ICANN83 | Foro sobre políticas – Debate del GAC sobre la mitigación del uso indebido del DNS
Martes, 10 de junio de 2025 – 9:00 a 10:15 CEST

JULIA CHARVOLEN

Bienvenidos a la sesión del GAC sobre el uso indebido del DNS, tengan en cuenta que esta sesión está siendo grabada y se rige por los estándares de comportamiento esperado de la ICANN, y la política antiacoso.

Durante la sesión las preguntas y comentarios solo se leerán en voz alta si se encuentran en el recuadro de preguntas de Zoom, esta sesión incluye interpretación en los seis idiomas de Naciones Unidas y portugués, si desean tomar la palabra durante la sesión levanten la mano en Zoom, cuando se mencione su nombre tendrán la posibilidad de tomar la palabra, por favor digan el idioma en que se expresarán si es diferente del idioma inglés y recuerden hablar a una velocidad razonable para la interpretación.

Ahora le doy la palabra al presidente del GAC, el Sr. Nicolás Caballero.

NICOLÁS CABALLERO

Gracias, Julia. Le damos la bienvenida a nuestros colegas, le damos la bienvenida a Martin Kunc del CSIRT de la República Checa, también tenemos a nuestros colegas de Interisle Consulting Group, tenemos a Karin y a Greg, a Graeme Bunton de NetBeacon, Susan Chalmers de Estados Unidos y representante de PSWG, también

contamos con nuestro representante Janos de la Comisión Europea y el Sr. Miyamoto, quien representa a Japón.

Vamos a tener una conversación muy interesante sobre el uso indebido del DNS y después vamos a darle la palabra a los presentes para poder tener una conversación interesante, así que, sin más, voy a darle la palabra a Tomo. Tomo, adelante por favor.

TOMONORI MIYAMOTO Buenos días, buenas tardes y buenas noches a todos aquellos colegas que estén conectados remotamente. Soy Tomonori, de Japón y aquí les presento la agenda para la sesión, después de mi presentación vamos a tener actualizaciones sobre el panorama del uso indebido del DNS y su mitigación, tendremos también una presentación del país anfitrión sobre campañas, phishing y una presentación de insights.

Luego vamos a hablar sobre los Procesos de Desarrollo de Políticas, o PDP, y los próximos pasos. Nos vamos a centrar en algunos PDP, también en la delegación de los nuevos gTLD para el próximo año. Aquí en esta diapositiva vemos cierta información de contexto, los contratos en la ICANN, el RAA requiere que las partes contratadas, los registros y registradores adopten medidas o acciones para la mitigación del uso indebido del DNS.

Mi país ha estado trabajando en la definición también de lo que es el uso indebido del DNS, dentro del contrato de la ICANN esto está limitado a lo que es malware, botnets, phishing, pharming y spam,

la enmienda del 2024 en estos contratos es un primer paso para poder tomar en cuenta la mitigación del uso indebido del DNS y considerar próximos pasos. Siguiente diapositiva.

Algunos de ustedes quizás estén familiarizados con este gráfico, esto demuestra cuál es el ámbito del contrato de la ICANN que está representado en el recuadro verde, como pueden ver, es bastante limitado para poder lidiar con el problema de manera efectiva, para esto hay que considerar la relación que existe entre los registros y registradores, también se puede buscar cooperación mediante la comunicación con lo que está resaltado en el recuadro rojo.

También se están trabajando con diferentes nuevos gTLD de la próxima ronda, pero es importante tener en cuenta todo el panorama, incluido en esta diapositiva. En nuestra reunión de Seattle hicimos una presentación sobre lo que es la situación y la evidencia del uso indebido del DNS, la semana pasada tuvimos diferentes seminarios del GAC y una presentación de NetBeacon sobre un posible PDP, además, la GNSO y su equipo reducido sobre uso indebido del DNS presentó sus plazos, objetivos y la colaboración con este equipo reducido podría ser una posible forma de avanzar.

Esta es la última diapositiva de la presentación, no es 100% exacta, pero muestra cómo se organizan algunos tópicos y debates. A la derecha vemos la medición durante lo que es el informe del uso indebido y la mitigación, esto está basado en lo que son los

contratos de la ICANN, esto se hace para los fines de la transparencia. Y también se puede pensar en medidas que tengan que ver con una transición, podemos pensar en medidas proactivas que incluyan informes y otro tipo de actividades, o vías que se den al momento de la registración.

Sobre la base de los resultados del estudio INFERMAL restringir, por ejemplo, las registraciones a granel, podría considerar la verificación, podría ser algo a tener en cuenta. Ahora vamos a invitar a Martin de CZ NIC para que dé su presentación. Martin, adelante por favor.

MARTIN KUNC Muchas gracias. Estoy aquí para compartir nuestro caso en relación al phishing. Siguiente diapositiva.

Les quiero contar un poco sobre nuestros proyectos, quizás ya conozcan los más importantes, por ejemplo, BIRD y las mediciones del DNS que nosotros hacemos, lo que se denomina ADAM, entre otros.

¿Quiénes somos? Bueno, CZ NIC es el registro del dominio CZ que también opera el CSIRT de .CZ y la historia comienza en junio de 2022 cuando vimos algunos casos de phishing, al principio esto no era de mucho interés, pero en CZ comenzamos a ocuparnos porque no era algo usual, en este caso, el gobierno comenzó a dar subsidio para ayudar a los ciudadanos en situaciones complejas, también con respecto a algunos personajes, teníamos algo como BankID,

esto no es muy común en varios países, pero en la República Checa los bancos se reúnen en algo que se llama BankID, utilizan las mismas credenciales y se verifican esas mismas credenciales para poder acceder a los sitios gubernamentales, también fueron víctimas de este tipo de delitos.

¿Cuál era el escenario de este phishing? La gente comenzó a recibir mensajes de texto donde se les decía que tenían cierto dinero, se enviaron bastantes de esos mensajes, como ustedes pueden ver, sé que es difícil para ustedes comprender qué es lo que dice aquí, pero básicamente el mensaje era el mismo, desde si les pedían que hicieran clic en un determinado lugar.

Entonces esto los llevaba a un sitio de phishing donde se les pedía utilizar la información bancaria y también otras cuestiones, por ejemplo, el tipo de autorización, autenticación, etc., lo interesante era que esto se podía hacer solamente durante el horario comercial, entonces hubo un ejemplo en República Checa donde se perdían algunas cosas y si se podía tener acceso a un sitio, en este caso, esto no funcionaba 24/7, sino durante el horario comercial. Esto era así porque los que estaban perpetrando el delito usaban las credenciales en tiempo real y necesitaban la confirmación.

Aquí vemos unos de los ejemplos del sitio que se asemeja muchísimo, excepto por la URL. Aquí vemos otro ejemplo, en este caso, se puede elegir el banco, no se podía elegir siempre cualquier banco, sino que, se requerían elegir entre algunos en particular,

aquí vemos la URL en la parte superior, había un número, se pedía hacer clic y así podían ver cuán exitosos eran con esta campaña. Siguiente, por favor.

En 2022 se comenzó con 11 dominios por mes, lo cual no era muy común, no eran tan malos. En febrero del 2023 la cantidad subió a 72 nombres de dominios registrados, lo cual representó un incremento importante para nosotros.

Sabemos que con el tiempo iban mejorando y nosotros también teníamos que mejorar, así que, comenzamos a hacer una búsqueda activa, a mejorar el proceso, estudiar y a tomar notas para poder comprender los detalles de una mejor manera.

Entre los ejemplos de la investigación activa pudimos analizar esta zona y ver los dominios que estaban registrados, entonces, al principio, comenzamos utilizando caracteres similares que se utilizaban para el sitio porque tenían que cambiar los nombres, entonces siempre surgían nuevas ideas y nuevos nombres que terminaban siendo de utilidad, así que, se comenzaba registrando distintos nombres de dominios.

Eso nos ayudó a crear una lista futura con dominios que sufrían phishing, hacíamos una verificación cada cinco minutos y en ningún momento nuestra dirección fue bloqueada, y tan pronto como nos dimos cuenta de cuáles eran los sitios de phishing que estaban activos, enviamos una notificación y pudimos actuar para poder bloquearlos a la brevedad posible, también pudimos acortar

este tiempo para dar de baja estos dominios, que fue crucial. Siguiente diapositiva.

Tomamos nota de lo que fuimos investigando y para poder también determinar el patrón había sitios webs que emergían varios días después de la registración porque, primero, se necesita registrar el nombre de dominio, pero después hay que tener los registros de DNS y, finalmente, los certificados, entonces una vez que todo esto estaba listo se habilitaba el listado en el directorio y se cargaba el archivo de zona, después se analizaba. Nosotros pudimos analizar estas muestras y vimos que, a veces, diferían y, a veces, mejoraban.

En caso de que tengan curiosidad, les cuento que los certificados son algo importantes, teníamos que tener en cuenta también las contraseñas, todas las sesiones que habían sido creadas y también otras cuestiones que no son visibles para nosotros, de antemano.

Finalmente, consideramos que este caso fue una victoria porque finalizó un mes después de que comenzó el ataque, unos 28 dominios registrados en marzo si lo comparamos con la registración de 72 dominios en febrero, por supuesto, hay varios intentos con otros TLD y otros dominios simples, pero nada se compara a lo que fue en el comienzo.

Este gráfico quizás presente cierta dificultad para entender, pero les voy a explicar. El color verde representa las consultas que no fueron resueltas de manera correcta, en este caso, los ponemos en

verde porque son las que no pudimos resolver de los dominios de phishing.

Las que están en negro son aquellas que sí fueron resueltas, es importante resaltar que este no es el número real de usuarios porque no vemos cuántos usuarios están detrás de una resolución o de un resolutor único, pero sí nos da una idea de hacia dónde vamos y cómo estamos trabajando. Siguiente, por favor.

En este gráfico la comparación es mucho más positiva porque vemos que las barras verdes son mayores, así que, para nosotros es una especie de victoria porque sabemos que estamos trabajando y ganando la batalla.

Detrás de escena tenemos nuestras reglas, el artículo 17 nos permite sacar los dominios de la zona que nos resultan sospechosos o que suponemos son desfavorables para la ciberseguridad, en este caso, lo que hacemos es ponerlos en un estado durante un mes y le damos al titular del nombre de dominio la posibilidad de que nos contacte y que nos cuente qué es lo que está sucediendo, que diga: “Esto soy yo, se supone que esto no tenía que estar sucediendo”, si hacemos algo que no está bien de esta manera lo podemos resolver y mejorar, y también publicamos una lista de dominios que bloqueamos.

Esto sería todo de mi parte, espero que hayan disfrutado mi presentación y si tienen preguntas, con gusto las responderé.

TOMONORI MIYAMOTO: Muchas gracias, Martin, por compartir la experiencia. Ahora quisiera darle a la audiencia la palabra para las preguntas y respuestas. No sé si tenemos preguntas o comentarios.

GABRIEL ANDREWS: Muchísimas gracias por la presentación, Martin. Me interesó muchísimo y realmente me impresiona cuando hablan de esta cuestión de reconocer que hay ciertos dominios que son sospechosos que están siendo registrados, pero que todavía no ven esos sitios de phishing, pero comienzan a hacer el monitoreo y a verificarlo, si entendí bien es una medida bastante proactiva.

Ahora me pregunto, ¿ustedes creen que tienen que esperar porque necesitan una evidencia más concreta antes de tomar acción?

MARTIN KUNC: Sí, exactamente. Nosotros esperamos a que surja la evidencia para tener algo más concreto, para poder tomar el nombre de dominio y evitar algún tipo de proyecto de investigación, nuestro proceso está determinado de tal manera que si nosotros, por ejemplo, vemos o tenemos evidencia, la podemos utilizar al momento del bloqueo.

GABRIEL ANDREWS: Bueno, nunca he visto una conducta tan proactiva, realmente me resulta muy interesante, sé que ha presentado varios desafíos en otros momentos, pero cuando todavía no tienen la evidencia esto muchas veces resulta un desafío, pero ustedes tienen estas reglas

que les permiten hacer un monitoreo y tomar la iniciativa cuando ustedes sospechan que el dominio va a utilizarse para, por ejemplo, hacer phishing.

MARTIN KUNC Bueno, esto se hizo para una campaña de phishing para poder detectar aquellos nombres que podrían ser utilizados para cometer phishing y analizarlo para ver si hay algún tipo nuevo de phishing.

TOMONORI MIYAMOTO Ashwin está solicitando la palabra.

ASHWIN SASONGKO SASTROSUBROTO Soy Ashwin de Indonesia. Muchas gracias a los oradores por sus presentaciones, quiero decir varias cosas, ¿cuán efectivo es el uso de las DNSSEC como medida de seguridad en un sitio web? Y también, ¿cuán efectivo es el uso de una certificación de seguridad? ¿Eso sirve para mitigar el uso indebido del DNS o no funciona?

Y con respecto a lo que dijo el segundo orador de .CZ, usted da varios ejemplos de phishing, etc., ¿en estos casos se utiliza el ccTLD .CZ o utilizan también un gTLD? Gracias.

MARTIN KUNC No sé si pueda responder la primera pregunta, pero con respecto a la segunda parte, en este caso, el estudio se basó específicamente

en el dominio .CZ, lo cual facilitó el seguimiento para nosotros, hemos visto casos en los cuales se utilizan otros dominios también, pero no han sido de la misma magnitud.

ASHWIN SASONGKO SASTROSUBROTO: Por ejemplo, con respecto a mi primera pregunta, en el sitio web de la ICANN siempre nos dicen que hay que activar las DNSSEC, ¿cuán efectiva es esta activación para evitar el uso indebido del DNS? En indonesia, al igual que en muchos otros países, trabajamos con una norma ISO 27.001 que tiene que ver con estándares para la gestión de sistemas de seguridad, entonces yo quiero saber cuán efectiva es.

MARTIN KUNC: Bueno, las DNSSEC no ayudan para nada a combatir el phishing y con respecto a la norma ISO 27.001, yo no soy la persona indicada para responder esta pregunta porque está fuera de mi alcance, le pido disculpas.

TOMONORI MIYAMOTO: ¿Alguien más está solicitando la palabra? Aderonke, tiene la palabra.

ADERONKE ADENIYI: Muchas gracias, Martin. Soy Aderonke de Nigeria. Las presentaciones han sido muy buenas, con respecto a la identificación bancaria BankID, ¿usted consideró trabajar con el

regulador bancario para mitigar el uso indebido del DNS? En Nigeria tenemos el número de verificación bancaria, que es algo similar, y se usa en todas las plataformas de servicios digitales, quería saber si en algún punto trabajó junto con la entidad reguladora del sector bancario para emitir esta identificación bancaria, este BankID.

MARTIN KUNC

No fuimos muy exitosos cuando nos quisimos comunicar con la entidad reguladora, pero afortunadamente ellos tomaron cartas en el asunto y empezaron a trabajar con sus usuarios, empezaron a trabajar en contra de los intentos de phishing enviándole notificaciones a sus usuarios, etc., y eso funcionó bien, hicieron lo mejor que pudieron.

TOMONORI MIYAMOTO

Bueno, ahora vamos a invitar a Karen y a Greg, quienes nos darán su presentación acerca de phishing en el uso indebido del DNS.

KAREN ROSE

Gracias. Estoy aquí junto a Greg Aaron, somos de Interisle Consulting Group, nosotros tenemos más de 20 años de experiencia en esta área de trabajo, venimos haciendo investigaciones de distintos usos indebidos de recursos de internet y delitos perpetrados, en el día de hoy específicamente tenemos que hablar acerca del uso indebido del DNS a través de phishing,

van a ver que nosotros hemos publicado un informe que abarca muchísimos más ejemplos y muchísimos más casos.

Tenemos poco tiempo, así que, voy a ser breve. En conclusión, desafortunadamente el phishing y el uso indebido del DNS están creciendo a ritmos alarmantes, hubo más de 2 millones de ataques de uso indebido y más de 1.5 millones de dominios fueron atacados en los últimos 12 meses.

Esto subestima el problema enormemente ya que hay muchísimos ataques que simplemente no se informan, en el 77% de los casos estos dominios se registraron específicamente para cometer un ciberataque y el phishing afecta muchísimo a la sociedad y es muy costoso, se estima que por minuto se dedican más de $18.000 en pérdidas financieras para solucionar todos estos problemas y recordemos que, a escala global, muchos de los casos no son informados.

Tenemos que reconocer que estas iniciativas para combatir el uso indebido del DNS al día de hoy no han sido efectivas en gran medida, aquí vemos un cuadro de una empresa que se llama Freenum. Freenum combatió el phishing por un tiempo, pero vemos que luego estos ataques de phishing volvieron a retomar su ritmo y hubo como un rebote de ataques. Los que perpetran el phishing explotan o se aprovechan de dos cosas, precios bajos y facilidad en la registración, cuando un dominio tiene un precio de $2 o menos, esto facilita la actividad de phishing y los perpetradores se aprovechan en gran medida de esta situación.

Vemos la participación de mercado de los nuevos gTLD, que es solo del 11%, está en amarillo. Ahora, en el otro cuadro vemos que los nuevos gTLD representan el 51% de los ataques de phishing en el último año, entonces esto significa que este tipo de dominio sigue siendo atractivo para los perpetradores de ataques de phishing.

.COM, .NET, por ejemplo, se utilizan para promociones gratuitas y para algunos combos de promociones de diferentes productos, también quienes cometen phishing aprovechan la facilidad de registración de un dominio con pocos requisitos, sin verificación de identidad, sin validación de datos, además, prefieren algún tipo de proveedores que son registradores y TLD que están en ese punto intermedio entre ser económicos y de fácil registración, estos siempre están entre los primeros registradores, los primeros 10 o los primeros cinco que se utilizan año a año.

Los atacantes registran nombres de manera llamativa y es muy fácil de identificarlos porque siguen ciertos patrones, aquí les doy algunos ejemplos de algunos ataques, nombres que se generan por algoritmos que son variaciones de un tema o bien cadenas de caracteres completamente aleatorias, también hay nombres que se parecen muchísimo a marcas comerciales y también utilizan los mismos datos de registración una y otra vez y si no generan información de registración que es falsa.

Entonces tenemos que detectar estos patrones, algunos ccTLD ya tienen sistemas en el DNS para detectar estos patrones y también

tenemos algunas herramientas comerciales que permiten validar direcciones.

GREG AARON

Cada año estudiamos cómo se registran estos dominios, los atacantes no registran uno o dos dominios a la vez, sino que registran un gran conjunto de dominios y, como dijo Karen, siguen un patrón y eso hace que se puedan detectar.

Si vemos que hay un dominio que se registra, luego otro y otro con el mismo registrador, vamos a ver que generalmente se les va a utilizar para phishing, en general, el 37% de estos dominios que se utilizan para phishing se registran así, en forma masiva, por lotes, aunque no siempre en estos lotes se puede encontrar un dominio que se utiliza para phishing, pero estos lotes, estos conjuntos de dominios a veces tienen muchísimos dominios registrados, por ejemplo, 17.000 que los registró un único ciberatacante.

Estos atacantes ahora avanzan con rapidez y la víctima cae presa de ese ciberataque inmediatamente en menos de ocho horas después de haber sido registrado el dominio, estos atacantes saben que el dominio va a ser suspendido posteriormente, pero trabajan de una manera que les permite seguir perpetrando este delito en un dominio, en otro y en otro, mientras puedan seguir adelante así lo harán.

Vemos muchos phishing, ¿por qué? Porque es exitoso para quienes lo cometen, ahora bien, tenemos que pensar por qué está

sucediendo esto y por qué tenemos esta generación constante de dominios.

KAREN ROSE

El uso indebido del DNS es posible gracias a elecciones y opciones que toma la ICANN que tienen que ver con cómo funciona el mercado y elecciones que toman las empresas para llevar adelante sus negocios. Nosotros siempre decimos que la competencia es buena, entonces tener más competencia sería aún mejor, aunque desde una perspectiva económica esto no siempre es así, mucha competencia sin las reglas correspondientes puede tener efectos negativos.

Entonces es como si tuviéramos una industria que genera polución, que genera muchos costos en la sociedad y en los consumidores. El mercado del DNS es muy competitivo hoy, tenemos más de 2.000 registradores, cientos de TLD abiertos y los nombres de dominios son intercambiables, son como commodity, productos básicos y tiene prácticamente un costo marginal cero.

Entonces si no tenemos una política efectiva contra el uso indebido, los criminales se aprovechan de estas posibilidades y dinámica de mercado. Nosotros creemos que necesitamos medidas razonables y proactivas para prevenir el uso indebido del DNS y no solo mitigar el daño una vez cometido, aunque también sería de utilidad tener una mitigación más eficiente.

Tenemos que hacerlo ahora, implementar estas políticas ahora porque a medida que se sumen potencialmente más nuevos gTLD al mercado, esto generará mucha más presión, una presión competitiva mayor en el mercado y también afectará los precios. Siguiente diapositiva, por favor.

GREG AARON

Estamos viendo una tendencia, sobre todo en Europa. Los operadores de registros están innovando, por ejemplo, en algunos casos no les piden a todos los registratarios que demuestren su identidad, sino que, siguen enfoques que implican un riesgo, por ejemplo, algunos operadores de registros dicen: “Las registraciones pasivas son un ejemplo de un riesgo”, no sabemos quién es el registratario, pero está registrando muchísimos dominios, en ese caso, sí podríamos pedirle que verifique su identidad y quizás no deberíamos permitir que esos dominios funcionen hasta que estemos tranquilos y sepamos quién los está registrando. Esto está sucediendo en algunos TLD de Europa.

La ICANN tiene requisitos de verificación que son prácticamente mínimos, de hecho, una de las iniciativas de cumplimiento contractual de la ICANN descubrió que en el 20% de los casos no se seguían los pasos mínimos de validación, entonces nosotros vemos aquí una oportunidad, estudiar estos enfoques basados en riesgos para justamente prevenir y de esta manera dificultar el accionar de los delincuentes.

Nosotros tenemos estas ideas, fortalecer los requisitos de verificación, ver qué pasa con estas registraciones masivas, esto va de la mano, se relaciona estrechamente y quizás ustedes no sepan que en los contratos de la ICANN se requiere que los operadores de registros trabajen con todos los registradores acreditados por la ICANN.

Esto tiene varios motivos, entre ellos, por ejemplo, que las reglas de juegos sean parejas para todas las empresas que participan, sin embargo, a los registros se le exige que trabajen con registradores que aun al día de hoy les traen algunos negocios, por así decirlo, que no son beneficiosos, que son perjudiciales porque justamente tienen registratarios que quizás no sean buenos actores, así que, ahí hay trabajo por delante.

Los registros tienen herramientas para detectar el uso indebido antes de que suceda y poder accionar, o sea que hay algunas soluciones. En resumen, queremos que sepan que hay herramientas que se pueden utilizar y que hay políticas que podrían mejorar toda esta situación.

KAREN ROSE

Tenemos un informe que se publicará en el tercer trimestre de este año, estén atentos a esta publicación. Nosotros en nuestros informes no solo estudiamos nombres de dominios, sino también subdominios, alojamiento web, phishing, spam, malware, entre

otras cosas, por eso los invitamos a visitar nuestro sitio web y a leer nuestros informes.

Nosotros tenemos nuestra propia web que se llama Cybercrime Information Center, ahí tenemos muchísimos datos, tenemos tablas de clasificación, listas, etc., también estamos en Substack, todas las semanas publicamos blog y, por supuesto, tienen nuestro sitio web en pantalla y con todo gusto podemos contactarnos con ustedes a través del correo electrónico. Muchas gracias por su atención.

TOMONORI MIYAMOTO: Muchas gracias a Karen y a Greg por sus presentaciones. En virtud del tiempo vamos a seguir avanzando y ahora le voy a dar la palabra a Janos.

JANOS DRIENYOVSZKI: Muchas gracias, Tomo. Vamos a pasar a los próximos pasos en desarrollo de políticas y a los procesos de políticas, o micro PDP, que se podrían desarrollar. Primero, le voy a dar la palabra a Graeme para que haga su presentación de NetBeacon.

GRAEME BUNTON: Hola, soy Graeme Bunton, soy el Director Ejecutivo de NetBeacon. Hace unas dos semanas aproximadamente publicamos un documento blanco donde proponemos cinco posibles ideas sobre PDP, no hay tiempo hoy para compartir todos los detalles de estos PDP en particular, pero voy a colocar el enlace a esta información,

es un documento de 22 páginas para que lo puedan leer, aunque aquí se los voy a comentar brevemente.

Bueno, brevemente. ¿Por qué trabajamos con este tema? NetBeacon trabaja y dedica mucho tiempo a pensar cómo reducir el uso indebido del DNS y también somos una parte contratada, entonces trabajamos de una manera muy similar a lo que hace Interisle, tenemos un proyecto para poder medir y entender el uso indebido del DNS, esto se llama NetBeacon Map, o mapa de NetBeacon, y tomando en cuenta estos datos queremos brindar… Sí, voy a reducir la velocidad, gracias, sé que hablo muy rápido.

Queremos ver si podemos dar apoyo a los debates que se dan en la comunidad con algunas ideas, que pensamos podrían ser logrables en un tiempo adecuado y que tendrían un impacto en las cuestiones de uso indebido del DNS, y quizás podríamos también pensar en tener PDP que fueran un poco más acotados en cuanto a su alcance para la comunidad. No voy a entrar en detalles, voy a ser breve, pero habrá una obligación para que los registros informen sobre el uso indebido del DNS, van a recibir un informe de uso indebido del DNS y hay que tomar acción donde existe esta evidencia concreta. Siguiente diapositiva.

API, bueno, uno de los puntos más importantes del informe INFERMAL; y felicitaciones al equipo de OCTO por la realización de este informe, tiene que ver con que los API, que no tienen acceso aproximado, tienen una posibilidad de 401% de sufrir abuso, entonces es importante que los registradores tengan acceso a este

tipo de herramientas para poder de alguna manera controlar estas conductas de registración, los contactos para el uso indebido de sub dominios se pueden aplicar a estos sub dominios que se utilizan, o que son utilizados por terceros, mecanismos de recursos para el registratario cuando hay registros y registratarios que trabajan de forma diligente para luchar contra el uso indebido del DNS a escala, bueno, se pueden cometer errores, por lo tanto, a veces los registratarios pueden estar impactados o recibir impacto de la mitigación de ese uso indebido y para eso tienen que tener herramientas para poder resolverlo.

Coordinación DGA y Botnets. Tenemos los algoritmos de registración de nombres de dominios que, muchas veces, no funcionan eficientemente, entonces aquí estamos proponiendo una función centralizada para que la ICANN recabe esa información y la disemine, y para que esto sea más eficiente al momento de efectuar la disrupción de los Botnets. Puedo contarles acerca de cada uno de esos PDP de manera individual, puedo tomarme todo el tiempo que lo deseen, con gusto lo puedo hacer en los pasillos, pero sí hay algunos mensajes claves que quiero que se lleven el día de hoy.

Esta es una oportunidad concreta de avanzar en esta comunidad en relación a los PDP, a los desarrollos de políticas, para marcar la diferencia en lo que es el uso indebido del DNS, pero tenemos que estar todos comprometidos de manera colectiva a tener un proceso que sea delimitado y que tenga un alcance también preciso, esto va a requerir un foco y también el progreso a tiempo

va a requerir que el foco sea muy intenso, muy específico. Esto se torna complejo a medida que nos vamos adentrando en los detalles y también tiene un impacto operativo porque hay cuestiones que se deben resolver, pero sí podemos hacer la diferencia, podemos dar pasos positivos y eso es mejor que no hacer nada.

El tamaño de lo que sucede tiene mucho que ver también con el tamaño de lo que podemos hacer y la última parte que quisiera enfatizar, teniendo también en cuenta lo que decía Interisle en relación al camino o los patrones que se ven en el uso indebido del DNS, tenemos que pasar de estos informes de uso indebido individuales para abordar el uso indebido del DNS a escala. En nuestros datos vemos, muchas veces, a registros y registradores que terminan suspendiendo nombres de dominios que son maliciosos, pero la obligación está a nivel también del informe individual del uso indebido y también en la restricción de las registraciones masivas.

Tenemos que llegar a un punto donde podamos abordar el uso indebido del DNS no solamente a un nivel individual, sino también cuando hay campañas que representan un uso indebido y me parece que estas son las nuevas ideas que la comunidad tiene que comenzar a abordar. Desde nuestra perspectiva nosotros hemos publicado este documento, creo que, hemos logrado nuestro objetivo, hablamos de ideas que pensamos que pueden ser exitosas y si no son estas están bastante enfocadas y es lo que nos

gustaría seguir viendo en nuestra comunidad, que la comunidad siga hablando y avanzando en esta dirección.

Gracias a todos por la oportunidad de tomar la palabra el día de hoy.

NICOLÁS CABALLERO Muchas gracias, Graeme. Antes de darle la palabra a Tomo me gustaría pedirles a nuestros representantes del GAC que tomen en cuenta la necesidad de actuar, sabemos que los criminales nos están mirando actualmente, desarrollar un PDP que lleve cinco años los va a poner a dos o tres pasos por delante de nosotros, entonces desde mi humilde opinión me parece que tendríamos que tomar acción rápidamente. Adelante, Tomo.

JANOS DRIENYOVSZKI Gracias. Vamos ahora a centrarnos en lo que el GAC se debería centrar. Me gustaría hablar, primero, de la idea que se presentó en la cámara de partes contratadas en una reunión de ayer, que me parece que es beneficiosa para la discusión, una de las ideas es solicitar el requisito de tener un informe accionable de lo que son los dominios registrados maliciosamente.

La segunda idea tenía que ver con una posible enmienda contractual para garantizar que los registradores puedan ofrecer una API, o un programa de revendedor, para tener las medidas contractuales necesarias, en caso de tener que actuar en el uso indebido del DNS. Y había otra idea que tenía que ver con el

desarrollo de un marco operativo para todos los operadores de registros de gTLD.

Y la cuarta idea era el desarrollo de mejores prácticas para mejorar la calidad de los informes. Ahora bien, se ha mencionado muchísimo la palabra o el término “medida proactiva” y “registraciones masivas”, actualmente nos encontramos explorando el terreno de estas medidas proactivas y también medidas reactivas, y la idea sería lograr algo significativo antes de la próxima ronda, creo que, tendría que haber cierta priorización en relación a algunas acciones específicas. Esto también tiene que ver con lo que se hablaba anteriormente de estos PDP más acotados.

En su comunicado el GAC ha indicado la importancia de analizar el tópico de las registraciones masivas de los nombres de dominios, por supuesto, estas registraciones masivas, como se dijo esta mañana, presentan un alto riesgo de tener relación con el uso indebido del DNS y, por supuesto, su impacto es mayor que si se registra un nombre individual, quizás políticas de registración más estrictas y medidas proactivas podrían mejorar la situación.

Con respecto a las partes contratadas una idea sería que implementaran medidas proactivas en relación a la registración masiva, esto podría restringir las registraciones masivas de API, por ejemplo, restringiendo al acceso al API o también haciendo una verificación del registrante, creemos que esta idea es una idea

bastante realista. También se podría requerir un mayor precio para estas registraciones masivas.

Estas medidas proactivas podrían, de alguna manera, complementar las medidas reactivas y las medidas de mitigación que las partes contratadas han planteado, también NetBeacon ha propuesto trabajar o verificar los dominios asociados, así que, creo que, tenemos aquí una combinación de medidas proactivas y reactivas.

Bien, hablando de otras medidas proactivas y de mitigación, en el comunicado de Hamburgo el GAC reiteró la importancia de considerar el monitoreo proactivo y también se mencionó la necesidad de prácticas para detectar el uso indebido del DNS. Y en el trabajo sobre los datos de registración de nombres de dominios el GAC insta o alienta a los registradores a que exploren el uso de sistemas de acción de uso indebido del DNS basados en API, esto podría también implicar identificar indicadores, registración masiva al momento de que se inicien. Esta medida estaría en línea con la recomendación 1 que hizo el equipo reducido sobre uso indebido del DNS del consejo de la GNSO allá por octubre del 2022, esto quiere decir que todas las registraciones que presenten cierto nivel de riesgo deberían estar sometidas a una verificación.

También tenemos ejemplos de medidas proactivas de algunos ccTLD en Europa que tienen la posibilidad de implementar estos sistemas de detección o implementación. También se ha hablado

del ciclo de vida del nombre de dominio y hacer verificaciones correspondientes. Y ahora le voy a dar la palabra a mi colega Susan.

SUSAN CHALMERS Muchas gracias, Janos. Voy a hablar brevemente sobre una tercera idea que fue debatida por los líderes del tema en el GAC y que tiene que ver con las obligaciones de hacer informes, es importante considerar contribuir al informe y a las mediciones en el instituto de NetBeacon, por ejemplo, brinda mediciones, nosotros también trabajamos en diferentes informes, por ejemplo, el de Interisle, tenemos el informe INFERMAL que fue debatido ampliamente durante la reunión ICANN82. Todos estos documentos son muy relevantes, el departamento de cumplimiento contractual de la ICANN también produce informes mensuales sobre uso indebido del DNS, que representa una muy buena evidencia, y también sabemos que las partes contratadas han implementado las obligaciones sobre uso indebido del DNS en el 2024.

Pero no hay requisitos para las partes contratadas para que públicamente hagan informes sobre las actividades de mitigación de uso indebido del DNS o la implementación correspondiente de las enmiendas, entonces nos podríamos comenzar a enfocar en las estadísticas de estos informes. Otra sugerencia que tiene que ver con las ideas que hemos escuchado el día de ayer… Pasemos, por favor, a la siguiente diapositiva.

Son los siguientes. Tenemos los próximos pasos, tenemos las diferentes avenidas para tomar acción en materia de política, si

participaron del seminario que se hizo anteriormente para la reunión 83 sabrán que hay un equipo reducido de la GNSO que está trabajando sobre el uso indebido del DNS, este grupo tiene como objetivo básicamente evaluar los esfuerzos de mitigación de uso indebido del DNS, redactar algunas recomendaciones para septiembre de este año y realizar un informe final en el mes de octubre.

Sabemos que este plazo probablemente tenga que ser acotado, no vamos a hablar de este equipo particularmente el día de hoy, pero sí quiero que los representantes del GAC sepan que este grupo está trabajando en la GNSO. También tuvimos una reunión bilateral con la Junta Directiva el día de hoy, le voy a pedir al personal que, por favor, ponga en pantalla las preguntas que les hemos propuesto. Vamos a discutir con la Junta Directiva lo siguiente.

Si ustedes preguntan, quizás muchos estén de acuerdo con que los PDP deberían realizarse en un plazo más reducido porque los PDP llevan años, entonces la pregunta que le hicimos a la Junta Directiva y esto no es específico del uso indebido del DNS, pero sí le preguntamos, ¿cómo podríamos comenzar a cambiar algunos pasos en los procesos de los PDP para que los resultados se presenten y obtengamos resultados más rápidamente? No en tres años, no en cinco años, pero quizás sí en un período de 12 meses, o quizás menos.

Bueno, esto también es algo a lo cual invito a los representantes del GAC a que consideren, muchos representantes del GAC

seguramente estén familiarizados sobre cómo pueden participar y cómo efectuar cambios de políticas dentro de la ICANN, hay diferentes Procesos de Desarrollos de Políticas, después están los Procesos de Desarrollo de Políticas o los procesos que son de múltiples partes interesadas y que requieren la participación de todas las partes de la comunidad de la ICANN, incluido el GAC. Los PDP dan como resultado una política de consenso y la política de consenso termina siendo parte de los contratos que son vinculantes para todas las partes.

Otra avenida podría ser también hacer cambios en las políticas, que se puedan implementar enmiendas a los contratos entre la ICANN y los registradores o la ICANN y los registratarios, y por el momento los contratos se negocian en una base bilateral. En el 2024 se hicieron enmiendas muy importantes que se comenzaron a implementar y estas enmiendas establecen nuevas obligaciones para los registros y registradores, pero son el resultado de básicamente negociaciones bilaterales.

A diferencia de los PDP las partes interesadas, que no son la ICANN o las partes contratadas, no están involucradas en este proceso. Para los representantes del GAC la herramienta primordial es el asesoramiento del GAC, con esto pueden generar un asesoramiento consensuado, que luego será considerado por la Junta Directiva y de esta manera el GAC puede efectuar cambios en las políticas. Esta es la herramienta con la que cuenta, esto es algo

que contamos especialmente para aquellos representantes que son nuevos en el comité. Siguiente diapositiva, por favor.

Nos quedan 15 minutos, ¿es correcto? Queríamos que quede tiempo para el debate dentro del GAC. El presidente lanzó una convocatoria para abordar cuestiones, antes de la reunión ICANN83 este equipo también brindó algún documento a la lista del GAC antes de la reunión y aquí lo que hice fue simplemente mencionar los puntos principales de lo que hemos circulado, para lo que son los temas de importancia vemos aquí cuestiones que tienen que ver con el uso indebido del DNS, hemos también sugerido la revisión del panorama del uso indebido del DNS y la mitigación, algunos tópicos para los PDP y los próximos pasos.

Y también hemos sugerido la creación de PDP que sean más focalizados, con un enfoque más acotado para poder tener resultados consensuados en un plazo más corto, esto es lo que queremos presentarles a ustedes y ahora sí darles la palabra para que efectúen comentarios.

NICOLÁS CABALLERO Muchas gracias a la representante de Estados Unidos. Quisiera volver a la diapositiva número 12, a ver, ahí está, la que vemos en pantalla. Antes de darle la palabra a Indonesia le pido disculpas porque continúa aguardando, Ashwin, ¿este es un nuevo pedido de la palabra? Veo que su mano está levantada en Zoom. Bien, antes

de darle la palabra entonces y antes de que todos puedan presentar sus preguntas o comentarios quiero resaltar lo siguiente.

El Proceso de Desarrollo de Políticas es importante, es importante que los miembros del GAC participen, queremos que se sientan a gusto y tengan la oportunidad de participar de manera significativa, que se sientan a gusto, es decir, quiero decir lo siguiente. ¿Para qué serviría participar en un Proceso de Desarrollo de Políticas si no tenemos la oportunidad de presentar nuestras perspectivas, de hacernos oír, etc.? Por ejemplo; y esto es solo un ejemplo, si la presidencia no es eficiente sus ideas entonces no van a poder ser compartidas porque le van a dar la palabra a otra persona antes de que ustedes puedan manifestar sus propias perspectivas dentro de ese PDP.

Entonces, como dije, la idea es que ustedes se sientan a gusto al participar en esos PDP y desde ya estoy totalmente de acuerdo con lo dicho por la representante de Estados Unidos, es decir, tener Procesos de Desarrollo de Políticas más efectivos y más breves, desde una perspectiva gubernamental no podemos permitirnos dos, tres, cuatro años o más, hasta llegar a una solución. No hace falta que les explique los períodos de gestión gubernamentales, en algunos países el período presidencial es de cuatro años, los ministros de Relaciones Exteriores quizás están en su gestión por dos años, también los de tecnologías de la información y la comunicación, eso depende de cada país, pero ustedes entienden

lo que les quiero comunicar. Ahora tiene la palabra el representante de Indonesia.

ASHWIN SASONGKO SASTROSUBROTO: Gracias, Nico. Mi pregunta guarda relación con lo que usted dijo, tengo una pregunta con respecto a la norma ISO 27.001, ¿es lo suficientemente robusta para evitar prevenir el uso indebido del DNS, en su experiencia? Y le pregunto al colega de la República Checa, en Indonesia tenemos un problema muy grave al respecto hoy en día y, además, Indonesia es miembro de la ISO IEC, que tiene un comité y un subcomité, el subcomité 27 se avoca específicamente a la ciberseguridad y otro comité que se encarga de las TIC.

Entonces si esta norma no es suficiente o lo suficientemente robusta tenemos que decírselo a la organización que hace las normas ISO, a la organización internacional de normalización, nosotros tendremos una reunión próximamente con ellos, entonces queremos justamente ver esto porque la idea es hacer una política en la cual se va a utilizar esta norma ISO 27.001 para proteger nuestros sistemas, entonces, desde la experiencia de la ICANN, si esta norma no es lo suficientemente robusta tenemos que decirle esto a la organización de normalización, tenemos que hablar esto con ellos. Muchas gracias.

NICOLÁS CABALLERO Gracias, Indonesia, tomamos nota de su comentario. Ahora toma la palabra el representante de India.

SUSHIL PAL Muchas gracias, Sr. Presidente, muchas gracias, Interisle y a NetBeacon, por sus presentaciones especialmente y también por esta propuesta de hacer PDP que sean más acotados. Insisto en que estamos viendo los síntomas y no la causa de esta situación, estamos hablando de la correlación entre las registraciones masivas y los bajos costos, y los actores maliciosos, pero, reitero, en mi opinión, estos son los síntomas y no la causa, la causa está en las políticas, en los datos y en la identificación.

Nosotros vivimos en un mundo físico, pero nosotros en ese mundo sabemos quién vive en nuestra misma zona, en nuestro mismo vecindario, ¿verdad? Pero, en cambio, en el mundo digital hay anonimato, no sabemos quiénes son los actores maliciosos, entonces ellos tienen vía libre para actuar y lo único que nos queda es dar de baja un dominio, llegado el caso. No creo que incrementar el costo de $2 a $10, por ejemplo, para registrar un dominio, redunde en una menor cantidad de dominios maliciosos porque los beneficios para estos actores maliciosos son cuantiosos, lo vimos en la presentación.

Entonces, creo que, lo que necesitamos es que no solo los registradores, sino también los registratarios sean responsables y rindan cuentas, además, habrá un costo adicional para

registradores y registratarios, tenemos que ver esa solución. Gracias.

NICOLÁS CABALLERO

Muchas gracias, India, por su participación. Nos quedan siete minutos y tenemos siete personas que solicitan la palabra, así que, les ruego encarecidamente que sean breves y concisos. Susan, ¿quiere agregar algo antes de que empecemos con las preguntas? Bueno, entonces le doy la palabra a la Comisión Europea.

GEMMA CAROLILLO

Gracias. Soy Gemma Carolillo de la Comisión Europea, muchas gracias a los colegas del GAC por haber organizado esta sesión, que fue tan informativa y gracias a los oradores también.

Con respecto a lo que vamos a considerar en el comunicado quiero decir lo siguiente. Nosotros vemos algo muy bueno en esta situación, vemos que hay un impulso, un ímpetu en la comunidad para avanzar en el uso indebido del DNS después de las enmiendas contractuales, vemos que las partes contratadas han tenido iniciativas, escuchamos a NetBeacon, vemos los estudios de Interisle, así que, vemos que hay mucho impulso, mucho ímpetu, tenemos que aprovecharlo y colaborar con los otros grupos de la comunidad.

La prioridad para el GAC siempre fue obtener medidas antes de una próxima ronda con lo cual debeos ser pragmáticos y poder lograr medidas concretables en el plazo disponible, esto significa tener

prioridades sin olvidarnos del panorama general, pero tenemos que priorizar. Entonces nos parece importante emitir un asesoramiento con respecto a tener PDP que sean más acotados, específicos y, a la vez, quisiéramos esta lista de prioridades o que identificáramos temas prioritarios, nosotros hemos escuchado acerca de medidas proactivas, acerca de patrones de comportamiento que hay que monitorear, vimos el tema de las registraciones masivas, se han hecho distintas propuestas con lo cual, además de todo esto, consideramos que es importante tener en cuenta las obligaciones en materia de transparencia, que fue parte de un comentario público que hizo el GAC con respecto a las enmiendas contractuales sobre uso indebido del DNS.

NICOLÁS CABALLERO Gracias, Comisión Europea. Tenemos seis sesiones para hablar del comunicado, así que, lo vamos a considerar. Tome la palabra, representante de Canadá.

IAN SHELDON Muchas gracias, Nico, voy a ser breve porque sé que muchas otras personas quieren tomar la palabra. Gracias, Graeme, por el informe de NetBeacon, estoy de acuerdo con usted en que lo mejor es enemigo de lo bueno y que hay que avanzar, entonces también estoy de acuerdo con el tema de los PDP, en ser oportunos, quiero invitar al GAC a que lean el informe de NetBeacon, que está muy bien redactado, no es excesivamente técnico y tiene muy buenas sugerencias. Muchas gracias y con todo gusto participaré en los

	debates del GAC para ver cómo seguimos adelante de cara a estos PDP.
NICOLÁS CABALLERO	Gracias, Canadá. Tiene la palabra Países Bajos.
MARCO HOGEWONING	Gracias. Me sumo a los agradecimientos por haber organizado esta sesión, tenemos que, como dijo nuestro colega, ser conscientes de que lo perfecto es enemigo de lo bueno, tenemos que avanzar y, creo que, llegó el momento de empezar a acotar las opciones que tenemos por delante, tenemos que trabajar con la GNSO y la Junta Directiva, y quizás podemos encontrar uno o dos temas para seguir trabajando de cara a la próxima reunión. Gracias.
NICOLÁS CABALLERO	Gracias. Suiza.
JORGE CANCIO	Gracias. Me sumo a los participantes anteriores, es importante ver qué es lo que hablamos con la GNSO y la Junta Directiva, y ver cómo seguimos adelante, de todas maneras, creo que, hay potencial en esta idea de tener Procesos de Desarrollo de Políticas más acotados, más específicos y quizás quiero corregir a Susan, si se me permite. No creo que se haya dado algún PDP que haya durado menos de un año, pero, por supuesto, puedo estar equivocado.

NICOLÁS CABALLERO Muchas gracias, esperemos que eso pueda cambiar. Ahora toma la palabra el representante de Dinamarca.

FINN PETERSEN Gracias, Sr. Presidente. Muchas gracias por la presentación, agradezco mucho esta sesión, estoy de acuerdo en que tenemos que tener PDP que sean más acotados y nos gustaría que esto se haga realidad antes del lanzamiento de la próxima ronda, queremos ver medidas proactivas, creo que, las registraciones masivas son un ejemplo. Nos gustaría ver obligaciones en materia de verificación de identidad o distintos tipos de validación de datos de contacto, creo que, eso es lo que necesitamos hoy en día, por supuesto, también hace falta trasparencia, pero a la hora de priorizar antes de la próxima ronda nosotros consideramos que hay que tener medidas proactivas y esto será apenas un paso hacia adelante, donde quiera que nos estemos dirigiendo.

Ahora bien, con respecto a las registraciones masivas, ¿en su análisis definieron cuál es el límite de registraciones para considerarla una registración masiva? Gracias.

GRAEME BUNTON Con respecto a las registraciones masivas cuando uno trata de poner un límite específico de dominios, ¿los actores maliciosos qué van a hacer? Van a ir por arriba o por debajo de ese número y eso tiene un impacto también en el mercado porque en una búsqueda

uno puede agregar equis cantidad de dominios, entonces eso también va a tener un impacto y ahí tenemos un impacto en el mercado, por eso es riesgoso poner un límite o una cantidad determinada a una registración masiva.

Nosotros utilizamos el informe INFERMAL, trabajamos con API para tener una herramienta y en lugar de ver ese enfoque nosotros trabajamos con esta herramienta que nos pareció más efectiva. En segundo lugar, tenemos que ver el tema de la verificación de nombres de dominios asociados, esto es algo reactivo, sí, pero si un registrador tiene que ver todos los dominios en la cuenta de uno de sus clientes, que pueden ser 10, 20 o 100 dominios, esto es costoso para el registrador, entonces ellos van a ser más cuidadosos en las registraciones porque tendrán esa obligación de verificar todos estos dominios y esperamos que esto tenga un impacto en el mercado e incentive el comportamiento correcto, por eso pusimos esta propuesta en nuestro informe. Gracias.

NICOLÁS CABALLERO Muchas gracias. Tenemos que dar por concluida esta sesión, es realmente muy positivo ver que hay consenso en nuestras sesiones porque en la situación o en el contexto internacional actual el consenso no es algo que se esté dando demasiado. Bueno, muy bien, veo que tenemos consenso en los tres temas de importancia, no los voy a leer, nuevamente, y también en el asesoramiento. Susan, ¿quiere decir algunas palabras de cierre? Dado que, usted lidera este tema para el PSWG.

SUSAN CHALMERS

Muchas gracias, Sr. Presidente. Brevemente, desde la perspectiva de Estados Unidos, los plazos de los PDP deben ser reducidos de manera significativa para concretar políticas cuando se expanda el DNS como resultado de la próxima ronda de nuevos gTLD y esto va dirigido a la comunidad de la ICANN en general, escuchamos propuestas de NetBeacon, la cámara de partes contratadas también hizo propuestas, el grupo de partes interesadas comerciales también, el comité asesor At-Large también tiene ideas, el grupo de partes interesadas no comerciales también tiene prioridades que tienen que ver con las políticas sobre uso indebido del DNS.

Ahora bien, vemos que estamos avanzando en una dirección conjunta y que la comunidad de múltiples partes interesadas de la ICANN debería trabajar en conjunto para obtener un resultado sobre este tema, este momento es muy importante para que se generen resultados concretos de políticas dentro de la ICANN. Muchas gracias.

NICOLÁS CABALLERO

Muchas gracias a la representante de Estados Unidos, les pido disculpas porque nos estamos excediendo del tiempo permitido para esta sesión, después de la pausa para el café tendremos una sesión conjunta con el ALAC y la GNSO. Muchas gracias, que disfruten de su café, gracias.

[FIN DE LA TRANSCRIPCIÓN]