que se maneje en cooperación con la comunidad por fuera, en tal caso que parte de la comunidad tiene que estar sentada a la mesa, y cómo hacemos para que esto tenga lugar.

Vamos a volver a los panelistas que intenten responder, sé que Ching levantó la mano antes, así que, no sé, Ching, si quiere tomar la palabra.

CHING CHIAO

Gracias, Justine. La reacción inicial que tenga después de escuchar a John, qué bueno que hizo referencia a estos muchos años de trabajo, creo que, hay una pieza que falta, que son los CC se sienten aquí también porque suceden no solo con los genéricos, sino también con los nombres de dominios con código país, entonces

es una observación, una pregunta que tengo para los organismos de aplicación de la ley, que están aquí en la sala, o para los colegas del GAC.

Noté que esta táctica, el sinkholing, quizás tener un sitio de suspensión no sea lo más efectivo ni lo más sofisticado, seguramente los organismos de aplicación de la ley intencionalmente dejan que algunos nombres maliciosos sigan operando o botnets, o IP maliciosos para conocer la red completa de hacia dónde van. Entonces hay que esperar con paciencia y mapear a todos los clientes de los DGA para poder agruparlos, como así decir. Gracias.

JUSTINE CHEW Creo que, John quizás responda.

JOHN CRANE En parte porque, por lo que yo sé, es del 2000 en adelante los ccTLD, bueno, esto es un proceso voluntario para los registros y registradores, hay una política acerca de cómo hacer esto, no hay una necesidad política de mitigar los DGA, por supuesto, aunque los CC no están cubiertos por esta política, la mayoría sí participan en este sitio, yo lo conocí de primera mano y sé que muchos lo hacen. El resto voy a dejar que lo conteste el PSWG.

NAOUM MENGOUDIS Con respecto a la pregunta del chat, si entendí bien, quizás la pregunta deba volver a formularse de otra manera, serán creados

porque, conociendo el algoritmo de generación, hay que saber en qué momento qué dominios se van a usar y ponerlos en una lista de reserva y, por supuesto, pueden dejar de estar reservados y ser liberados.

Las policías, los organismos de seguridad, tienen flujos de trabajo en funcionamiento para DGA o botnets, con el sinkholing lo que queremos es proteger a las víctimas y rastrear las máquinas infectadas para poder contactarlas o notificarlas, o para tener estadísticas, a veces, algunas policías cuando toman un servidor malicioso toma control del servidor de comando y control para que siga funcionando, o para que no siga funcionando, y deje de infectar a otras máquinas, si dejamos que funcione es para aprender más de la red y localizar a los delincuentes.

JOHN CRANE

Gracias. El trabajo es para resolver la base infectada, no sé si la palabra es sofisticado, pero es más amplio, da la impresión de que muchas organizaciones que recopilan… Hay una organización que se llama “Shadow Server”, con lo cual yo trabajo, que trabaja con muchos organismos de aplicación de la ley que van recabando todos estos datos y tienen mecanismos para los equipos de respuesta ante emergencias nacionales y demás.

Entonces con los años hemos visto que gran parte del trabajo importante tiene que ver con llegar a la base de la infección y prevenir el prejuicio en los usuarios finales.

JUSTINE CHEW

Muchísimas gracias por esta enriquecedora conversación, vamos a mostrar las preguntas en el Zoom, les voy a pedir que respondan las preguntas en el Zoom, tenemos un par de minutos más, no mucho, sobre este tema. Primero, Michele y luego Steinar, no sé si alguien quiere hacer otro comentario o hacer una pregunta, por favor, indíquenlo levantando la mano en Zoom para que podamos seguirlos. Michele.

MICHELE NEYLON

Gracias. Esto de los DGA, como John bien lo señaló, hay mucha cooperación entre los ccTLD y los gTLD, los ccTLD tienen mucha flexibilidad en lo que hace, no están restringidos por los contratos con la ICANN, un ccTLD, por ejemplo, cuando habla con un registrador sobre un nombre de dominio marca los usos indebidos y hay un gran volumen de dominios registrados, a veces, cuando reciben estas notificaciones reconocen que hay un problema, suspenden los dominios y luego se hace el reembolso, no se los penaliza financieramente por hacer lo correcto.

El hecho de que un registro o un registrador sea penalizado económicamente por intentar sacar lo malo de internet es la situación más tonta, más ridícula de todo este circo, no tiene, para mí, absolutamente ningún sentido y no llego a entender por qué alguien con una cara de piedra pueda defenderlo. En lo que hace a los registradores nosotros tenemos límites muy estrictos en el número de nombres de dominios que podemos tener, en lo que se

llama el período de gracia, básicamente cuando un dominio se registra en los primeros cinco días podemos suprimirlo, pero, por varias cosas, el límite es muy bajo hoy día, para los registradores más grandes tienen gran volumen de registraciones mensuales y ese porcentaje se basa en eso, el número de dominios que se pueden suprimir sin ser penalizados también es bastante alto.

Con los registradores más pequeños, que es mi caso, si nos identifican como malos actores, ¿qué pasa? Eso significa que nuestro número de supresiones sube radicalmente y cruzamos el umbral, y eso cuesta miles de euros en gastos administrativos para conseguir reembolsos y tiempo, para mí, es más un problema esta verificación de los dominios asociados, operativamente, en mi opinión, es algo absolutamente imposible de implementar. Gracias.

JUSTINE CHEW: Gracias, Michele. Bueno, creo que, yo también estaría de acuerdo con usted, en ese sentido, hay otras cosas que podríamos hacer más allá de un PDP, que pensamos, son más prioritarias. Steinar. Disculpas, Siva, tengo que cerrar la lista de preguntas porque tengo que continuar, así que, solo Steinar, un minuto.

STEINAR GRØTTERØD: Sí, quería aclarar lo que preguntaba en el chat, que era, ¿es realmente posible crear esta lista para el registro que le impida la registración? ¿Esa lista es algo que hay que monitorear a diario?

Quizás para añadir, quitar, ajustar, etc., etc., esto es personal, yo quiero entender este problema desde este punto de vista. Gracias.

JUSTINE CHEW ¿Alguien quiere responder?

NAOUM MENGOUDIS Sí, primero, tiene que hacer la ingeniería reversa del algoritmo del DGA y cuando lo haya hecho sabrá en qué momento qué dominio se va a generar, entonces usted sabrá, no sé, será hoy, el martes a las 10:30, sabemos que el algoritmo va a generar una URL específica, un nombre de dominio, y si uno lo sabe con antelación lo puede bloquear, quizás lo puede poner en una lista, todos los registros pueden acceder a esta lista y verificar si un dominio; que se va a asignar, esté en la lista reservada o puede uno trabajar individualmente, bloquear dinámicamente el dominio.

Y con respecto a la pregunta de Justine sobre las mejores prácticas, creo que, el primer paso es la coordinación, quizás la política tenga que venir después para que todos la cumplan.

JUSTINE CHEW Bueno, creo que, esta es la primera sugerencia que se ha planteado como un posible curso a seguir, así que, muchas gracias. Siva, debo seguir adelante con la sesión, así que, le pido que ingrese su pregunta o comentario en el espacio del chat de la sala de Zoom.

Muchísimas gracias por este intercambio de ideas, ahora continuamos con la presentación, por favor, Michelle. Quisiera pasar a la próxima diapositiva, por favor.

Disculpen, parece que tenemos un pequeño inconveniente técnico con la presentación, Michelle o el personal que esté a cargo de la presentación, por favor, ¿pueden avanzar las diapositivas? Muchísimas gracias. Ahí vemos la próxima diapositiva, muchas gracias.

Bien, ahora en esta sección de nuestra reunión vamos a plantear temas que deberían ser de importancia para la GNSO, para que lo plasmen en un PDP o para que tomen otro curso de acción viable, por ejemplo, en el formato de mejores prácticas, en ese caso, la comunidad lo puede hacer fuera de un PDP. Ahora voy a pedirle a los panelistas que nombren uno o dos de sus prioridades, más allá de las tres que ya han sido identificadas, la cuestión de las registraciones maliciosas; que es el PDP 2, y también los algoritmos que generan dominios, los DGA, que ya hemos hablado junto con una tercera temática; que también está siendo abordada.

Más allá de esos temas, ahora pueden plantear el cuarto tema o el quinto, o el sexto, al cual se le debería dar prioridad, ahora vamos a darle prioridad, nuevamente, a los panelistas y quizás alguien del grupo de trabajo sobre seguridad pública quiera hablar acerca de este tema.

JANOS DRIENYOVSZKI

Voy a empezar yo. En el GAC, en el grupo de trabajo sobre seguridad pública, estamos interesados en ahondar en la exactitud de los datos de registración porque consideramos que no está donde debería estar, está el tema de los revendedores, los servicios de privacidad y representación. Esta cuestión, a nuestro criterio, se vería beneficiada a raíz de una política pertinente y hago referencia al informe preliminar de la GNSO del mes de septiembre, en el cual se identifican áreas a remediar que tienen que ver con la registración, con las actividades sospechosas, entonces nosotros consideramos que este informe de cuestiones de la GNSO podría profundizarse.

Y también nos preocupa el tema de las denuncias de los informes, quisiéramos saber también cuáles son los datos que mantienen las partes contratadas y cuáles son los que informan o reportan al departamento de cumplimiento contractual de la ICANN, por supuesto, que esto es más amplio, es una categoría más amplia que las que fuimos mencionando anteriormente. Con esto finalizo mi presentación y esas son mis sugerencias iniciales.

JUSTINE CHEW

Para los que están presentes en la sala y también participando por Zoom, por favor, presten atención a lo que están diciendo los panelistas, luego la audiencia podrá participar, pero necesitan prestar atención a lo que están sugiriendo, entonces si ustedes tienen sugerencias adicionales las pueden hacer después de estas

presentaciones si prestan atención, debemos avanzar más rápido, por favor, en virtud del tiempo.

NAOUM MENGOUDIS Muchas gracias. Yo iría por el uso indebido de los subdominios, lo veo en campañas de malware, entre otras campañas, son subdominios que pueden causar spoofing, por ejemplo, de buscadores web de dispositivos móviles, por ejemplo, si tengo PayPal/login/algo ese subdominio malicioso me puede engañar y puedo entrar en un lugar no deseado, además, creo que, como dijo Volker, deberíamos concentrarnos en que todas las cosas funcionen en todo el ecosistema, no alcanza con que los registradores actúen por sí mismos, hay que intercambiar información, intercambiar señales entre todo el ecosistema de registros, registradores y demás participantes.

JUSTINE CHEW Pasamos a Michaela, por favor, tiene la palabra.

MICHAELA SHAPIRO Nosotros queremos hablar acerca del proceso de mitigación de uso indebido del DNS, queremos tener mecanismos accesibles y estandarizados para los registratarios, por ejemplo, podrían ser vías para que los registratarios, que han demostrado el uso indebido y que ha sido remediado, que puedan solicitar que se reactive su dominio. También estamos pensando en un proceso de reclamos y apelaciones, en el cual los registratarios puedan

presentar sus reclamos o sus denuncias y que, luego, también tengan la posibilidad de apelación y que esto abarque distintos tipos de uso indebido del DNS.

Janos habló de la transparencia en los informes, nosotros queremos que las acciones que tienen que ver con el uso indebido de nombres de dominios y las decisiones pertinentes, que todo eso sea transparente y que se transparente la clase de acciones de mitigación y el proceso de toma de decisiones para llegar a esas acciones de mitigación. Contestaré sus preguntas con todo gusto, pero con esto finalizo mi intervención.

JUSTINE CHEW Gracias por ser tan concisa, Michaela. Ahora tiene la palabra Ching.

CHING CHIAO Quiero reiterar lo que ha planteado el PSWG, lo digo a título personal, también quiero enfatizar el potencial de los dominios creados mediante DGA, por ejemplo, qué pasa con un DGA que parece remediado, bueno, eso insumiría muchísimos días y luego tenemos un subdominio que podría utilizar esos nombres generados, entre otras cosas, por los DGA y esos podrían ser utilizados a través de diferentes campañas, pero retomo el punto principal de lo que quiero decir y sí, mi preocupación son los subdominios, como dijeron previamente.

JUSTINE CHEW: Ahora le agradezco por ser tan conciso, a Ching. Le doy la palabra a Kathleen.

KATHLEEN SCOGGIN: Nosotros queremos identificar cuestiones muy acotadas y queremos tener información no solo acerca de lo que hay que remediar, sino también de los mecanismos correspondientes antes de comenzar con el PDP o para tener un cierto orden y no proceder de manera aleatoria, nosotros queremos ver qué hacemos si, además del PDP, tenemos que tomar medidas más proactivas como, por ejemplo, algoritmos proactivos.

A nosotros en el ALAC nos interesa para darle un mejor servicio al usuario final y entonces ahí tendríamos otro alcance de actividad, direccionaríamos nuestros esfuerzos de otra manera, veremos qué pasa con el PDP, sí, pero nosotros vemos otro curso de acción que sería de interés más específico para el ALAC.

JUSTINE CHEW: Muchas gracias, Kathleen. Ahora sí puede participar la audiencia, pasamos a ese segmento de esta sección, de esta presentación, espero que tengamos el tiempo suficiente. Dicho esto, vamos a recibir los aportes de los miembros presentes y los miembros que están en Zoom, esta parte la va a coordinar Kathleen.

KATHLEEN SCOGGIN: Muy bien, queremos demostrarles las brechas detectadas en el informe de la GNSO, no las hemos tratado extensivamente hoy,

pero tenemos cinco de estas brechas aquí, hablamos de los algoritmos que generan dominios, hablamos de la verificación de los contactos de los registratarios y esta es otra preocupación, y la detección en tiempo real. Vamos a hacer una breve encuesta para ver cuáles son sus prioridades, luego tendremos la prioridad 4 y la 5, si ustedes contestan otro quiere decir en la encuesta que para ustedes la prioridad es otra, entonces adaptaremos nuestra presentación o esta sección.

Voy a detenerme un segundo para que puedan leer la encuesta y vamos a aguardar a los resultados para ver cómo avanzamos, creo que, tienen un código QR que pueden escanear.

JUSTINE CHEW Vamos a avanzar con la encuesta con el código QR, también está la herramienta Mentimeter que tiene un enlace y pueden acceder mediante el enlace, a lo mejor alguien del personal lo puede hacer, puede incluir el enlace para entrar a la plataforma Mentimeter y hacer la encuesta. Me dicen que ese enlace ya está en el chat en la sala de Zoom, entonces les vamos a dar unos segundos para que decidan cómo quieren responder la encuesta, a través del QR o del enlace a la plataforma Mentimeter. Veamos la diapositiva que le estábamos mostrando previamente para que puedan comprender qué les estamos preguntando efectivamente en la encuesta.

Estas son las cinco prioridades que identificamos después de leer el informe final de cuestiones de la GNSO, estas las identificó la GNSO, las identificó como medidas preventivas porque en At-Large

queremos hacer medidas preventivas, queremos ser preventivos, en lugar de reactivos, queremos hacer más foco en la prevención, por eso tenemos estas prioridades que sacamos del informe, como dijo Kathleen, esto no es exhaustivo, si ustedes piensan alguna otra medida preventiva pertinente, por favor, compártanla con nosotros.

KATHLEEN SCOGGIN Quiero decirle algo al personal. Una vez que se responde la primer pregunta ustedes, como son los administradores de la encuesta, tienen que hacer clic para que se sigan habilitando las preguntas y los miembros del público puedan seguir respondiendo.

MICHELE NEYLON Como ustedes están respondiendo la encuesta aprovecho para hacer algunos comentarios, veo algunas de las opciones y no me queda claro cuándo se las implementaría o cuándo se supone que las tenemos que poner en práctica, vemos la opción 3, 4 y 5 que, a mi criterios, son un poco repetitivas, se superponen, pero no sé si están dentro del alcance o el ámbito de acción de un registro o un registrador, nosotros no tenemos la capacidad de implementar gran parte de estas medidas. Veo la palabra “algoritmo” y me da escalofríos, además.

JUSTINE CHEW Muchas gracias, Michele. Nosotros extrajimos estas opciones del informe de cuestiones elaborado por la GNSO, si usted quiere optar

por la respuesta o por la opción “otros”, allí puede sugerir más opciones, esto se basa en un proceso ya consolidado para no empezar desde cero, esto sale del informe de cuestiones, es lo que está allí y tiene razón, en algunos casos, son un tanto repetitivas estas opciones, por eso se podrían combinar algunas de ellas, podemos consolidarlas y justamente quisiéramos ver qué piensan ustedes al respecto para llevarle las ideas al consejo.

MICHELE NEYLON

Gracias, Justine. No quiero entrar en demasiado detalle, pero si hay dos o tres personas que tienen cuestiones potenciales y las quieren plantear, bueno, este es un buen ejercicio y está muy bien. Ahora bien, cuando vamos a la realidad práctica de registros y registradores enfrentando la mitigación de uso indebido a gran escala esta cuestión, por ejemplo, de verificación de contacto del registratario es algo muy sencillo, pero vemos que los actores maliciosos utilizan identidades falsas o roban identidades.

Hace unas semanas llamó una señora muy amable de Asia que tenía mucha curiosidad por saber por qué tal o cual compañía había sacado dinero de su cuenta bancaria y nosotros dijimos: “Pero ¿nosotros estamos sacando dinero de la cuenta bancaria de esta señora?” Y lo que pasó fue que le habían hackeado su cuenta de Home Banking y bueno, habían pasado la autenticación de dos factores, las otras medidas de seguridad que, se supone que, son como el chaleco antibalas de internet hoy en día.

Entonces esta cuestión de verificar el contacto del registratario realmente no es de mucha utilidad. Luego el tema de los algoritmos predictivos, por ejemplo, si hay una persona que no tiene los datos de la tarjeta de crédito de la persona que está comprando los dominios, bueno, no se puede llegar a todo esto, es decir, en resumen, el problema es que no tenemos la manera de hacerlo y, reitero, cuando escucho la palabra "algoritmo" realmente me resulta aterrador.

JUSTINE CHEW Muchas gracias, le reitero, esto fue sacado de una lista que resulta de un proceso de consulta que hicimos con la comunidad, lo que usted plantea seguramente lo plantea su grupo de partes interesadas y se plantea también en el consejo. ¿Cómo vamos con los resultados? Estoy teniendo en cuenta el tiempo porque nos quedan siete minutos. Kathleen.

KATHLEEN SCOGGIN Sí, debiéramos mostrar los resultados actuales, continuar actualizando después y más adelante mostrar los resultados de la encuesta, vamos a ir a la siguiente pregunta.

MICHELLE DESMYTER Un momento, Kathleen.

JUSTINE CHEW Mientras tanto veo que Michaela ha pedido la palabra. Michaela.

MICHAELA SHAPIRO Justine, Michele tiene razón, yo tenía un par de preocupaciones sobre los algoritmos generados por la Inteligencia Artificial, pero mis consejeros en el NCSG están haciendo un trabajo impresionante con esto. Hay una pregunta, ¿cuáles son los temas de mitigación del uso indebido del DNS preventivos? Quería aquí hacer una distinción, son preocupaciones muy válidas, pero les aliento a que consideren si un PDP y manejar esto desde la ICANN es necesariamente la respuesta, no sé si tengo una respuesta clara, pero solo quería marcarlo.

JUSTINE CHEW Sí, gracias por el cometario, Michaela. La pregunta es, ¿qué debiéramos abordar en la forma de un PDP? Básicamente es una manera, a través de la participación que ustedes hagan en el Mentimeter, de entender qué piensan ustedes, si es una prioridad, es decir, qué es lo que va a aparecer en el consejo de la GNSO para decidir cómo seguir, el feedback.

KATHLEEN SCOGGIN Vamos a avanzar a la siguiente pregunta, espero que aparezca el Mentimeter, háganmelo saber.

JUSTINE CHEW No me gusta que haya tanto silencio, por eso, mientras esperamos, voy a invitar a que quien tenga cualquier comentario aprovechemos este tiempo para intervenir. No veo manos en la

sala de Zoom, entiendo que esta información quizás sea difícil de procesar, pero si es que alguno de ustedes puede hacer un aporte informado, no duden en hacerlo, simplemente es para tener una impresión de qué piensan. Michele.

MICHELE NEYLON

Finalmente, encontramos un terreno común, lo cual es bueno, creo que, algunas cosas en qué pensar es si hay otras formas de mitigar el uso indebido, hay cosas técnicas que pueden hacerse y debieran hacerse, o podrían necesitar hacerse, cosas como la tecnología de los resolutores del DNS, varios resolutores públicos y algunos privados ofrecen capas de seguridad, verifican respecto de varias listas, bloquean ciertos tipos de dominios, pueden bloquear TLD completos… Muchas cosas distintas, por supuesto, esto genera ciertas inquietudes en cuanto a Derechos Humanos, libertad de expresión, no voy a ignorarlo, pero también hay soluciones, por ejemplo, la conexión a internet en una escuela, uno limita el acceso, no sé, a un sitio web de pornografía.

No sería bueno que los alumnos de una escuela primaria puedan acceder a pornografía, en lugar de aprender el alfabeto y bueno, quizás ese es un lugar donde sí es apropiado mitigar estos problemas porque, como registrador, no solo tenemos una capacidad muy limitada de hacer cosas, solo podemos hacer cosas en algunos lugares, no en todas partes y yo no puedo, por ejemplo, tomar una imagen del sitio web que usa un dominio registrado con nosotros, a menos que esté en nuestros servidores, es físicamente

imposible, a menos que se opere algún tipo de proxy inverso, o algo por el estilo, nosotros no podemos hacerlo.

Y otra cosa es que, la solución ante la ICANN siempre se expresa en términos de uso indebido de internet, creo que, es un poquito engañoso, o ingenuo, porque nosotros cada vez que queremos hablar con la ICANN al respecto no nos dan opción porque no lo encuentran los navegadores, no encuentran el enlace, no lo comparten, solo aparecen en publicidades en distintas plataformas que todos utilizamos, entonces quizás sean esas plataformas las que haya que limpiar.

JUSTINE CHEW

Sí, gracias, es difícil considerar todo el universo de uso indebido del DNS y ni hablar del uso indebido del internet, creo que, nosotros tratamos de encontrar nuestros caminos para la mitigación y nuestro rol ahí. Bueno, tengo en cuenta que es el horario del almuerzo, así que, no veo que haya otra pregunta, así que, vamos a la última diapositiva.

Quiero cerrar agradeciendo a los panelistas, a los participantes, un gran agradecimiento, espero que consideren aceptar nuestra invitación, si es que armamos algo para Sevilla, lo cual, creo que, es probable y a todos los participantes que están en la sala y en la sala de Zoom muchas gracias por su atención, su participación en el chat, los comentarios y en la encuesta de Mentimeter.

Gracias al personal de apoyo, creo que, no lo agradecemos lo suficiente, gracias al personal involucrado en la sesión, en particular al de At-Large, a los intérpretes, muchísimas gracias por su servicio y al personal técnico por mantenernos en funcionamiento, muchísimas gracias.

[FIN DE LA TRANSCRIPCIÓN]